Allegato “a”

AGGIORNAMENTO DOCUMENTO PROGRAMMATICO

DELLA SICUREZZA 2021

DEI TRATTAMENTI DATI PERSONALI

Aggiornato a Settembre 2021

Sommario

Parte Prima – Finalità, organizzazione e obiettivi del D.P.S.

a) Scopo del Documento e modalità di adozione del D.P.S.

Il D.P.S. è un documento di natura programmatica e rappresenta il documento fondamentale per la definizione della strategia di prevenzione del rischio privacy in Azienda.

Il D.P.S. deve essere concepito non come un documento formale, statico, compiuto e con una data di conclusione certa, ma come uno strumento in costante e continua evoluzione nella consapevolezza che i processi di miglioramento di un'organizzazione sono lunghi e complessi e che è necessario affrontarli con una serie di strumenti che vengono progressivamente affinati, modificati, perfezionati o sostituiti in relazione al feedback ottenuto dalla loro applicazione e in base all'esperienza via via acquisita nel corso degli anni.

Il presente D.P.S. aziendale è stato elaborato in un contesto di collaborazione allargata e condivisa in cui i dipendenti sono stati invitati a fornire un proprio contributo alla elaborazione del documento, con suggerimenti, osservazioni e consigli, al fine di migliorare la qualità dei contenuti.

Il presente documento riguarda un arco temporale fino al 2021 e tiene conto degli adeguamenti resisi necessari, anche temporaneamente ed in via sperimentale, per affrontare l'emergenza COVID 19 ed aggiorna il documento adottato dalla Direzione Generale con deliberazione n. 347 del 9.7.2020, ed entro un mese dalla sua adozione verrà pubblicato sul sito intranet aziendale.

Il D.P.S.si compone del presente documento e dei suoi allegati.

Al suo interno sono inseriti i seguenti macro contenuti:

- le misure di prevenzione disposte;
- i rischi e le relative misure specifiche, individuate in base alle risultanze del processo della "gestione del rischio", quale misura di precauzione ;
- i soggetti che intervengono nelle attività di prevenzione e precauzione;
- i tempi e le modalità di monitoraggio da effettuarsi per verificare il rispetto degli obblighi ivi contenuti;
- gli obiettivi fissati e raggiunti nel corso degli anni 2018, 2019, 2020 e quelli previsti dal 2021.

I principi, gli obiettivi e le misure indicate nel presente documento sono e saranno raccordati con gli altri strumenti di programmazione aziendale, in primis con il Piano della Performance.

Tutte le attività e le iniziative in materia di prevenzione contenute nel presente D.P.S. presentano un minimo comune denominatore: creare un percorso di cambiamento culturale che porti a considerare i valori di sicurezza privacy intrinsecamente connessi ad ogni azione e decisione amministrativa per il miglioramento della qualità dei servizi e delle relazioni tra amministrazione e cittadini.

Trattandosi di un cambiamento culturale importante, deve essere accompagnato con una serie di interventi mirati e progressivi. Il 2018 è stato, pertanto, dedicato a "fotografare" lo stato del "sistema privacy" aziendale ed a porre le basi, attraverso un processo bottom up, per la revisione progressiva dello stesso a decorrere dal 2019, in sintonia con il principio dell'*accountability* che permea il regolamento europeo in materia.

Inoltre si rappresenta che l'organizzazione aziendale è in corso di completa revisione, come da nuovo atto di autonomia aziendale adottato con deliberazione n°239 del 19.4.2018, la cui piena applicazione organizzativa è ancora in corso, con conseguente necessità di revisione in base al nuovo assetto organizzativo delle denominazioni delle strutture preposte ai trattamenti ed alle funzioni evidenziate dal presente D.P.S..

Con deliberazione n.260 del 23.5.2018 è stata adottata una prima versione del D.P.S. aziendale in materia privacy, in adeguamento alla normativa europea del Regolamento UE 679/2016.

Con D.lgs. 10.8.2018 n.101 sono state emanate le disposizioni nazionali di armonizzazione dell'ordinamento nazionale alle disposizioni del Regolamento UE 679/2016.

Con deliberazione n. 239 del 19/4/2018 si era proceduto all'adozione dell'Atto Aziendale di diritto privato ai sensi dell'art. 3 c. 1-bis, del D.Lgs. n. 502 del 30/12/1992 e s.m.i. rimodulato secondo gli aspetti e/o rilievi rappresentati da A.Li.Sa. e Regione Liguria;

Con deliberazione n.353 del 2/8/2018 si è preso atto della D.G.R. della Regione Liguria n. 547 del 13/7/2018, che ha dichiarato il suddetto Atto di Autonomia Aziendale *"coerente con il vigente quadro normativo e programmatorio regionale",* prevedendo prescrizioni alle quali l'ASL3 prevede ivi di dare progressiva attuazione, come anche precisato nella successiva deliberazione n.558 del 22/11/2018, ad oggetto: "*Ulteriori procedure attuative conseguenti alla presa d'atto della D.G.R. della Regione Liguria n. 547 del 13/7/2018 ad oggetto "Atto di Autonomia Aziendale della A.S.L. n. 3.Provvedimenti conseguenti*";

Si ritiene pertanto opportuno provvedere ad una revisione del D.P.S. aziendale che tenga conto della normativa nazionale sopravvenuta nonché delle modifiche organizzative e delle modifiche applicative intervenute successivamente alla prima stesura del maggio 2018 ed ancora in corso di definizione.

Il D.P.S. aziendale –ovviamente- quale documento dinamico, potrà essere oggetto di ulteriori revisioni in relazione all'evolversi della regolamentazione della materia e dell'organizzazione aziendale.

In punto si deve tener conto della situazione emergenziale dichiarata con **D.P.C.M. del 31.01.2020** (Dichiarazione dello stato di emergenza nazionale in conseguenza del rischio sanitario connesso l'insorgenza di patologie derivanti da agenti virali trasmissibili) e successive proroghe , alla quale è conseguita tutta una serie di interventi normativi che hanno introdotto temporanee limitazioni e/o esclusioni nell'esercizio dei diritti correlati al trattamento dati, previsto possibilità di informazioni e/o autorizzazioni orali, demandato al post emergenza la formalizzazione di alcuni degli obblighi nascenti dalla nuova normativa Europea, al fine di agevolare l'intervento sanitario in occasione della pandemia in corso, previsto l'introduzione di obblighi vaccinali e/o di controllo del possesso di green pass per l'espletamento di alcune attività.

Inoltre la natura di azienda sanitaria di A.S.L. 3 ha ovviamente reso poco percorribile nel 2021 l'assegnazione alle strutture, soprattutto a vocazione sanitaria, di obiettivi che non fossero correlati strettamente alla gestione della pandemia ed il perseguimento di iniziative di formazione e/o monitoraggio on the job che coinvolgessero il personale impegnato nella gestione quotidiana dell'emergenza e delle conseguenze anche organizzative della stessa.

b) Novità del presente aggiornamento e fonti normative consultate

Ai fini di favorire una maggiore diffusione dei contenuti del documento e facilitarne la lettura da parte dei cittadini/utenti e dei dipendenti dell'Azienda il presente aggiornamento si è proposto di rendere il D.P.S. più articolato e dettagliato, ma al contempo di facile lettura.

A tal fine le prime cinque sezioni illustrano il "sistema privacy" aziendale da un punto di vista organizzativo, la sesta sezione e gli allegati, le policy generali ed i format di supporto allo stesso.

Si è cercato di:

- chiarire alcuni aspetti inerenti alla procedura organizzativa, alla luce delle novità introdotte dalla normativa europea;
- non inserire le mappature e gli elenchi dei trattamenti nel corpo del documento (pubblicandole sul sito intranet aziendale);
- non inserire le singole valutazioni del rischio (pubblicandole sul sito intranet aziendale);
- semplificare la metodologia della gestione del rischio avviata dando risalto all'attività di analisi e riducendo al minimo il numero dei format da compilare;
- pubblicare i format della gestione del rischio come allegati separati dal corpo del documento (pubblicandoli anche sul sito intranet aziendale);
- pubblicare come allegato al D.P.S. una policy privacy riassuntiva dell'assetto del "Sistema privacy" di ASL3;
- prendere atto del lavoro di omogeneizzazione regionale nella gestione del "Sistema privacy", intervenuto a seguito della costituzione del Gruppo di Lavoro degli R.P.D. delle aziende sanitarie liguri di cui alla deliberazione n.173 del 6.7.2018 di A.Li.Sa.

Inoltre il presente aggiornamento ha previsto:

- il coinvolgimento degli organi di indirizzo nella predisposizione del piano, attraverso l'individuazione degli obiettivi strategici di riprogettazione della gestione del rischio privacy;
- la previsione delle future attività di monitoraggio sull'attuazione delle misure di sicurezza, da intendersi come strumento di responsabilizzazione dei soggetti coinvolti nell'attuazione delle misure, concependo le misure stesse e la loro applicazione come obiettivi di performance organizzativa ed individuale;
- il rafforzamento della formazione come strumento fondamentale della prevenzione, mirato a favorire non solo un'acquisizione di cognizioni tecniche o giuridiche relative alla normativa privacy e ad una più puntuale conoscenza dei fattori di rischio, ma anche a favorire un cambiamento culturale nell'Azienda;
- l'aggiornamento della modulistica di supporto al "Sistema privacy" aziendale, anche tenendo conto delle esigenze nascenti dall'emergenza COVID 19 per un'Azienda Socio Sanitaria *(**ALLEGATI A, A1, A2, A3, C, H, I, J, L, R e allegati da 19 a 26.4**)*;
- la creazione di una connessione stringente tra il D.P.S. , comunque mantenuto negli anni precedenti come strumento aziendale di sintesi delle politiche in materia dell'Azienda, ed il ciclo della Performance;
- una capillare azione di sensibilizzazione all'interno dell'Azienda per favorire la creazione di gruppi di lavoro per l'aggiornamento della gestione del rischio privacy;
- la ribadita richiesta di acquisizione di un applicativo che faciliti la gestione ed il monitoraggio del "Sistema privacy" aziendale ed il suo progressivo aggiornamento a decorrere dalla data di acquisizione dello stesso;
- l'instaurazione di un forte legame di collaborazione da parte di tutti i dipendenti dell'Azienda e la creazione di una rete di referenti per il R.P.D. , al fine di capillarizzare il "sistema privacy" in tutte le articolazioni organizzative aziendali;
- la creazione di sinergie a livello regionale tra i responsabili protezione dati delle Aziende del Servizio Sanitario regionale, con partecipazione al Gruppo di lavoro formalizzato con deliberazione di A.Li.Sa. n. 173 del 6.7.2018.

Il Regolamento UE 679/2016 introduce, infatti, energeticamente il principio della responsabilizzazione (c.d. *accountability*).

Per "responsabilizzazione" si deve intendere il compito che hanno i titolari di adottare comportamenti volti a garantire e dimostrare la concreta adozione di misure tecniche ed organizzative per assicurare l'applicazione del Regolamento UE e di conseguenza la conformità alle sue disposizioni.

Detto principio si manifesta concretamente nel Regolamento UE con due concetti, vale a dire la «protezione dei dati fin dalla progettazione (privacy by design)» e la «protezione dei dati per impostazione predefinita (privacy by default)», evidenziati all'art. 25 del Regolamento UE, e con gli adempimenti di cui al capo IV del Regolamento UE 679/2016.

Detti risultati non si possono raggiungere se non con un mutamento culturale complessivo nell'ambito dell'Azienda, con il supporto di R.P.D e strutture aziendali di riferimento per le aree di rispettiva competenza (es. S.C. SIA, S.C. Affari Generali), che dovrà essere costruito e rafforzato nel tempo con gli strumenti evidenziati nel presente documento.

***

Per la predisposizione della presente revisione, oltre al Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*)., e della norma nazionale di armonizzazione D.lgs. n.101 del 10.8.2018 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27.4.2016 , relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*", ci si è avvalsi delle indicazioni del Garante della Privacy previgenti (Linee Guida, Provvedimenti, etc.), con particolare riguardo ai "Chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario" intervenuti con Provvedimento dell'Autorità Garante per la protezione dei dati personali n. 55 del 07.03.2019, compatibili con i principi europei e successive norme e/o linee guida di armonizzazione (es. WP 248 -linee guida concernenti la valutazione di impatto sulla protezione dei dati 4.10.2017; linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29" 3.10.2017), nonché con riferimento ai provvedimenti, indicazioni e chiarimenti in materia di *"coronavirus e protezione dei dati"*, sempre emanati dall'Autorità di controllo, fatti propri dal Titolare quale policy aziendali di sicurezza nei trattamenti di dati personali e da intendersi parte integrante del presente documento.

Si intendono inoltre richiamate in quanto compatibili con le suddette previsioni tutte le policy aziendali in materia, tra le quali quelle di:

- gestione della videosorveglianza di cui alla deliberazione n. 640 del 11.11.2013

- gestione dei contenuti del sito intranet aziendale di cui alla deliberazione n. 271 del 07.05.2014

- inserimento del personale neoassunto-trasferito di cui alla deliberazione n.383 del 20.6.2016

-gestione documentale di cui alla deliberazione n. 405 del 29.6.2016

- gestione dell'attività provvedimentale aziendale di cui alla deliberazione n. 329 del 4.7.2019

- esercizio del diritto di accesso di cui alla deliberazione n. 291 del 21.6.2017

- gestione della dotazione informatica e posta elettronica aziendale di cui alla regolamentazione vigente come da determinazione del S.I.A. n.62 del 14.1.2019, pubblicata sul sito intranet aziendale sezione "Normativa/Privacy" e sua modifica intervenuta con nota ID 75609714 del 15.6.2020 della S.C.S.I.A. **(ALLEGATO 7).**

- regolamentazione dello smartworking in Azienda (Piano Organizzativo del Lavoro Agile – POLA 2021) come riformulato anche sulla base della normativa emergenziale per far fronte alla pandemia e nell'ottica della sua implementazione post emergenziale

- policy privacy aziendale allegata **(ALLEGATO 1).**

- policy analisi rischi a cui sono soggetti i dati **(ALLEGATI 2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 e 2.8).**

- policy aziendale esercizio dei diritti **(ALLEGATI 3 e 3.1).**

- policy aziendale data breach **(ALLEGATI 4 e 4.1).**

- vademecum sperimentazioni cliniche (ALLEGATO B)

-GEN-DG-PR Trattamento per scopi di ricerca scientifica-00 **(ALLEGATI 5 e 5.1).**

- GEN-DG-PR Trattamento dati genetici-00 **(ALLEGATI 6 e 6.1)**

- Ufficio RPD/DPO - Regolamento attività **(ALLEGATO 8).**

c) Resoconto sul raggiungimento degli obiettivi strategici 2018-2019

Sintesi obiettivi 2018

La Direzione Generale ha definito nel 2018 gli obiettivi strategici e le finalità da perseguire, di cui si fornisce di seguito una sintesi:

1. Formazione come strumento di diffusione della cultura in materia di privacy
   1.1. attivazione corso FAD aggiornato alla nuova regolamentazione europea e nazionale della materia;
   1.2. incontri formativi e/o audit dedicati per area di appartenenza per i dirigenti responsabili privacy ed i referenti del progetto privacy.
2. Avvio del progetto "gestione del rischio"
   2.1 Individuazione di una rete di referenti e di "una cabina di regia" per la gestione del progetto privacy e del "sistema privacy" aziendale
   2.2 Revisione della mappatura dei procedimenti aziendali ai fini della valutazione del rischio privacy creazione del registro dei trattamenti
   2.3 Valutazione e gestione del rischio privacy (risk assessment)
   2.4 Revisione della modulistica di supporto al progetto

2.5 Revisione della gestione dei trasferimenti ed incarichi esterni (trasferimenti dati, responsabili esterni)
2.6 Rivisitazione dell'Informativa, tenendo conto delle eventuali indicazioni di A.Li.Sa.
2.7 Definizione dei rapporti con il **Data Protection Officer** (Responsabile Protezione Dati-R.P.D.)

3 Collegare il D.P.S.al Ciclo della Performance attraverso l'assegnazione di obiettivi organizzativi e individuali relativi alla progettualità del "sistema privacy" Aziendale.

4 Revisione della gestione delle autorizzazioni al trattamento.

Attività svolte nel corso del 2018-2019-2020 e programmate a decorrere dal 2021 per dare seguito agli obiettivi strategici, compatibilmente con le criticità determinate dalla pandemia.

1. Formazione come strumento di diffusione della cultura in materia di privacy
   1.1. attivazione corso FAD aggiornato alla nuova regolamentazione europea e nazionale della materia: lo stesso è stato reso disponibile a decorrere da fine giugno 2018, ed è stato revisionato per adeguamento alle norme di armonizzazione nazionali sopravvenute in materia. Tutti i dipendenti individuati quali referenti per l'avvio del progetto del nuovo "Sistema privacy" (dirigenti autorizzati o individuati dai relativi dirigenti responsabili quali autorizzati ai trattamenti) dovevano effettuare il corso FAD base entro la fine dell'anno 2018 e frequentare l'aggiornamento a decorrere dal 2020;
   1.2. incontri formativi e/o audit dedicati per area di appartenenza per i dirigenti responsabili privacy ed i referenti del progetto privacy: si sono tenuti incontri con il coordinamento della S.C. Affari Generali, con tutti i referenti privacy, a presentazione e supporto al progetto a partire dal primo semestre del 2018. Nel corso del 2019-2020 gli incontri sono stati mirati alla soluzione di specifiche problematiche di settore. Dal 2021 sono previsti ulteriori incontri per area di riferimento per supportare l'aggiornamento del registro dei trattamenti, compatibilmente con l'emergenza pandemica COVID 19.
2. Avvio del progetto "gestione del rischio"
   2.1. Individuazione di una rete di referenti e di "una cabina di regia" per la gestione del progetto privacy e del "sistema privacy" aziendale: la "cabina di regia" è stata costituita con nota prot.n 20355 del 9.2.2018 e formata una rete di referenti aziendale condivisa con i responsabili delle strutture aziendali, come da elenco pubblicato su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") e periodicamente aggiornato.
   2.2. Revisione della mappatura dei procedimenti aziendali ai fini della valutazione del rischio privacy creazione del registro dei trattamenti: effettuata entro il 25.5.2018 come da registro dei trattamenti pubblicato, nelle sue articolazioni, su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") e previsione relativi aggiornamenti entro 15 giorni dalle relative variazioni, con correlativa informativa a R.P.D, referente privacy di afferenza e S.C. Affari Generali.

2.3. Valutazione e gestione del rischio privacy (risk assessment): effettuata con metodologia "bottom up" entro il 25.5.2018, come da format pubblicati, nelle loro articolazioni, su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") e previsione relativi aggiornamenti entro 15 giorni dalle relative variazioni, con correlativa informativa a R.P.D, referente privacy di afferenza e S.C. Affari Generali.

2.4. Revisione della modulistica di supporto al progetto: entro il 25.5.2018 format pubblicati su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") ed allegati al presente documento, nelle versioni aggiornate in sede applicativa, a tutto il 2021.

2.5. Revisione della gestione dei trasferimenti ed incarichi esterni (trasferimenti dati, responsabili esterni): entro il 25.5.2018 format pubblicati su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") ed allegati al presente documento nelle versioni aggiornate in sede applicativa al 2021 **(ALLEGATI 9, 9.1 e 9.2)** ed ai relativi contratti-accordi contrattuali (sulla base eventualmente delle indicazioni di A.Li.Sa. per quelli in corso), entro 30 giorni dalla pubblicazione del relativo format ed allegato al presente documento nella versione aggiornata in sede applicativa al 2021 **(ALLEGATO 10)**.

2.6. Rivisitazione dell'Informativa, tenendo conto delle eventuali indicazioni di A.Li.Sa. in punto in caso di trattamenti di interesse regionale: entro il 25.5.2018 format pubblicati su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") (sulla base eventualmente delle indicazioni di A.Li.Sa. per i trattamenti in corso di interesse regionale) ed allegati al presente documento nelle versioni aggiornate in sede applicativa per i format generali a tutto il 2021 **(ALLEGATI 11, 11.1, 12, 13 e 14)**.

2.7. Definizione dei rapporti con il **Data Protection Officer** (Responsabile Protezione Dati-R.P.D.): come previsti nel presente D.P.S e nell'atto di nomina dello stesso, anche in relazione alle previsioni dell'atto di autonomia aziendale in materia di competenze della S.C. Affari Generali e collaborazione con lo stesso per gli adempimenti di competenza da parte di tutti i dipendenti nei tempi e modi fissati dal D.P.S e dallo stesso e nella totalità delle richieste – casi di interesse **(ALLEGATO 8).**

3. Collegare il D.P.S. al Ciclo della Performance attraverso l'assegnazione di obiettivi organizzativi e individuali relativi alla progettualità del "Sistema privacy" aziendale: tutte le strutture aziendali hanno ricevuto, in sede di discussione dei budget dal 2018 obiettivi coerenti al progetto privacy aziendale.

4. Revisione della gestione delle autorizzazioni al trattamento: entro il 25.5.2018 format pubblicati su specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") ed allegati al presente documento nella versione aggiornata in sede applicativa a tutto il 2021 e revisione delle autorizzazioni entro 30 giorni dalla pubblicazione del registro trattamenti e/o sua revisione incidente sull'autorizzazione **(ALLEGATI 15, 16, 17).**

E' stato altresì previsto il costante aggiornamento della gestione del rischio, inteso come processo dinamico i cui risultati sono frutto della maturazione e dell'esperienza che si consolida col tempo:

a. **Mappatura**: per ogni trattamento individuare l'origine del processo (input), il risultato atteso (output), la sequenza delle attività che consente di raggiungere il risultato, i tempi, i vincoli, le risorse, le interrelazioni tra i trattamenti. La stessa è stata effettuata entro il 25.5.2018, rivista ed eventualmente aggiornata nel corso del 2019 e del 2020 e ne è prevista una ulteriormente revisione a decorrere dal 2021 **(ALLEGATO 2.3)**, anche in correlazione alla riorganizzazione in corso di attuazione sulla base di rimodulazione di dettaglio in relazione alle esigenze operative riscontrate, della scheda di rilevazione;

b. **Valutazione e trattamento del rischio**: I rischi devono essere reali e specifici e calati nel contesto di riferimento. Le misure dovranno essere adeguatamente progettate, sostenibili, verificabili, con la previsione di indicatori di monitoraggio e di valori attesi. Una prima valutazione è stata effettuata entro il 25.5.2018. Per il 2020 e/o data successiva di effettiva fornitura del supporto informatico necessario, è prevista una revisione della stessa, anche sulla base della struttura del suddetto supporto informatico che verrà fornito per la gestione del "Sistema privacy" aziendale. In merito alla metodologia utilizzata si fa riferimento alla specifica policy aziendale allegata. (**ALLEGATI 2, 2.1, 2.2 2.3, 2.4, 2.5, 2.6, 2.7 e 2.8).**

Inoltre l'introduzione di un sistema di "*internal auditing*", avviato con il supporto della S.C. Affari generali già nel 2018, a supporto dell'avvio del progetto del nuovo "Sistema privacy" e che si è sviluppato dal 2019 a tutt'oggi nelle singole strutture aziendali, facendone oggetto anche di specifico obiettivo di budget, garantisce uno strumento per rafforzare il sistema dei controlli finalizzati alla prevenzione del rischio privacy:

c. Identificazione dei soggetti addetti alle attività di auditing (dirigenti, referenti, facilitatori, etc. già individuati nel "Sistema-privacy" aziendale nel 2018 ed altri dipendenti della struttura secondo un cronoprogramma gestito dalla stessa)

d. Identificazione di un processo standardizzato per effettuare l'audit (con indicazioni di tempi e modalità di effettuazione) e programmazione di audit periodici. E' stato oggetto di specifici obiettivi di budget dal 2019.

e. Definizione di monitoraggi periodici attraverso controlli sul campo, con acquisizione della documentazione (check – list, verbali ecc..): che è stato oggetto di specifici obiettivi di budget dal 2019.

f. Monitoraggio dei trattamenti (accertandone la funzionalità e l'affidabilità) e delle misure di prevenzione (accertandone la congruità e l'efficacia reale): sulla base del format pubblicato in specifica sottosezione del sito intranet aziendale (sezione "Normativa – Privacy") ed allegato al presente documento. E' stato oggetto di specifici obiettivi di budget dal 2019.

Obiettivi 2019

In particolare nel 2019 sono stati previsti per tutte le strutture aziendali:

- almeno due audit privacy interni con la partecipazione obbligatoria di Dirigenti responsabili della struttura e facilitatori della struttura e di dipendenti dagli stessi individuati.
- eventuale aggiornamento della mappatura e della valutazione del rischio per i trattamenti di afferenza , anche in correlazione con intervenute modifiche organizzative e loro pubblicazione con le modalità previste dal DPS
- almeno un audit privacy esterno-controllo, anche correlato ad altre attività di ispezione e controllo quali-quantitativo nell'ambito dell'esecuzione del rapporto, nei confronti di soggetto nominato responsabile esterno o contitolare in trattamento che afferisce alla struttura per competenza tecnico-economico-gestionale

- almeno un incontro formativo/illustrativo in materia di privacy con i dipendenti
- frequenza del corso FAD 2018 privacy dai dipendenti individuati dal direttore della struttura e comunicati alla SC Aggiornamento e Formazione.

Obiettivi 2020

In particolare nel 2020, compatibilmente con le esigenze nascenti dalla gestione dell'emergenza pandemica, sono state previste per alcune strutture aziendali:

almeno un audit privacy interno annuale , con la partecipazione obbligatoria di Dirigenti responsabili della struttura e facilitatori della struttura ed eventualmente di dipendenti dagli stessi individuati.
- aggiornamento della mappatura e della valutazione del rischio per i trattamenti di afferenza, anche in correlazione con intervenute modifiche organizzative, sulla base di format di dettaglio pubblicato sul sito intranet aziendale e loro pubblicazione con le modalità previste dal DPS.

Obiettivi a decorrere dal 2021

A decorrere dal 2021 e per il solo secondo semestre dell'anno (essendo gli obiettivi di budget del primo semestre ricollegati alla gestione del piano pandemico aziendale), compatibilmente con le esigenze nascenti dalla gestione dell'emergenza pandemica è stata proposta l'implementazione nelle strutture –aree aziendali delle seguenti attività:

- effettuazione di un audit privacy interno, con modalità compatibili alla situazione pandemica in atto, con finalità anche formative, condotto con un gruppo di lavoro interno che aggiorni la mappatura e la valutazione del rischio per i trattamenti di afferenza nelle relative schede del registro dei trattamenti, completandolo con la scheda di analisi del trattamento rev 2020 (intranet/Normativa/Privacy/modelli) per i trattamenti interessati

- almeno un incontro formativo/illustrativo annuale in materia di privacy con i dipendenti - frequenza del modulo di aggiornamento corso FAD 2019 privacy dai dipendenti individuati dal direttore della struttura e comunicati alla SC Aggiornamento e Formazione.

Proseguirà quindi nelle prossime annualità il collegamento del D.P.S. con il ciclo della Performance, con una maggior flessibilità organizzativa in capo ai direttori delle relative strutture-aree aziendali, quali dirigenti con compiti specifici del Sistema privacy aziendale, che potranno declinare specifici obiettivi interni al proprio personale in materia.

La rivalutazione del rischio e la regolarizzazione dell'attività di auditing consentiranno infatti progressivamente – a regime - in sede di discussione di budget, di:

g. definire specifici obiettivi di prevenzione per i trattamenti delle strutture a maggior rischio

h. diversificare gli obiettivi avendo riguardo alla realtà e alla criticità dei trattamenti delle strutture

i. inserire tra gli obiettivi anche l'applicazione delle specifiche misure di prevenzione individuate dalle singole strutture

j. Far individuare ai dirigenti obiettivi individuali di prevenzione per i propri collaboratori.

L'intero sistema è stato poi supportato a decorrere dal 2019 dall'effettuazione di audit di sistema, sulla base delle indicazioni della ISO UNI 19011 e da reportistica di analisi delle check list di controllo, quale fotografia dello stato dell'arte aziendale di implementazione del Sistema Privacy di n. 94 strutture aziendali (di cui 2 in corso di riorganizzazione), raggruppate in n.11 Dipartimenti e n. 4 staff.

d) ***Attori coinvolti nelle politiche di prevenzione***

a) Ruolo della Direzione Generale

Il Direttore Generale individua il **Data Protection Officer** (Responsabile Protezione Dati-R.P.D.).

Inoltre definisce, di concerto con quest'ultimo e con il supporto della S.C. Affari Generali e della S.C.S.I.A., gli obiettivi strategici in materia di prevenzione che costituiscono contenuto necessario dei documenti di programmazione strategico-gestionale e del D.P.S.. L'organo di indirizzo adotta il D.P.S. su proposta della S.C. Affari Generali , tenuto conto delle indicazioni del R.P.D. e con il supporto della S.C.S.I.A., di norma, entro il primo semestre di ogni triennio, a decorrere dal 2021, e, comunque, provvede ad aggiornamenti ogniqualvolta ritenuti necessari.

L'aggiornamento di format e policy aziendali avviene costantemente, anche separatamente rispetto alla revisione del D.P.S. aziendale ed è oggetto di adeguata pubblicità sul sito intranet aziendale (sezione "Normativa – Privacy") e, ove previsto, sul sito internet aziendale.

b) Nomina e compiti del Data Protection Officer (Responsabile Protezione Dati-R.P.D.).

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile Protezione dei dati personali (R.P.D.) (artt. 37-39).
Il predetto Regolamento prevede l'obbligo per il titolare di designare il R.P.D. *«quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali»* (art. 37, paragrafo 1, lett a).
Le predette disposizioni prevedono che il R.P.D. *«può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»* (art. 37, paragrafo 6) e deve essere individuato *«in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39»* (art. 37, paragrafo 5) *e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»* (considerando n. 97 del RGPD).
A.S.L. 3 è tenuta alla designazione obbligatoria del R.P.D. nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD.
Nel proprio atto di autonomia aziendale, da ultimo riadottato con deliberazione n.239 del 19.4.2018, ha posto in capo alla S.C. Affari Generali l'attività di coordinamento delle politiche aziendali in materia di tutela dei dati personali, ai sensi di quanto previsto dal Regolamento Europeo (General Data Protection Regulatione n. 679/2016- RGPD) e norme correlate, compresi il monitoraggio normativo e la definizione degli atti regolamentari e/o direttive di settore e loro diffusione, l'implementazione nell'ambito dell'Azienda di un sistema di gestione del rischio privacy, le attività di esercizio diritti degli utenti, la formazione e sviluppo di progettualità aziendali in materia, anche a supporto del R.P.D. aziendale.
Con deliberazione n.258 del 18.5.2018 A.S.L. 3 ha nominato, pertanto, il proprio R.P.D., interno, valutandone il possesso del livello di conoscenza specialistica e delle competenze

richieste dall'art. 37, par. 5, del RGPD e l'assenza di situazioni di conflitto di interesse con la posizione da ricoprire ed i compiti e le funzioni da espletare.

Il R.P.D., nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) tenere copia del registro delle attività di trattamento del Titolare, la cui redazione, aggiornamento, conservazione e pubblicità, come previsto nel D.P.S. aziendale, rimane sotto la responsabilità delle strutture aziendali competenti, per gli ambiti di rispettiva competenza.

I suddetti compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dall' A.S.L. 3.

A.S.L.3, in qualità di titolare, si impegna a:

a. mettere a disposizione del R.P.D. risorse adeguate al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate ed a prevedere la consulenza e/o collaborazione di tutti i professionisti operanti all'interno dell'Azienda nell'ambito dell'attività istituzionale degli stessi per gli aspetti di relativa competenza, dato che le prestazioni svolte dal R.P.D. non solleveranno, comunque, dalle specifiche responsabilità le funzioni aziendali formalmente preposte, ma si coordineranno con esse per la migliore realizzazione degli obiettivi individuati;
b. non rimuovere o penalizzare il R.P.D. in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
c. garantire che il R.P.D. eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

d. mettere a disposizione del R.P.D. una rete operativa di referenti all'interno delle strutture aziendali, con il compito di facilitare l'implementazione degli strumenti di risk management in materia di privacy nelle proprie realtà operative e di diffondere nelle stesse un corretto approccio alla sicurezza nella gestione operativa quotidiana. Detta rete è definita di concerto con i responsabili delle strutture di volta in volta coinvolte nella progettualità di gestione del rischio privacy;
e. rendere disponibile il nominativo e i dati di contatto del R.P.D. (recapito postale, telefono, email) nella intranet dell'A.S.L. 3 e comunicarli al Garante per la protezione dei dati personali. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale.

I dati di contatto del R.P.D. sono pubblicati sul sito intranet aziendale, in specifica sottosezione della sezione "Normativa Privacy" e sul sito internet aziendale in specifica sottosezione "Politiche della Privacy" della sezione "Siti Tematici ed in "Amministrazione Trasparente".

L'ufficio del DPO è regolato da specifica policy aziendale.

c) Nomina e ruolo dei Referenti

Per l'applicazione delle politiche di prevenzione è imprescindibile una stretta collaborazione da parte di tutta l'organizzazione.

Per questa ragione sono stati designati dei Referenti per la Prevenzione del rischio privacy (Responsabile Protezione Dati –R.P.D., Responsabile della Prevenzione della Corruzione e della Trasparenza -R.P.C.T, medico competente -pur essendo lo stesso titolare autonomo-, direttori di dipartimento di area territoriale, di area amministrativo-tecnico-professionale, direzioni strategiche amministrativa sanitaria e sociosanitaria, S.C. Direzione Medica del P.O.U. e responsabile ex art.37.4 LR ligure 41/2006 e s.m.i., Direttori di Distretto, Strutture Di Staff Della Direzione Generale, nell'ambito delle loro rispettive competenze e funzioni), essi stessi autorizzati al trattamento dati dal Titolare, anche con delega alla sottoscrizione in capo alle direzioni strategiche amministrativa sanitaria e sociosanitaria per area di rispettiva afferenza, anche a sostegno dell'attività del R.P.D.. Il ruolo dei Referenti si caratterizza nel fatto di porsi come "intermediari" tra il R.P.D. ed i Dirigenti o altri Dipendenti. I Referenti informano il R.P.D. sull'organizzazione e sull'attività dell'amministrazione, "monitorando" l'attività svolta dai Dirigenti-Dipendenti assegnati alle aree di riferimento.

Di seguito si elencano le principali attività in capo ai Referenti:

- coordinano le attività ed i compiti in materia di prevenzione del rischio privacy dei Dirigenti-Dipendenti dell'area di afferenza, fornendo al R.P.D. tutte le informazioni ed i dati delle strutture inserite nell'area di riferimento, necessarie per la concreta applicazione delle misure di prevenzione del rischio in materia privacy;
- relazionano il R.P.D. (e per conoscenza la S.C. Affari Generali) almeno con cadenza annuale sull'attività svolta in materia di privacy e sul rispetto dell'applicazione delle norme contenute nel D.P.S. da parte dei Dirigenti-Dipendenti assegnati alle aree di riferimento;
- relazionano il R.P.D. monitorando l'attività svolta dai Dirigenti-Dipendenti con riferimento alla conoscenza della normativa in materia;
- trasmettono al R.P.D., per il tramite dei Facilitatori di area (vedi successiva lett. d), le schede, relative alla rivalutazione e monitoraggio del rischio, di tutte le strutture appartenenti alla propria area di riferimento se non fatto direttamente dalle stesse;
- provvedono al costante monitoraggio dell'aggiornamento per il tramite dei Facilitatori e dei Dirigenti delle aree di riferimento del registro dei trattamenti, a supporto del R.P.D.;
- adottano adeguate misure organizzative al fine di ricevere da parte dei Dirigenti responsabili dell'area di riferimento e/o far pervenire al R.P.D., tutti gli aggiornamenti in merito alle revisioni del registro dei trattamenti, alla valutazione del rischio, alle misure di sicurezza, alle revisioni delle nomine di responsabili esterni, conferite o ricevute in relazione all'area diretta, e soggetti autorizzati al trattamento dati afferenti alle strutture dirette, firmate dagli stessi Dirigenti, per conto del titolare, per delega o sub delega alla sottoscrizione, nonché le richieste di valutazione preventiva di impatto di nuovi trattamenti;
- individuano il Facilitatore della prevenzione afferente alla propria area di riferimento (vedi lett. e);
- si accertano che all'interno di ogni struttura afferente alla propria area di riferimento venga svolto il processo della gestione del rischio privacy, secondo i criteri previsti dal D.P.S ., dal Titolare e dal R.P.D.;
- si accertano che all'interno delle aree di riferimento siano costituiti ed organizzati appositi **gruppi di lavoro** per garantire la massima partecipazione possibile nelle attività di individuazione dei rischi privacy e di predisposizione delle misure di contenimento degli stessi.

Si precisa che, laddove manchi, sia temporaneamente vacante o non venga individuato, ad esempio un Direttore di Dipartimento, i compiti del Referente aziendale sono automaticamente trasferiti ai dirigenti responsabili delle singole strutture afferenti al Dipartimento stesso (che vengono delegati direttamente dal Titolare alla sottoscrizione dell'au-

torizzazione di direttori di S.S.D. e dipendenti di afferenza), parimenti laddove sia temporaneamente vacante o non venga individuato il dirigente responsabile della S.C. o della S.S.D., i compiti del Referente aziendale sono automaticamente trasferiti ai dirigenti-direttori responsabili a cui afferiscono le relative funzioni per area di riferimento.

Nelle more della piena attuazione della nuova organizzazione aziendale analogo principio verrà applicato alle strutture attualmente esistenti con riferimento ai Dipartimenti attualmente individuati di effettiva afferenza e/o alle diverse denominazioni date alla medesima articolazione operativa-ambito di competenze.

Le autorizzazioni già rilasciate dal Titolare sulla base del suddetto sistema di delega alla sottoscrizione rimangono valide, ad invarianza delle funzioni svolte, fino a cessazione dalle funzioni per qualsiasi causa e/o assegnazione ad altre funzioni dell'autorizzato, indipendentemente dall'eventuale mutamento della denominazione della struttura-area di appartenenza sulla base del vigente atto di autonomia aziendale. A dette autorizzazioni si ricollegano automaticamente le istruzioni ed obbligazioni eventualmente sopravvenute, anche a modifica dei format e delle policy ed indicazioni aziendali in materia, all'atto della loro pubblicazione sul sito intranet aziendale nella specifica sottosezione della sezione "Normativa Privacy".
Le nomine a responsabile esterno e/o gli accordi di contitolarità già sottoscritti sulla base del suddetto sistema di delega di firma rimangono valide fino alla scadenza e/o revoca delle stesse, indipendentemente dall'eventuale mutamento della denominazione della struttura-area di appartenenza del delegato alla sottoscrizione sulla base del vigente atto di autonomia aziendale e/o alla sua cessazione dalle funzioni per qualsiasi causa e/o assegnazione ad altre funzioni.

d) Ruolo dei dirigenti di Struttura Complessa o S.S.D. o strutture assimilate ai fini privacy

I dirigenti direttori di S.C. o di S.S.D. o strutture assimilate ai fini privacy:

1) sono autorizzati dal Titolare al trattamento dati personali e categorie particolari di dati personali afferenti la struttura dagli stessi diretta, con ***designazione all'espletamento degli specifici compiti*** *infra precisati per la gestione del sistema privacy nella struttura dagli stessi diretta (con eventuale delega alla sottoscrizione delle autorizzazioni degli stessi per conto del Titolare in capo al relativo direttore –dirigente referente di afferenza) e sub delegati per conto dello stesso Titolare dal direttore –dirigente referente di afferenza alla sottoscrizione per conto del titolare delle autorizzazioni al trattamento dati personali e categorie particolari di dati personali per i Dipen-*

denti afferenti alle strutture dagli stessi dirette, per i dati di competenza trattati; concorrono alla definizione di misure idonee a prevenire il rischio privacy ed a controllarne il rispetto da parte dei Dipendenti della struttura cui sono preposti, coordinandosi con il Referente di area ed il R.P.D.;

2) forniscono le informazioni richieste dal R.P.D. con particolare riguardo alle attività nell'ambito delle quali è più elevato il rischio privacy e formulano specifiche proposte volte alla prevenzione del rischio medesimo;

3) sono responsabili della redazione, aggiornamento, conservazione e pubblicità, come previsto nel D.P.S. aziendale, del registro dei trattamenti e documenti correlati di mappatura e risk assessment e risk management, per la struttura a cui sono preposti;

4) provvedono al monitoraggio delle attività svolte nella struttura a cui sono preposti, con particolare riguardo all'ambito di quelle nelle quali è più elevato il rischio privacy, nonché a quelle svolte da responsabili esterni e/o contitolari che collaborano ai trattamenti della struttura-area di afferenza, anche attraverso un'attività periodica di auditing.

Alla luce di quanto sopra il compito fondamentale assegnato ai Dirigenti delle varie strutture è quello di **curare il processo della gestione del rischio ed il suo aggiornamento**, concorrendo all'individuazione dei rischi, alla loro valutazione ed all'individuazione delle misure di prevenzione, alla gestione di eventuali violazioni. L'individuazione dei rischi e delle misure deve avvenire attraverso un'attività di analisi meditata e partecipativa. Di conseguenza ai Dirigenti è richiesto di avvalersi del proprio personale e di costituire apposito/i **gruppo/i di lavoro** sovraintendendone le attività ed i lavori.

La collaborazione dei Dirigenti è fondamentale per consentire al titolare che adotta il D.P.S., con la collaborazione del R.P.D. e delle S.S.C.C. S.I.A. ed Affari Generali, di definire misure concrete e sostenibili da un punto di vista organizzativo, entro tempi chiaramente definiti. Il Titolare deve infatti individuare e programmare le misure in termini di precisi obiettivi da raggiungere da parte di ciascuna delle strutture coinvolte anche ai fini della responsabilità dirigenziale.

Oltre a quanto sopra riportato i Dirigenti:

- individuano un proprio Facilitatore della prevenzione del rischio privacy (vedi punto e);

- verificano la presenza, la correttezza, la completezza, l'aggiornamento, la semplicità di consultazione, l'omogeneità di tutte le informazioni ed i dati delle strutture dirette, necessarie per la concreta applicazione delle misure di prevenzione del rischio in materia privacy;
- accertano che l'aggiornamento e trasmissione dei dati al R.P.D. avvenga secondo la procedura e le tempistiche prevista nel presente D.P.S.;
- garantiscono un adeguato sostegno ai Referenti riguardo a tutti i compiti loro assegnati, sulla prevenzione del rischio, come indicato alla lett. c);
- trasmettono tempestivamente (e comunque entro 15 giorni dalla variazione) al Referente ed al R.P.D. e per conoscenza alla S.C. Affari Generali i dati di gestione del rischio privacy della propria struttura ed i relativi aggiornamenti;
- promuovono e accertano la conoscenza della normativa privacy e del D.P.S. aziendale, da parte del proprio personale, relazionando il Referente di area ed il R.P.D. sulle criticità che hanno accertato;
- sono delegati alla sottoscrizione per conto del Titolare delle designazioni dei responsabili esterni del trattamento che collaborano ai trattamenti della propria struttura (come compito specifico nel "Sistema privacy" aziendale del dirigente alla cui struttura-area afferiscono per competenza tecnico –economico-gestionale i relativi trattamenti), secondo le procedure, tempistiche e modalità previste dal D.P.S., fornendo agli stessi le necessarie istruzioni, nonché degli accordi di contitolarità, inerenti i trattamenti di competenza della propria struttura, effettuando audit periodici di controllo del rispetto da parte dei designati responsabili/contitolari delle istruzioni fornite in materia privacy e gestendo eventuali violazioni che li coinvolgano ed aggiornando in punto il R.P.D. e la S.C. Affari Generali.

e) Facilitatori tra il R.P.D. ed i Referenti e Dirigenti delle strutture aziendali

Per rendere più snello ed efficace il coordinamento tra il R.P.D. ed i Referenti e tra questi e i Dirigenti responsabili di struttura, sono individuate figure di collegamento denominati ***Facilitatori*** scelti tra quei dipendenti forniti di esperienza al fine di trattare gli aspetti operativi connessi alla prevenzione, alla gestione del rischio privacy e per le attività di supporto nelle attività di monitoraggio e di informare i Referenti/Dirigenti su problemi, criticità riscontrate. Lo scopo dell'introduzione di queste figure è volta, da un lato, ad agevolare e velocizzare le procedure ed i tempi degli adempimenti, snellendo i compiti dei Dirigenti (i quali, pur rimanendo responsabili delle attività e specifici compiti previsti dal D.P.S. in materia di gestione privacy nelle proprie

strutture, sono sgravati da compiti meramente operativi) e dei Referenti; dall'altro, a rendere più omogenee, tra le strutture, le attività di prevenzione del rischio privacy.

Queste figure si dividono in:

1) **I facilitatori dei Referenti**: nominati da questi ultimi, in sintesi si occupano di raccogliere e/o rendere omogenei i dati relativi alla gestione del rischio, ai monitoraggi e agli altri adempimenti di tutte le strutture dell'area di riferimento ed, una volta acquisito l'assenso del proprio Referente di trasmetterli al R.P.D.. In particolare i Facilitatori dei Referenti hanno il compito di aiutare il Referente nella programmazione dei monitoraggi interni e/o nella trasmissione al R.P.D. delle relative relazioni a riscontro della suddetta attività di controllo, trasmettendo via mail (all'email dedicata dello stesso rpd@asl3.liguria.it e per conoscenza alla S.C. Affari Generali: email segreteria.contratticonvenzioni@asl3.liguria.it) i documenti e le relazioni richieste e le richieste dei referenti di valutazione preventiva di impatto di nuovi trattamenti;

2) **I facilitatori dei Dirigenti** delle strutture aziendali, che si occupano di raccogliere i dati relativi ai trattamenti delle singole strutture, inviandoli al facilitatore del Referente di area. In particolare i Facilitatori delle varie strutture sono chiamati a tenere i contatti con i **gruppi di lavoro**, a raccogliere i dati della gestione del rischio, dei monitoraggi e dei vari adempimenti richiesti alle singole strutture ed, una volta acquisito l'assenso del proprio Dirigente, a trasmetterli al facilitatore del Referente di area, al R.P.D. (all'email dedicata dello stesso rpd@asl3.liguria.it e per conoscenza alla S.C. Affari Generali: email segreteria.contratticonvenzioni@asl3.liguria.it).

E' rimessa alla discrezione dei Referenti/Dirigenti la possibilità di individuare uno o più facilitatori. Normalmente la scelta dovrebbe ricadere sul personale del comparto, ma è possibile individuare anche figure dirigenziali. In una prima fase, la scelta consigliata per il 2018 è stata di utilizzare le stesse figure individuate quali facilitatori per la trasparenza e la prevenzione della corruzione e/o per l'attività di gestione del rischio clinico, già abituate ad un'attività di *risk management*.

E' importante ribadire che il Facilitatore, occupandosi di dare supporto al Referente di area sulle attività di prevenzione e aiutarlo nell'organizzare, all'interno della struttura-area, le attività di prevenzione, non ha il compito di «fare» tutto il lavoro connesso alla gestione privacy; infatti la relativa responsabilità ricade sempre sui Dirigenti responsabili della struttura-area, che devono elaborare le attività di analisi richieste, coinvolgendo il proprio personale attraverso appositi **gruppi di lavoro.** Il compito dei facilitatori, invece, è quello di facilitare il dialogo interno ed esterno per

fare in modo che le incombenze siano adempiute nei tempi previsti e secondo le modalità e le procedure stabilite.

f) Tutti i Dipendenti

I Dipendenti sono chiamati ad osservare con scrupolo le disposizioni riportate nel presente D.P.S., in particolare:

- osservano le misure contenute nel D.P.S., nella normativa privacy e definite dall'Azienda come idonee a contenere il rischio di violazione;
- qualora trattino dati personali, sono autorizzati al trattamento dal Titolare, attraverso atto scritto, sottoscritto per delega dello stesso, dal Dirigente responsabile della struttura-area cui afferiscono;
- segnalano tempestivamente al proprio Dirigente responsabile di Struttura-area le situazioni di violazione privacy che rilevano , secondo le indicazioni previste dal D.P.S. e dalla normativa vigente in materia e, se ritengono probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati, effettuano **entro e non oltre 24 ore** la segnalazione di *data breach* , come regolamentata dal presente D.P.S. , al proprio Dirigente responsabile di struttura-area, al Referente privacy di riferimento e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali (email segreteria.contratticonvenzioni@asl3.liguria.it);
- danno il proprio contributo al processo della gestione del rischio privacy, con compiti e mansioni assegnate dal proprio Dirigente responsabile di struttura-area, in accordo con il Referente di area, il Titolare ed il R.P.D., attraverso la partecipazione di appositi **gruppi di lavoro** (infatti, senza una fattiva partecipazione del personale nella gestione del rischio, l'attività di prevenzione perde la sua efficacia);
- relazionano il proprio Dirigente in merito a qualsiasi anomalia accertata, indicando per ciascun trattamento, che ha comportato delle criticità, le cause accertate e le azioni tempestivamente intraprese per la minimizzazione delle conseguenze, o le motivazioni, in fatto ed in diritto, che giustificano il ritardo nell'intervento.

Parte Seconda - La gestione del rischio: un nuovo approccio

a) Introduzione

L'evoluzione normativa in materia di trattamento dei dati personali, con la piena operatività del Regolamento Europeo (General Data Protection Regulatione n.679/2016) dal 25 maggio 2018, ha mutato completamente la filosofia di gestione della privacy nell'ambito aziendale. Da un sistema di adempimenti ad obbligazioni di legge e linee guida del Garante della privacy si deve passare ad impostare un vero e proprio sistema di gestione del rischio privacy, con autovalutazione dello stesso ed individuazione delle misure di sicurezza personalizzate aziendali più idonee e di un cronoprogramma di loro implementazione nell'ambito dell'Azienda.

Partendo dalla considerazione che l'annullamento del rischio di violazione privacy, soprattutto in aziende complesse e che trattano categorie di dati particolari quotidianamente come le aziende sanitarie, è impossibile, quello che si mira a definire è un "modello di gestione" di detto rischio.

"The safety management principle is to facilitate everyday work, to anticipate developments and events, and to maintain the adaptive capacity to respond effectively to the inevitable surprises" (Finkel 2011).

Poiché il nostro Sistema sanitario continua a sviluppare ed introdurre maggiore complessità, si rende necessario "adattare" gli approcci alla sicurezza tradizionali ad una realtà in costante cambiamento, focalizzandosi non tanto sull'obiettivo di mantenere il numero di incidenti più basso possibile, misurare il numero di casi in cui è fallito il sistema di gestione della sicurezza ed assumere nell'analisi un approccio reattivo, ma mirando a mantenere il numero dei risultati positivi previsti il più alto possibile, misurare i casi in cui le cose vanno bene ed assumere un approccio proattivo (valutando le azioni che hanno consentito che le cose vadano bene).

Infatti "things that go right and things that go wrong happen in the same way", la base della sicurezza è capire che cosa varia in ogni performance che porta ad un *outcome* positivo per valutare la replicabilità delle azioni – misure ivi adottate nelle performance con *outcome* negativo.

La sicurezza non diventa, quindi, esito dell'applicazione di norme miranti a far corrispondere le prestazioni reali alle idealizzate rappresentazioni delle procedure, ma esito emergente delle diffuse capacità di valutare e prevenire i rischi e di gestire il rischio residuo, non essendovi un rischio azzerabile.

In quest'ottica i Dirigenti aziendali, sulla base dell'esperienza quotidiana di trattamento, hanno analizzato le singole tipologie di trattamento, le misure di sicurezza già operanti ed il loro impatto - nello storico - sulla sicurezza del trattamento stesso, valutando la percentuale di rischio residuo e proponendo eventuali possibili modalità di sua ulteriore gestione (**ALLEGATO 2.1).**

Il D.P.S. diventa così non un documento di studio o di indagine, ma uno strumento per l'individuazione di misure concrete, da realizzare con certezza e da vigilare quanto ad effettiva applicazione e quanto ad efficacia preventiva ed in base ad un principio di precauzione in relazione al rischio specifico.

L'obiettivo è quello di dare avvio ad un processo agile e concreto, la cui essenza non sia costituita dalla mera compilazione di modelli di calcolo, ma da un'analisi interna dei rischi e dei rimedi possibili, mediante la partecipazione allargata dei Dipendenti. A questo fine si è cercato di sollecitare le strutture aziendali a privilegiare la partecipazione interna per far venire fuori le conoscenze acquisite dal proprio personale nel corso degli anni, facendo emergere in modo più efficace i rischi privacy, tralasciando la meccanica applicazione di parametri e formule per il calcolo del rischio.

Pertanto il tentativo è di garantire un alto livello di qualità del processo di analisi e di individuazione di appropriate misure di prevenzione attraverso:

1) un miglioramento nelle comunicazioni tra il R.P.D., i Referenti ed i Dirigenti responsabili delle strutture aziendali, rendendo concreto il ruolo dei Referenti di area quali anelli di congiunzione tra il R.P.D. e le strutture aziendali: i Dirigenti hanno il compito di porre in essere il processo di valutazione, gestione e monitoraggio del rischio all'interno delle proprie strutture, mentre i Referenti coordinano le attività di analisi delle singole strutture, verificando ed assemblando eventualmente i dati da trasmettere al R.P.D.. I Referenti ed i Dirigenti si avvalgono dei "Facilitatori", i cui compiti sono stati illustrati al punto e) – Parte prima;
2) l'utilizzo di un approccio "bottom – up" basato, quindi, sulla partecipazione e sull'ascolto delle esperienze dei dipendenti che concretamente operano nelle varie aree. Tutti i Referenti sono stati invitati a incentivare, all'interno delle strutture delle proprie aree, l'utilizzo di appositi **gruppi di lavoro**, composti da personale non solo amministrativo, ma anche professionale, tecnico e sanitario, per valutare insieme quali siano i trattamenti più soggetti a rischio, individuando rischi e misure non astratte ma fattibili, concrete e programmate. Si vuole evitare che il processo del rischio si riduca ad una mera compilazione di tabelle svolta dal Dirigente o da un amministrativo ma venga inteso come una autoanalisi dei propri trattamenti che coinvolga più persone possibili;
3) l'impiego di ***format comuni*** per la valutazione e gestione del rischio, il suo aggiornamento e monitoraggio, che racchiude tutte le fasi di cui si compone la suddetta analisi. Attraverso questi strumenti si è cercato di ottenere una riduzione dei tempi di trasmissione dei dati velocizzando e semplificando il lavoro alle strutture coinvolte e definendo contestualmente i parametri minimi di un futuro applicativo per la gestione del rischio privacy, nel quale poter riversare facilmente i dati raccolti in questa fase di avvio del "sistema privacy" aziendale;

4) i dati relativi al monitoraggio del trattamento del rischio sono stati impostati per renderli articolati ed analitici, in modo da mettere in evidenza l'importanza di una verifica all'interno di ogni struttura sull'applicazione delle misure dichiarate, individuando l'effettiva incidenza di tali misure per ridurre le cause di rischio;
5) un concreto supporto alle singole strutture ed ai gruppi di lavoro da parte del R.P.D. , della S.C. Affari Generali e Referenti per l'area ospedaliera e territoriale e del sistema informativo, per l'espletamento e la compilazione dei ***format*** relativi alla gestione del rischio, mediante la trasmissione di apposite ***slide informative***, **incontri formativi dedicati** ed ***audit*** con i **gruppi di lavoro** per collaborare allo svolgimento e revisione delle mappature dei trattamenti ed analisi e valutazione dei rischi.

b) Il contesto esterno e interno

Le fasi della gestione del rischio (la mappatura, la valutazione ed il trattamento) sono precedute da una analisi del contesto esterno ed interno al fine di evidenziare la complessità dell'organizzazione e delle attività svolte dall'azienda. L'analisi dell'organizzazione dovrebbe mirare a rafforzare le misure di prevenzione interne all'Amministrazione.

c) Il contesto esterno

L'analisi del contesto esterno prende in esame gli aspetti culturali, criminologici, sociali ed economici del territorio, per determinare se possano agevolare criticità nella gestione privacy all'interno dell'ente.

L'ASL 3 è costituita da 40 comuni, per una superficie totale di circa 1060 Km2, pari a un quinto del territorio della Regione Liguria.

Il territorio è suddiviso in 6 Distretti Socio-Sanitari, dal numero 8 al numero 13 dei 19 Distretti di cui si compone la Regione Liguria – i cui confini coincidono con quelli dei distretti sanitari, definiti ai sensi del D.Lgs. n. 502/92 e s.m.i. e delle Zone Sociali di cui alla Legge Regionale 12/2006 e s.m.i. , così articolati:

DISTRETTO	NUMERO ABITANTI	ESTENSIONE KMQ	DENSITA' ABITATIVA MEDIA/KMQ
n. 8 - PONENTE	94.584	263,1	359,49
n. 9 – MEDIO PONENETE	128.987	25,83	4.994
n. 10 – VAL POLC/VALLESCRIVIA	113.372	346,3	327,4
n. 11 – CENTRO	148.692	13,1	11.350

n. 12 – VALBISAGNO/VALTREBBIA	14.3867	310,1	463
n. 13 – LEVANTE	95.745	97,9	977,9

L'età media è molto elevata (48 anni), in linea con quella ligure ma notevolmente più elevata della media italiana, pari a 43 anni.

Il territorio dell'Azienda confina con le province di Alessandria e Piacenza a nord/nord-est, con il territorio dall'ASL 4 ad est/sud-est, con la provincia di Savona ad ovest ed è delimitato a sud dal Mar Ligure.

Le superfici abitative urbane, sedi di insediamenti industriali ed artigianali e di strutture varie, sono pari a circa il 28 % del territorio, ma si assiste a una concentrazione di oltre il 90% dei residenti nella fascia costiera ed in aree prossime al mare con il conseguente abbandono, continuo e progressivo, delle attività legate al territorio, in particolare quelle agricole, con una rilevante riduzione degli abitanti delle zone interne. Recentemente, tuttavia, si sta verificando un'inversione di tendenza, coerentemente con il trend nazionale.

La popolazione genovese presenta una "criticità di tipo demografico", dovuta all'alto indice di vecchiaia e al basso tasso di natalità. Al contrario, gli indicatori socio-economici presentano in genere valori comparabili o migliori rispetto a quelli nazionali e regionali. All' 1 gennaio 2013 la popolazione residente nella ASL 3, secondo i dati ISTAT integrati con le Anagrafi Comunali, era di 725.247 unità.

Il saldo demografico è variabile negli anni, con una prima inversione di tendenza verso un saldo positivo nel 2014 (dato riferibile alla provincia di Genova, fonte www.geodemo.it).

d) Il contesto interno

L'analisi del contesto interno, prende in considerazione la struttura organizzativa, dei ruoli e delle responsabilità interne; pertanto valuterà i seguenti elementi: gli organi di indirizzo, la struttura organizzativa, i ruoli e le responsabilità. I dati sono tratti dall'Atto Aziendale e dalla Carta dei Servizi.

Compito primario dell'Azienda è quello di assicurare i livelli essenziali uniformi di assistenza definiti nell'ambito del Piano Sanitario Nazionale e Regionale. Tale obiettivo viene perseguito attraverso una rete territoriale a matrice distrettuale.

I Distretti rappresentano l'unità funzionale dell'assistenza sanitaria erogata dall'ASL: il punto di partenza dei percorsi clinici, che possono prevedere o meno - al loro interno - una "tappa" ospedaliera, ma nel territorio debbono concludersi. Fanno parte del territorio di ASL 3 quat-

tro stabilimenti ospedalieri (Villa Scassi a Sampierdarena, Padre Antero Micone a Sestri Ponente, Gallino a Pontedecimo, La Colletta ad Arenzano) integrati tra loro nel Presidio Ospedaliero Unico, in grado di erogare prestazioni specialistiche in regime di ricovero. Il Direttore Generale, nominato dalla Regione, è l'organo di indirizzo, programmazione e governo dell'Azienda. E' il legale rappresentante dell'Azienda ed ha la responsabilità complessiva della stessa. E' responsabile del raggiungimento degli obiettivi indicati dalla Regione nonché della corretta ed economica gestione dell'Azienda.

In particolare, sono riservati al Direttore Generale:

a) la nomina, la sospensione o la decadenza del Direttore Amministrativo, del Direttore Sanitario e del Direttore Sociosanitario;

b) la nomina dei membri del Collegio Sindacale, su designazione delle Amministrazioni competenti;

c) la nomina dei responsabili delle strutture Aziendali ed il conferimento, la sospensione e la revoca degli incarichi dirigenziali, in conformità a quanto stabilito dal D.Lgs. n. 502/1992, dal D.Lgs. n. 165/2001 e ss.mm.ii., dai contratti collettivi di lavoro nel tempo vigenti e dal Regolamento Aziendale;

d) l'adozione dell'atto aziendale, nonché le modificazioni e integrazioni allo stesso;

e) gli atti di bilancio compresa l'adozione del budget;

f) gli atti di programmazione sanitaria locale;

g) le funzioni non delegabili in materia di sicurezza, salute ed igiene sul lavoro.

Altri organi dell'Azienda sono il Collegio Sindacale ed il Collegio di Direzione.

La Pianificazione Strategica è il processo attraverso il quale l'Azienda definisce le finalità dell'organizzazione e le principali linee strategiche nel medio/lungo periodo, partendo dalle indicazioni che provengono dal livello sovraordinato, quindi dalla traccia di riferimento istituzionale dello Stato e della Regione, e dall'ambiente esterno ossia i portatori di interesse.

Il processo di definizione della "meta" a cui tendere, pertanto, si sviluppa analizzando la domanda di bisogno e le aree di intervento, attraverso la selezione degli obiettivi istituzionali individuando le priorità e valutando, in rapporto alle disponibilità economiche, le risorse e i tempi necessari al raggiungimento degli obiettivi stessi.

Il Processo di Programmazione si occupa dell'implementazione delle strategie e del raggiungimento delle finalità assunte in sede di pianificazione strategica attraverso la definizione del

percorso da seguire per raggiungere gli obiettivi partendo dalla gestione corrente e dalla conoscenza del proprio ambiente anche in ordine ai cosiddetti "punti di forza e di debolezza" dell'Azienda.

E' quindi un processo continuo e regolare nel quale si stabiliscono le azioni, le modalità e i mezzi economici ed organizzativi da porre in essere per raggiungere la "meta" definita dalla pianificazione strategica.

Lo strumento operativo del controllo di gestione è il budget, in quanto raccoglie gli obiettivi da perseguire e le risorse da impiegare nell'anno, suddivise per centri di responsabilità; la logica del budget è quella di tradurre i macro obiettivi aziendali in obiettivi specifici delle strutture organizzative aziendali, collegando le risorse ai risultati da conseguire per centro di responsabilità con ampia autonomia organizzativa, sviluppando così la responsabilizzazione economica all'interno dei tipici processi sanitari.

La rilevanza di questo processo deriva dal fatto che pone l'attenzione sui risultati conseguiti e sulle risorse impiegate nei processi aziendali e permette di correlare le responsabilità organizzative ai risultati economici.

La ASL 3 ha optato per un *processo di budgeting* di tipo "bottom up", in cui però la formulazione delle proposte dei centri di responsabilità viene indirizzata dalle linee guida della Direzione Generale.

Particolare attenzione verrà posta nella definizione del Budget distrettuale sociosanitario inteso come il complesso delle risorse disponibili da parte della ASL e dei Comuni, articolato per quota capitaria in analogia a quanto avviene per i riparti nazionale e regionali.

e) La mappatura dei trattamenti: il registro dei trattamenti

La «mappatura dei trattamenti» è l'elenco dei trattamenti di dati personali o categorie particolari di dati personali.

Per la mappatura ci si è basati sui dati richiesti dall'art. 30 del Regolamento (UE) 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e norme attuative, che prevede:

"1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.".

Il processo non è assimilabile al concetto di procedimento amministrativo; malgrado, in alcuni casi esso possa anche coincidere, spesso è più ampio e flessibile.

I dati sono attualmente inseriti per il registro del titolare e per il registro del responsabile nei formati allegati **(ALLEGATI 2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7 e 2.8),** rivisti per garantire un maggior detta-

glio di analisi dei trattamenti e differenziati a seconda del ruolo dell'Azienda di Titolare o Responsabile ex art.28 GDPR, comprensivi di una scheda riportante il registro delle banche dati utilizzate e presentati con una **scheda di accompagnamento** (**ALLEGATO 2.6).**

L'identificazione dei trattamenti avviene, come già ampiamente motivato attraverso **gruppi di lavoro** composti dal personale della struttura.

Copia dei suddetti format è pubblicata, a cura e sotto la responsabilità dei Dirigenti responsabili delle strutture-aree alle quali i trattamenti afferiscono per competenza, sul sito intranet aziendale nella **sezione "Normativa –Privacy"** in specifica sottosezione, e deve essere trasmessa preferibilmente in formato elettronico al R.P.D. (**e mail dedicata** rpd@asl3.liguria.it) ed alla S.C. Affari Generali (**e mail:** segreteria.contratticonvenzioni@asl3.liguria.it) e conservata , per la parte di competenza, presso la struttura dei cui trattamenti si tratta (sotto la responsabilità del Dirigente responsabile della stessa o soggetto dallo stesso individuato come responsabile della conservazione stessa e comunicato al Referente privacy di afferenza , al R.P.D. ed alla S.C. Affari Generali) ed eventualmente presso il Referente privacy di afferenza.

Nella prima fase di mappatura dei trattamenti non è stato possibile procedere all'indicazione nel registro dei trattamenti di tempi specifici di conservazione, per i singoli trattamenti, evincibili, comunque, dalla normativa a supporto della liceità stessa del trattamento o dal regolamento aziendale in materia di gestione documentale e massimario di scarto (adottato con deliberazione n. 405 del 29.6.2016 ed in corso di revisione in modo uniforme nell'ambito del S.S.R.) ed improntati in ogni caso al principio della necessità del trattamento in relazione alle finalità istituzionali perseguite da A.S.L.3. Si potrà avviare un processo di ulteriore revisione e coordinamento delle informazioni contenute nei suddetti documenti sulla base del supporto informatico che verrà fornito per la sua gestione.

Ciascuna struttura- tiene inoltre costantemente aggiornata la documentazione delle nomine a responsabile esterno effettuate o ricevute e degli accordi di contitolarità sottoscritti per delega alla sottoscrizione del Titolare, a cura e sotto la responsabilità del Dirigente responsabile della struttura-area alla quale i relativi trattamenti afferiscono per competenza tecnico –economico-gestionale. I format sono stati revisionati anche per garantirne l'uniformità –ove possibile- a livello di S.S.R- **(ALLEGATI 9, 9.1, 9.2, 9.3 e 10).**

Il Dirigente responsabile della struttura-area compente in riferimento agli aspetti tecnico-economico-gestionali presupposto delle suddette nomine e/o accordi provvede, inoltre, attraverso audit periodici, anche correlati ad altre attività di ispezione e controllo quali-quantitativo nell'ambito dell'esecuzione del rapporto, alla verifica del rispetto delle previsioni in materia di privacy, tenendo traccia documentale degli stessi **e relazionando il R.P.D. e la S.C. Affari Generali in merito ad eventuali criticità rilevate.**

f) La valutazione del rischio: identificazione, analisi e ponderazione

La seconda fase della gestione è denominata **«valutazione del rischio»**. Consente di «acquisire un elevato numero di informazioni sulla vulnerabilità e permeabilità dell'Amministrazione ai componenti di violazione privacy, sul modo in cui tali violazioni potrebbero emergere e diffondersi all'interno dell'Amministrazione e sulle priorità delle misure di prevenzione da adottare».

La valutazione del rischio si articola nelle seguenti Sub -fasi:

- Identificazione del rischio: "ha l'obiettivo di individuare gli eventi di violazione che possono verificarsi in relazione ai trattamenti od alle fasi dei trattamenti".

  Gli strumenti utili per l'identificazione del rischio sono:

  - lista esemplificativa di possibili rischi , come riportata nello specifico "format " (**ALLEGATO 2.2**).
  - confronto tra soggetti coinvolti e i Dirigenti responsabili delle strutture (**gruppi di lavoro**);
  - dati tratti da precedenti giudiziari;
  - le risultanze dell'analisi della mappatura dei trattamenti;
  - segnalazioni.

I rischi devono essere inseriti nel format (**ALLEGATO 2.2**) della gestione del rischio "Analisi e valutazione dei rischi potenziali e relative misure di sicurezza" (e nel format **ALLEGATO 2.1** del suo monitoraggio "Monitoraggio rischi potenziali").

L'identificazione dei rischi deve essere ragionata; non si configura come adempimento ma come analisi che si realizza attraverso l'utilizzo di appositi **gruppi di lavoro** interni. Infatti è imprescindibile un forte coinvolgimento dell'intera struttura dell'ente in tutte le fasi di predisposizione e di attuazione delle misure privacy. Ad ogni rischio sono collegate le misure di prevenzione ad esso associate.

- Analisi: consiste nel calcolare il livello di rischio in termini di **probabilità**, del suo effettivo verificarsi, e di **impatto** sull'ente. Analizzare il rischio significa, assegnare un valore che pesa il rischio. In fase di avvio è stato deciso di eliminare il calcolo numerico legato a parametri predeterminati, troppo formale ed utilizzare una valutazione percentuale del rischio stimato al netto delle misure di sicurezza adottate sulla base delle valutazioni della struttura.

- Ponderazione del rischio: "consiste nel considerare il rischio alla luce dell'analisi e nel raffrontarlo con altri rischi al fine di decidere le priorità e l'urgenza del trattamento".

La ponderazione ha lo scopo di stabilire le priorità di trattamento dei rischi, attraverso il loro confronto. La ponderazione del rischio può anche portare alla decisione di non sottoporre alla fase del trattamento il rischio, trattamenti non giudicati particolarmente rischiosi, limitandosi a mantenere attive le misure già esistenti, pur adottando il criterio della «prudenza».

Nel corso del 2018 e 2019 la ponderazione ha portato a mantenere le misure di sicurezza in essere per i trattamenti mappati, programmando per le annualità successive, una rivalutazione del rischio ed una riponderazione dello stesso alla luce dei primi monitoraggi che sono stati effettuati a decorrere dal 2020, delle proposte di nuove misure di sicurezza raccolte e delle eventuali nuove modalità di valutazione supportate dall'applicativo informatico deputato alla gestione del "sistema privacy" aziendale che dovrà essere acquisito.

L'analisi dei rischi è un momento fondamentale di crescita per il sistema privacy aziendale e non un semplice adempimento, pertanto già in fase di avvio ASL 3 ha dato indicazioni per una sua conduzione attraverso gruppi di lavoro interni alle singole strutture-aree aziendali interessate.

In una prima fase è stata preferita l'adozione di un modello semplificato di analisi, che già, peraltro, rispettasse le indicazioni sopra riportate.

Sono perciò state individuare tre aree di rischio e per ognuna alcune tipologie di rischio, lasciando un campo "altro" implementabile dal compilatore e richiesta la valutazione dell'impatto graduata su 3 livelli (BASSO, MEDIO, ALTO).

Per ognuno degli item di rischio è stata richiesta l'individuazione di misure di sicurezza informatica o non informatica coerenti ed una valutazione del grado di incidenza sul rischio individuato e della responsabilità di attuazione.

Nel 2019 l'analisi effettuata è stata sottoposta a verifica e monitoraggio e richiesta la formulazione di eventuali proposte migliorative, con indicazione dei tempi di attuazione e l'evidenziazione di criticità riscontrate.

L'analisi effettuata è entrata a far parte integrante del registro dei trattamenti aziendale di cui all'art.30 par.2 del RGPD.

Inoltre è stata richiesta alle strutture aziendali una autovalutazione di check sul livello di *compliance* col sistema privacy aziendale.

AREA DI RISCHIO	TIPOLOGIA DI RISCHIO
COMPORTAMENTI DEGLI OPERATORI	SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE
	CARENZA DI FORMAZIONE, DISATTENZIONE, INCURIA
	COMPORTAMENTI SLEALI O FRAUDOLENTI
	ERRORE MATERIALE
	ALTRO (SPECIFICARE)
EVENTI RELATIVI AGLI STRUMENTI	AZIONE DI VIRUS INFORMATICI O PROGRAMMI IN GRADO DI VIOLARE IN SISTEMA
	SPAMMING O TENCICHE DI SABOTAGGIO
	MALFUNZIONAMENTO, OBSOLESCENZA OD INDISPONIBILITA' DEGLI STRUMENTI
	ACCESSI ESTERNI NON AUTORIZZATI
	INTERCETTAZIONI DI INFORMAZIONI IN RETE
	ALTRO (SPECIFICARE)
ALTRI EVENTI	ACCESSI NON AUTORIZZATI AD AREE AD ACCESSO RISTRETTO
	ASPORTAZIONE - FURTO DI STRUMENTI CONTENETI DATI
	DISTRUZIONE CONSEGUENTE AD EVENTI NATURALI OD ARTIFICIALI (DOLOSI, ACCIDENZIALI O DOVUTI AD INCURIA)
	GUASTO AI SISTEMI DI SUPPORTO (IMPIANTI ELETTRICI, CLIMATIZZAZIONE, ETC.)
	ERRORI UMANI NELLA GESTIONE OPERATIVA DELLA SICUREZZA
	ALTRO (SPECIFICARE)

E’ stata inoltre effettuata in tal modo una prima sintesi delle valutazioni dei rischi mappati e delle relative misure di sicurezza adottate:

EVENTO	GRAVITA' STIMATA	CONTROMISURE
Furto credenziali autenticazione	BASSA	Disposizioni sulla custodia e segretezza delle credenziali
Carenza di formazione, disattenzione, incuria o errore materiale degli autorizzati	BASSA	Formazione, internal auditing ed Istruzioni agli autorizzati circa l'attenzione da porre durante un trattamento
Comportamenti sleali o fraudolenti	BASSA	Informazione e formazione agli autorizzati al trattamento sulle responsabilità penali, civili e disciplinari ed internal auditing
Azioni di virus informatici o programmi in grado di violare il sistema informativo aziendale	MEDIA	Il sistemi server sono protetti da antivirus aggiornati quotidianamente. I personal computer connessi alla Rete Aziendale e facenti parte del dominio ASL 3 sono protetti da antivirus centralizzato aggiornato quotidianamente. I rimanenti pc acquisiscono l'aggiornamento dell'antivirus a richiesta dell'utente, attraverso il servizio di assistenza, e, comunque, almeno ogni tre mesi.
Spamming o altre tecniche di sabotaggio	BASSA	Utilizzo regolamentato dell'uso di Internet e della posta elettronica. Implementazione su server aziendali di programma antispam, che blocca la ricezione di e-mail indesiderate.
Malfunzionamento o degrado degli strumenti elettronici	BASSA	Aggiornamento programmato del parco macchine e installazione di patch per le applicazioni

		da parte del servizio di assistenza
Accessi esterni non autorizzati agli strumenti elettronici	BASSA	La Rete Aziendale si configura come una rete privata e l'accesso avviene attraverso credenziali di autenticazione personali.
Accessi non autorizzati a locali o reparti ad accesso ristretto	BASSA	Disposizioni sulle procedure di accesso e dispositivi di sicurezza fisici
Asportazione e furto di strumenti contenenti dati	BASSA	Dispositivi di sicurezza fisica e sorveglianza
Eventi distruttivi, naturali o artificiali, dolosi, accidentali	BASSA	Adozione sistema antincendio e sorveglianza
Guasti ai sistemi complementari	BASSA	Gruppi di continuità e gruppo elettrogeno per il CED
Errori umani nella gestione operativa della sicurezza	BASSA	copie di back up – formazione dipendenti - policy aziendali

Alla quale si è aggiunto il documento redatto secondo lo schema stabilito dalla circolare AGID 2/2017 del 18/04/2017 "Misure Minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del presidente del Consiglio dei Ministri 1 Agosto 2015), con le specifiche misure di sicurezza evidenziate nel DPS aziendale (**ALLEGATO M).**

3. Il trattamento del rischio

E' questa la fase del processo nella quale sono individuate le misure specifiche di prevenzioni per ridurre i rischi (descritti nella fase precedente). Si tratta di predisporre i correttivi, le contromisure più idonee a prevenirli.

Si divide in due fasi: l'identificazione e la programmazione delle misure.

Identificazione delle misure

Per evitare che tutto il processo non si riduca ad un mero adempimento le misure individuate in questa fase devono essere concrete; devono essere individuate avendo a mente la situazione e il contesto in cui si opera, le risorse a disposizione e la propria struttura organizzativa. A seguito dell'analisi dei **gruppi di lavoro** le misure identificate sono state inserite nel format **ALLEGATO 2.2** e nel format **ALLEGATO 2.1**. Ogni misura è collegata al rischio che si vuole ridurre. A seconda delle caratteristiche del trattamento è possibile individuare una sola misura ovvero più misure per ogni singolo rischio.

Programmazione delle misure

Per fare in modo che le misure individuate come da attuarsi siano davvero concrete ed efficaci, traducibili in azioni precise e fattibili, devono essere adeguatamente programmate, indicando lo stato, i tempi e le fasi di attuazione delle misure (da inserire nel "format (**ALLEGATO 2.2**).

Copie dei suddetti format devono essere pubblicate sul **sito intranet aziendale nella sezione "Normativa –Privacy**" in specifica sottosezione, essere trasmesse preferibilmente in formato elettronico al R.P.D. **(e mail dedicata** rpd@asl3.liguria.it) ed alla S.C. Affari Generali (**e mail:** segreteria.contratticonvenzioni@asl3.liguria.it) e conservate , per la parte di competenza, presso la struttura dei cui trattamenti si tratta (sotto la responsabilità del Dirigente-responsabile della stessa o soggetto dallo stesso individuato come responsabile della conservazione stessa e comunicato al Referente privacy di afferenza, al R.P.D. ed alla S.C. Affari Generali) ed eventualmente presso il Referente privacy di afferenza.

Evoluzione prevista per le prossime revisioni

Acquisita dagli operatori la familiarità con lo strumento di valutazione e con il lavoro di gruppo, in sinergia con il SIA, e di internal auditing , al fine di oggettivare ulteriormente la valutazione effettuata, una volta che si concluderà la fase di preventiva revisione di dettaglio dei trattamenti delle singole strutture-aree, laddove ancora raggruppati in macro categorie, secondo un format di analisi predefinito, il passo successivo aziendale sarà quello di richiedere una rivalutazione del rischio sulla base del format di questionario per aree di attenzione.

Le fasi che si prevede di attuare come futura implementazione del sistema sono, quindi, nuovamente:

1. Definizione dell'operazione di trattamento e del suo contesto, con applicazione del format scheda di analisi di dettaglio **(format ALLEGATO 2.3)**

2. Comprensione e valutazione dell'impatto, utilizzando una scala di valori a tre livelli (**BASSO, MEDIO, ALTO/MOLTO ALTO**).

Solo dopo il completamento dell'analisi si potrà procedere in azienda ad una rivalutazione del rischio seguendo una metodologia ispirata alle linee guida dell'ENISA (Agenzia Europea per la

sicurezza delle reti e delle informazioni) tradotte in italiano nel dicembre 2017, che propongono un approccio alla valutazione del rischio, che si basa su quattro fasi:

-. Definizione dell'operazione di trattamento e del suo contesto.

- Comprensione e valutazione dell'impatto, utilizzando una scala di valori a tre livelli (**BASSO, MEDIO, ALTO**).

- Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia) mediante un questionario di 20 domande suddiviso in 4 aree rilevanti, che esita in un risultato graduato su una scala di valori a 3 livelli **(BASSO, MEDIO, ALTO**).

- Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto, in una griglia 3x3, che esita in un risultato graduato su una scala di valori a tre livelli (**BASSO, MEDIO, ALTO)**.

Le misure di sicurezza tecnico-organizzativa vengono poi individuate in coerenza con il livello di rischio così definito e tenendo conto delle indicazioni della norma ISO 27001:2013 sulla sicurezza delle informazioni (ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements :http://www.iso.org/iso/catalogue_detail?csnumber=54534).

I parametri sono quelli indicati dall'art.32 del RGPD: riservatezza del dato, disponibilità del dato, integrità del dato.

La valutazione d'impatto è un processo qualitativo e il Titolare del trattamento deve considerare una serie di fattori quali la tipologia di dati personali, la criticità dell'operazione di trattamento, il volume dei dati personali, le caratteristiche speciali del Titolare del trattamento, come anche le speciali categorie di interessati.

La valutazione ovviamente non può che essere effettuata a priori, prendendo in considerazione un evento ipotetico in cui vengano a mancare i suddetti parametri.

Il livello di impatto sarà, pertanto, valutato:

basso: quando gli interessati possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, maggior tempo di compilazione, fastidi, irritazioni, ecc.).

medio: quando gli interessati possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).

alto/molto alto: quando gli interessati possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà,

perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.)/ quando gli interessati possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).
Detta valutazione di impatto dovrà essere effettuata per ognuno dei tre parametri: riservatezza del dato, disponibilità del dato, integrità del dato.
Dopo questa valutazione, saranno ottenuti tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità). Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali. Se manca un parametro, si prende come livello di impatto quello più alto dei tre livelli. Un set domande supporta la valutazione.

3. Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia) mediante un questionario di 20 domande suddiviso in 4 aree rilevanti, che esita in un risultato graduato su una scala di valori a 3 livelli (**BASSO, MEDIO, ALTO**).

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

- ✓ Basso: è improbabile che la minaccia si materializzi.
- ✓ Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- ✓ Alto/Molto Alto: la minaccia potrebbe materializzarsi.

In questa fase, lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia).
Un set domande supporta la valutazione in relazione all'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce).
In tale prospettiva, le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

- Risorse di rete e tecniche (hardware e software)
- Processi / procedure relativi all'operazione di trattamento dei dati
- Diverse parti e persone coinvolte nell'operazione di trattamento
- Settore di operatività e scala del trattamento

Si dovrà valutare il livello di probabilità di occorrenza di ogni singola minaccia.

4. Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto, in una matrice 3x3, che esita in un risultato graduato su una scala di valori a tre livelli (**BASSO, MEDIO, ALTO**).

Le misure di sicurezza tecnico-organizzativa vengono poi individuate in coerenza con il livello di rischio così definito e tenendo conto delle indicazioni della norma ISO 27001:2013 sulla sicurezza delle informazioni (ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=54534).

Le linee guida ENISA (Tab. A allegata al Manuale sulla sicurezza nel trattamento dei dati personali) considerano due ampie categorie di misure (organizzative e tecniche), ulteriormente suddivise in sottocategorie specifiche codificate. In ogni sottocategoria vengono presentate le misure per livello di rischio (basso: verde, medio: giallo, alto: rosso). Al fine di ottenere la scalabilità, si assume che tutte le misure descritte nel livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, misure presentate nel livello medio (giallo) sono applicabili anche ad alto livello di rischio. Misure presentate nel livello alto (rosso) non sono applicabili a qualsiasi altro livello di rischio.

Ovviamente il valutatore potrà effettuare tutte le integrazioni ritenute, anche in relazione a specifici obblighi normativi connessi allo specifico trattamento.

Il tutto come da **POLICY AZIENDALE PER L'ANALISI DEI RISCHI A CUI SONO SOGGETTI I DATI (ALLEGATO 2).**

Parte terza – Flussi informativi

a) Organizzazione dei flussi informativi: la pubblicazione informatizzata dei dati sul sito intranet aziendale

L'attività di pubblicazione è affidata a ciascun Dirigente responsabile di struttura complessa o S.S.D. o struttura assimilata del "Sistema privacy" aziendale, per i dati di rispettiva competenza, con il supporto dei Facilitatori di struttura e del Referente individuati e con costante informazione del Referente privacy di afferenza, del R.P.D. e della S.C. Affari Generali.

L'informatizzazione del flusso dei dati è garantita dall'utilizzo dell'applicazione web denominata "Redmine", che si basa su di un sistema di apertura di richieste informatizzato in modo da consentire automaticamente la loro tracciabilità. In questo modo l'ufficio che ha inviato la richiesta è in grado, in ogni momento, di conoscerne lo stato di avanzamento, con la certezza che la pratica verrà correttamente evasa.

A seguito di una richiesta di pubblicazione di dati soggetti a pubblicità l'Ufficio Stampa, Comunicazione e URP si impegna a pubblicare i file, senza alterarne i contenuti, la grafica e senza modificarne l'estensione, nella sezione del sito intranet aziendale denominata "Normativa-Privacy", inserendoli nella corretta sotto sezione così come precisata dal richiedente.

La tempistica di conclusione della richiesta varia a seconda dei seguenti fattori:

- la chiarezza nell'esposizione del problema da parte dell'utente;

- l'urgenza e della complessità dell'intervento: se la richiesta riguarda il semplice aggiornamento dei dati essa è evasa nell'arco di poche ore; viceversa se riguarda ad esempio, una modifica strutturale di una sezione della sezione del sito intranet, i tempi vengono preventivamente stabiliti dai tecnici, informando l'interessato;
- le priorità dell'intervento (nel caso, ad esempio, sia obbligatorio per legge la pubblicazione di un certo dato entro un determinato periodo di tempo, viene assegnata la precedenza a questo intervento).

b) Disposizioni organizzative per assicurare la regolarità dei flussi informativi

I Dirigenti hanno individuato un Facilitatore con lo scopo di sgravarli delle attività meramente operative riguardo ai flussi, per velocizzare gli scambi di informazione tra Referenti e R.P.D. ed aiutare i Referenti.

Ciascun Dirigente si farà carico altresì di ottemperare al generale divieto di diffusione dei dati idonei a rilevare lo stato di salute dei singoli interessati. Per i beneficiari di provvidenze di natura economica, occorre che non siano diffusi ulteriori dati non pertinenti quali l'indirizzo di abitazione, il codice fiscale, le coordinate bancarie. A questo proposito si rinvia ai principi di non eccedenza e pertinenza del trattamento ed alle particolari prescrizioni sulla protezione dei dati personali.

Il presente D.P.S. recepisce, anche per il ***sito intranet***, nella misura in cui sono applicabili, le disposizioni del D.Lgs. n.82/2005 art. 68 e ss.sm.ii. (Codice dell'amministrazione digitale) sulle caratteristiche dei dati informatici da pubblicare in formato aperto, in coerenza con le "Linee Guida Siti Web" pubblicate sul sito del DFP alla pagina http://www.funzionepubblica.gov.it/lazione-del-ministro/linee-guida-siti-web-pa.aspx. I file in formato aperto sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità. A questo riguardo, il presente programma fa proprie le indicazioni presenti per la trasparenza sulle linee guida dell'ex CIVIT di cui alla Del. n. 105/2010, le quali, tra l'altro prevedono che i dati dovranno essere possibilmente:

- pubblicati in almeno uno dei formati aperti: pdf (non immagine), odf, xml ecc…
- raggiungibili direttamente dalla pagina dove le informazioni di riferimento sono riportate.

c) Performance e R.P.D.

Il collegamento fondamentale tra R.P.D. e il ciclo della Performance si realizza pienamente prevedendo l'inserimento nel piano della Performance di obiettivi strategici relativi alla prevenzione del rischio privacy.

L'Azienda ha individuato tra gli obiettivi strategici proprio la realizzazione di un effettivo collegamento tra il ciclo di gestione della performance e il D.P.S. prevedendo specifici obiettivi organizzativi riguardo alle attività di prevenzione del rischio privacy anche ai fini del raggiungimento degli obiettivi strategici previsti nel presente D.P.S..

Gli stessi Dirigenti, a capo delle strutture coinvolte negli obiettivi, così come definiti nel processo di budget, sono stati chiamati, a loro volta, ad individuare eventuali **obiettivi individuali**, nell'ambito della scheda di valutazione prevista, da assegnare ai propri collaboratori, coinvolti nelle attività della prevenzione del rischio privacy o con incarichi specifici ("Facilitatori"). Nelle schede di budget sono peraltro già previsti **obiettivi specifici** per il personale del comparto.

Gli obiettivi sono stati diversificati a seconda delle caratteristiche delle varie Strutture. E' possibile classificarli per "macro-obiettivi" in modo da delineare le caratteristiche comuni e da evidenziare anche la connessione tra questi e gli obiettivi strategici stabiliti dal Direttore Generale.

La S.C. P.P.C. effettua un *check* di norma con cadenza annuale per la valutazione dell'implementazione degli obiettivi assegnati alle strutture in materia di privacy e fornisce le relative risultanze al R.P.D. per la valutazione di eventuali azioni correttive.

Analoghi *check* verranno effettuati dai Dirigenti responsabili delle singole strutture-aree, anche a supporto dei relativi Referenti di area di afferenza, con cadenza almeno semestrale.

Il raggiungimento o meno degli specifici obiettivi di budget sarà indicato all'interno della Relazione della Performance; quindi a consuntivo l'Amministrazione dovrà verificare i risultati organizzativi raggiunti rispetto all'obiettivo programmato con rilevazione degli eventuali scostamenti.

Parte Quarta - Le misure di sicurezza

a) *Formazione in tema di privacy*

L'attività formativa nel 2018 e 2019 si è divisa in lezioni in aula, in incontri formativi ed *audit* e in corsi da frequentare a distanza, come illustrato nel presente D.P.S. a cui si rinvia.

Attività formativa anni 2018 -2019 – 2020 - 2021

Si è data continuità nel 2018, 2019, 2020 e 2021 all'attività formativa svolta negli anni precedenti, anche attraverso la continuazione dell'attività formativa a distanza (corsi FAD), di incontri mirati a singoli Dipartimenti/Strutture, con il coinvolgimento dei gruppi di lavoro e di incontri formativi sul Codice di Comportamento aziendale curati dai singoli Dirigenti di struttura-area.

a) <u>Corsi FAD</u>

- Corso privacy generale

  L'attività di formazione è stata rivolta a tutti i Dipendenti (di ruolo e neo assunti). Ma, in particolare è stata rivolta ai dipendenti che ricoprono un ruolo attivo nella identificazione dei rischi e nella definizione e implementazione delle misure di prevenzione (Referenti, Dirigenti responsabili di struttura-area, Facilitatori).

  Il corso FAD è stato elaborato tenendo presenti le numerose novità normative intervenute a cominciare dal Regolamento UE 679/2016. Inoltre, si è tenuto conto della modifiche organizzative che hanno riguardato le responsabilità ed i poteri dei soggetti interni e le loro relazioni con il R.P.D. e l'analisi dei rischi dei trattamenti nell'ambito sanitario, nonché in generale il nuovo "Sistema privacy" avviato.

  Il corso è stato articolato in un unico modulo diviso nei seguenti capitoli:

  1. Il Regolamento Europeo: disposizioni generali
  2. Il Regolamento Europeo: principi applicabili
  3. Il Regolamento Europeo: l'informativa
  4. Il Regolamento Europeo: condizioni del consenso
  5. Il Regolamento Europeo: il principio di responsabilizzazione
  6. Il Regolamento Europeo: la privacy by design
  7. Il Regolamento Europeo: la privacy by default
  8. Soggetti del trattamento dati ante Regolamento Europeo
  9. Soggetti del trattamento dati nel Regolamento Europeo
  10. Il Titolare del trattamento: principali obblighi
  11. Il responsabile del trattamento

12. Il responsabile del trattamento: elementi del contratto col titolare
13. Il responsabile per la protezione dei dati personali (R.P.D.)
14. Sicurezza dei dati personali
15. Notificazione delle violazioni di dati personali (data breach)
16. Valutazione di impatto sulla protezione dei dati
17. Consultazione preventiva
18. Il registro dei trattamenti
19. Il Regolamento Europeo: i diritti degli interessati
20. Le norme nazionali attuative
21. Il progetto aziendale.

Il corso ha l'obiettivo di informare i dipendenti di ASL 3 sul sistema delle politiche, dei programmi e degli strumenti utilizzati per affrontare il complesso tema della privacy all'interno dell'Azienda.

Il corso FAD è stato aggiornato a seguito dell'entrata in vigore delle norme di armonizzazione al Regolamento Europeo e dei chiarimenti del Garante Italiano e messo a disposizione del S.S.R. ligure.

- Corso sul Fasciolo Sanitario elettronico e sul Dossier Sanitario

  Il corso è stato reso obbligatorio per quei dipendenti che utilizzano detti strumenti, scelti dai singoli Dirigenti.

  Il corso si divide in due moduli: il primo a carattere generale coincide con il modulo del corso generale; il secondo riguarda un approfondimento dei rischi e delle misure di prevenzioni specifiche da adottare nell'ambito dell'area.

Dipendenti coinvolti

I corsi sono obbligatori per tutti i Dipendenti, identificati dai propri Dirigenti e per Referenti e facilitatori. Ovviamente nel 2018 la priorità di aggiornamento formativo è stato in capo ai Direttori-Dirigenti responsabili di struttura-area ed ai relativi Facilitatori.

Il monitoraggio della frequenza è effettuato con cadenza annuale dalla S.C. Aggiornamento e Formazione, sulla base delle indicazioni dei Dirigenti delle strutture-aree aziendali.

Detta attività formativa è stata inserita quale obiettivo di budget alle singole strutture aziendali già nel 2018, per cui a decorrere dal 2019 si è monitorato il numero dei destinatari e il numero dei dipendenti che lo hanno effettivamente concluso in ciascuna annualità.

b) Incontri mirati a singoli Dipartimenti/Strutture con il coinvolgimento dei gruppi di lavoro

Si sono tenuti incontri con il coordinamento della S.C. Affari Generali e del R.P.D., con tutti i Referenti privacy, a presentazione e supporto al progetto a decorrere dal primo semestre del 2018.

c) Formazione interna alle strutture/aree - Incontri di divulgazione del progetto aziendale e delle norme in materia di privacy, attività di *internal auditing*

E' stato suggerito ai Dirigenti responsabili di struttura-area di tenere **incontri almeno annuali di divulgazione ed approfondimento** ed **audit interni** sul progetto privacy e sulla normativa relativa, da organizzarsi a decorrere dal 2019.

Nello specifico i Dirigenti hanno il compito di accertarsi almeno annualmente della conoscenza dei propri dipendenti attraverso incontri formativi/illustrativi e di predisporre un **verbale sottoscritto** dai partecipanti, **da inviarsi al Referente di area ed al R.P.D. e per conoscenza alla S.C. Affari Generali**. Detta attività è stata oggetto di specifici obiettivi di budget e prevede la partecipazione obbligatoria di Dirigenti responsabili della struttura e facilitatori della struttura e di dipendenti dagli stessi individuati ed è finalizzata a documentare il grado di autoanalisi portato avanti nelle singole strutture-aree dai dirigenti responsabili, nel rispetto del principio di accountability che permea il nuovo Sistema Privacy aziendale.

b) Codici di Comportamento

I Codici di condotta sono probabilmente gli strumenti più noti «dell'integrity management», volti a tracciare il contesto entro cui i dipendenti sono tenuti a svolgere i loro doveri, arrivando a definire in modo chiaro i comportamenti inaccettabili.

Offrono ai dipendenti alcune regole di comportamento che vanno al di là del rispetto della legge, collocandosi in quelle zone grigie che separano i comportamenti sicuramente leciti da quelli gravemente sanzionati. La legge nel riscrivere l'art. 54 del D.Lgs. n. 165/2001 e s.m.i., chiarisce la natura dei codici quale fonte che individua doveri di comportamento giuridicamente rilevanti, quindi sanzionabili in termini di responsabilità disciplinare, civile, amministrativa e contabile. Inoltre le violazioni grave e rei-

terate del codice comportano l'applicazione del licenziamento. Le norme in essi contenuti «regolano in senso legale ed eticamente corretto il comportamento dei dipendenti e, per tale via, indirizzano l'azione amministrativa».

Con deliberazione n305 del 28.6.2018 questa Azienda ha proceduto ad aggiornare il proprio Codice di Comportamento, mediante procedura aperta; nell'intento di favorire il più ampio coinvolgimento dei vari portatori d'interesse (stakeholder), come richiesto dall'art. 54 c. 5 del D.Lgs. n. 165/2001 e dalla Delibera n. 75/2013 della Autorità Nazionale Anticorruzione recante "*Linee guida in materia di codici di comportamento delle pubbliche amministrazioni*", i cittadini e le varie associazioni che li rappresentano, i sindacati, o altre forme di organizzazioni rappresentative di interessi e/o che fruiscono delle attività e dei servizi prestati da questo ente sono stati invitati a presentare eventuali integrazioni, proposte e/o osservazioni, ai fini dell'aggiornamento del proprio Codice.

Nello stesso tra gli obblighi dei dipendenti vi è ovviamente il rispetto della normativa in materia di privacy e segreto professionale.

Tra gli obiettivi assegnati alle strutture aziendali nell'ambito del ciclo della performance 2018 vi era anche quello di divulgare tra i dipendenti i contenuti del nuovo codice di comportamento aziendale.

Parte Quinta - Monitoraggio a decorrere dal 2019 relativo alla prevenzione del rischio privacy

a) Monitoraggio sul trattamento del rischio

Il processo della gestione del rischio si completa con la successiva azione di monitoraggio.

Nello specifico il monitoraggio mira a verificare l'effettiva attuazione delle misure, la tipologia di misure adottate - specificando se si tratta di una nuova misura o di una misura già esistente - le criticità riscontrate, il grado di incidenza delle misure sulla neutralizzazione dei rischi, allo scopo di comprendere il livello qualitativo di analisi condotto dai vari uffici nell'ambito della gestione del rischio e di identificare le strutture e i processi su cui dovrà essere rivolta una più accurata attività di analisi in futuro.

Nel 2018 è stato realizzato un *format specifico* per il monitoraggio, pubblicato in specifica sottosezione della sezione "Normativa-Privacy" del sito intranet aziendale ed allegato al presente documento (**ALLEGATO 2.1),** nelle more della fornitura di applicativo informatico per la relativa gestione:

Il suddetto format (**ALLEGATO 2.1)** si compone delle seguenti parti:

1) Dati riassuntivi del trattamento
2) Dati relativi alle misure di prevenzione
3) Dichiarazione Dirigente responsabile della struttura

1) Dati riassuntivi del trattamento

I dati di sintesi del trattamento sono: la denominazione e la descrizione del trattamento sottoposto ad analisi, il livello del rischio ed i rischi di violazione privacy individuati. Ogni rischio viene collegato con le misure di prevenzione ad esso associate.

2) Dati relativi alle misure di prevenzione

In questa parte sono precisati i seguenti dati:

- Descrizione della misura con indicazione del rischio che si vuole ridurre, così come risulta dal trattamento del rischio di cui alla Parte Seconda lett. g):
  - MISURA GIA' ADOTTATA - si intende una misura già in esecuzione
  - NUOVA MISURA "PROPOSTA" - si intende una nuova misura, mai applicata
- Grado di incidenza sulle cause di rischio: indicazione in percentuale del grado di incidenza della misura sul rischio.
- Tempi previsti di attuazione: per nuova misura è indicata la data prevista.
- Struttura/Settore/Ufficio Responsabile: sono indicati "Struttura/Settore/Ufficio destinati all'attuazione della misura; diversi Struttura/Settore/Ufficio possono essere responsabili di una o più fasi di adozione delle misure".
- Tempi e modalità di monitoraggio interno: indicazione di eventuali verifiche per accertare che le misure siano state intese e applicate all'interno del trattamento, indicando anche le ragioni del mancato svolgimento.
- Precisazione sull'applicazione delle misure: indicazione per ogni misura di eventuali criticità.

Si precisa che i dati richiesti su questa scheda sono stati impostati con lo scopo, non solo di verificare le attività svolte per l'individuazione dei correttivi più idonei a prevenire i rischi, ma anche di fornire degli spunti per favorire un'analisi più approfondita degli eventi rischiosi esaminati (modifica dei rischi e/o delle misure di prevenzione già inserite nel *format* della gestione del rischio, individuazione di nuove misure più specifiche e concrete ecc.).

3) Dichiarazione Dirigente responsabile della struttura-area

Nell'ultima parte del *format* viene attestato, da parte del Dirigente responsabile della struttura-area competente alla gestione del trattamento a rischio privacy, il

livello di analisi condotto a seguito del monitoraggio del trattamento del rischio e le eventuali conseguenti integrazioni/modifiche delle misure, al fine di renderle concrete e capaci di incidere efficacemente sui rischi.

Per specifiche esigenze di approfondimento sull'analisi del rischio condotta dalle strutture, i singoli *format* compilati saranno pubblicati, unitamente al D.P.S., in specifica sotto sezione nella Sezione "Normativa-Privacy" del sito intranet di A.S.L. 3, per singola struttura.

Per migliorare la qualità di analisi e del conseguente monitoraggio ci si avvarrà del sistema di ***"internal auditing",*** quale strumento non solo di controllo ma anche di supporto alle strutture deficitarie per un innalzamento qualitativo della gestione del rischio.

Nel 2019 è stato attivato il primo monitoraggio dal quale è emersa la sostanziale conferma delle misure di sicurezza già implementate. La situazione emergenziale venutasi a creare in sanità già ad inizio 2020 e continuata anche nel 2021 ha peraltro rallentato l'attività di ulteriore implementazione del monitoraggio.

b) Monitoraggio sul rispetto del D.P.S.

Il monitoraggio complessivo, sull'attuazione delle norme (generali e specifiche), previste dal presente D.P.S., si basa sui singoli monitoraggi compiuti dai Referenti all'interno dei propri Dipartimenti e Strutture Complesse o SSD o strutture assimilabili nel "Sistema privacy" aziendale. E' compito specifico dei Referenti accertare il rispetto e la corretta applicazione delle misure di prevenzione, da parte dei propri Dirigenti di area. Questi ultimi sono chiamati ad una fattiva collaborazione nei confronti del Referente, verificando costantemente il rispetto della privacy da parte dei propri collaboratori. E' indispensabile, perciò che i Referenti creino un contesto organizzativo idoneo per favorire lo scambio di flussi di dati ed informazioni all'interno delle strutture aziendali coinvolte nelle attività di prevenzione del rischio privacy.

Per la verifica sull'assolvimento degli obblighi, la conoscenza, il rispetto e la vigilanza delle misure di prevenzione del rischio, sono stati predisposti nel 2019 dei questionari da compilare e trasmettere da parte dei Referenti Aziendali **(Check list)** contenenti report sui dati 2019.

Si è ritenuto opportuno utilizzare detta check list per avere un rapido sistema di reporting, in fase di prima applicazione del nuovo sistema privacy, per tutti i servizi della A.S.L. 3 al fine di favorire maggiore omogeneità, puntualità e concretezza al processo di analisi e verifica, ed in considerazione della peculiarità e complessità organizzativa di questa

Azienda. Rispetto alla relazione libera, infatti, con questo strumento sono già stati individuati gli argomenti, le materie ed i trattamenti che, in una fase iniziale di implementazione del sistema privacy aziendale, si riteneva più utile sottoporre a controllo. Essi contengono una serie di domande che hanno lo scopo, da un lato, di appurare l'assolvimento degli obblighi, la conoscenza ed il rispetto delle misure di prevenzione introdotte nelle strutture della A.S.L.; dall'altro di comprendere, a grandi linee, l'organizzazione di cui i vari uffici si sono dotati per rendere possibile l'applicazione delle nuove norme in materia di privacy.

Le domande ed i quesiti posti sono serviti anche ad evidenziare le eventuali criticità riscontrate nel corso del tempo. Le risposte, a seconda dei casi, sono a contenuto libero, ovvero predeterminato. E' stata inserita una colonna denominata "Note", in cui era possibile appunto chiarire meglio le risposte. I questionari non devono essere intesi come uno strumento di valutazione, ma come un tentativo di comprendere l'efficacia dei passi fin qui svolti nell'ambito della prevenzione del rischio privacy.

Nel 2019 i questionari hanno riguardato la parte “generale”: il rispetto e la vigilanza degli obblighi contenuti: a) nel D.P.S.; b) nelle ulteriori attività richieste alle strutture come sopra individuate.

I risultati dei questionari hanno consentito al R.P.D. ed al Titolare di possedere uno strumento di valutazione per individuare gli aspetti della normativa attuati secondo quanto richiesto dalle disposizioni dei D.P.S. e gli aspetti critici su cui ancora sarà necessario focalizzare l’attenzione nel futuro.

I dati dei questionari pervenuti a fine 2019 sono stati analizzati e realizzata dal R.P.D. una **tabella aggregata** messa a disposizione del Titolare ed evidenziata la necessità di ulteriormente implementare la necessaria *compliance* soprattutto nelle strutture di area sanitaria, ove maggiori sono le problematiche correlate al trattamento di dati particolari, anche attraverso nuove tecnologie informatiche, con conseguente necessità di favorire ulteriormente il mutamento culturale nel ruolo del dirigente con responsabilità specifiche nell’ambito del Sistema Privacy, indipendentemente dall’area di attività, che in applicazione del principio di “privacy by design”, deve valutare preventivamente l’impatto delle proprie scelte organizzative e gestionali anche in termini di privacy, prima che i trattamenti abbiamo effettivamente inizio, al fine di valutarne la concreta gestibilità a livello di sicurezza del trattamento e di individuare le migliori misure di sicurezza per minimizzare i rischi connessi allo stesso.

Analogamente nell’ambito tecnico-amministrativo diventa fondamentale implementare la *compliance* soprattutto in quelle aree che sovrintendono alle procedure di affidamento di forniture, beni, lavori e servizi, laddove è necessario o l’affidamento di trattamenti a responsabili esterni, la cui affidabilità, anche dal punto di vista privacy, deve essere oggetto di preventiva valutazione e, comunque, in presenza di forniture e/o servizi che implicano trattamenti su larga scala di dati particolari dei pazienti (es. elettromedicali, servizi

informatici, telemedicina), per i quali attraverso la procedura di gara dovrebbe già essere garantita la “privacy by default” del prodotto-servizio oggetto di affidamento, al fine di garantire la minimizzazione dei rischi connessi ai trattamenti correlati.

Ovviamente detti risultati possono essere raggiunti solo attraverso una collaborazione trasversale tra utilizzatori e gestori del trattamento (normalmente di area sanitaria), amministratori di sistema del sistema informativo aziendale e area tecnico-amministrativa deputata agli affidamenti.

Proprio per facilitare detta attività di collaborazione, nel 2019 si è puntato, anche nel sistema di valutazione della performance, sull’avvio dell’attività di *internal auditing* (che andrà a sostituirsi al format di check list sopra citato, lasciando una maggiore flessibilità di analisi ai dirigenti responsabili delle singole strutture-aree) e sulla revisione della parte del registro dei trattamenti deputata alla valutazione del rischio e definizione delle misure di sicurezza, da vedersi quale occasione per familiarizzare con modalità di *auto check* applicate alla privacy.

E già dal 2020 ogni struttura , anche grazie a detto processo di autovalutazione, doveva iniziare a declinare in maggior dettaglio le macro categorie di trattamento allo stato individuate nella propria sezione del registro dei trattamenti, sulla base di specifico **format (ALLEGATO 2.3),** focalizzandosi su ognuna di quelle che per la particolarità del processo di trattamento richiedono uno specifico dettaglio di misure di sicurezza e base giuridica del trattamento, il coinvolgimento di responsabili esterni e/o il trasferimento dei dati, anche per il tramite di responsabili esterni intra od extra UE (es. dati archiviati *in cloud*).

Ovviamente detto tipo di analisi non potrà che essere condotta dalla struttura che concretamente ha la gestione tecnico-professionale-contabile del trattamento e che già, probabilmente, ne controlla gli aspetti qualitativi, quantitativi e professionali, in linea con le indicazioni di letteratura.

Pertanto, ad es. la struttura sanitaria che fruisce di un’attività sanitaria da parte di un soggetto esterno sia esso pubblico o privato, sulla base di un rapporto contrattuale-convenzionale, dovrà registrare il trattamento correlato a detto rapporto nel proprio registro dei trattamenti, analizzandone tutti gli aspetti ivi richiesti, designare ove necessario il soggetto erogatore quale responsabile esterno (e fornirgli le relative istruzioni di trattamento) e/o contitolare, procedere al monitoraggio delle attività svolte dallo stesso affinchè siano rispettose dei principi del sistema privacy aziendale e/o nazionale e/o della UE, documentare dette attività così da poter riscontrare, in persona del dirigente delegato/subdelegato dal Titolare e autorizzato con compiti specifici, ad eventuali richieste di informazioni , gestire eventuali violazioni e/o garantire l’esercizio dei diritti degli interessati.

Proprio per implementare la sensibilizzazione su detti aspetti, compatibilmente con la gestione dell’emergenza sanitaria in corso, che ha impedito di fatto la focalizzazione su dette

problematiche, sono previsti ulteriori incontri formativi mirati e, ad esempio, una focalizzazione nell'ambito del Collegio di Direzione da parte della Direzione Strategica sull'importanza e le ripercussioni della mancata e/o non corretta implementazione del Sistema Privacy aziendale, quale strumento da affiancare agli obiettivi di budget per le prossime annualità per orientare i comportamenti.

Solo, infatti, la prosecuzione del percorso di implementazione della "cultura del dato" può supportare il cambiamento, tenuto conto dell'innegabile peso operativo che la stessa comporta, soprattutto in una fase di avviamento e soprattutto per aree quali quelle sanitarie tradizionalmente formate ad attività professionali di assistenza diretta all'utenza e di gestione di processi assistenziali, con focus sulla salute del paziente, tanto più centrale in momenti di emergenza sanitaria quale quello attualmente vissuto a livello mondiale.

Una fonte di informazioni da non trascurarsi a tal fine, è lo studio dei processi assistenziali e delle loro fasi operative, già avviato per altri ambiti di revisione organizzativa (es. sistema qualità aziendale, certificazione, accreditamento, trasparenza, rischio clinico), che consente di delineare i percorsi assistenziali e, quindi, focalizzare le fasi degli stessi nelle quali intervengono trattamenti dati ed i soggetti interessati dagli stessi, le infrastrutture coinvolte e le misure di sicurezza adottate.

c) L'audit di sistema

Il monitoraggio relativo al rispetto della normativa e del DPS passa anche attraverso il processo di implementazione dell'audit, che riguarda anche l'"*audit di sistema*" attraverso le seguenti fasi:

- ✓ Identificazione del soggetto di coordinamento-responsabile del processo dell'audit (individuato nel RPD).
- ✓ Identificazione di un processo standardizzato per effettuare l'audit basandosi su linee guida specifiche (è stato stabilito di utilizzare le "Linee Guida per audit di sistemi di gestione (UNI EN ISO 19011) come riferimento procedurale per lo svolgimento degli audit; le Linee Guida saranno adattate alla realtà specifica che si dovrà analizzare).
- ✓ Definizione degli obiettivi, ampiezza e criteri dell'audit.
  Gli obiettivi possono riguardare:
  a) determinazione dell'estensione della conformità del sistema di gestione del valutando, o di parti di esso, rispetto ai criteri dell'audit;
  b) valutazione della capacità del sistema di gestione di assicurare la conformità con i requisiti cogenti e contrattuali;
  c) valutazione dell'efficacia del sistema di gestione nel conseguire obiettivi specificati;
  d) identificazione di aree di potenziale miglioramento del sistema di gestione.
  L'ampiezza dell'audit descrive l'estensione ed i limiti dell'audit quali localizzazioni fisiche, unità organizzative, attività e processi-trattamenti da sottoporre ad audit ed il periodo di tempo interessato dall'audit.
  I criteri dell'audit possono comprendere le politiche, le procedure, le norme, le leggi ed i regolamenti, i requisiti del sistema di gestione, i requisiti contrattuali o i codici comportamentali applicabili del settore.

- ✓ Monitoraggi periodici a campione attraverso controlli sul campo, con verifica della documentazione.
- ✓ Identificazione delle strutture da sottoporre a controllo scegliendo eventualmente i trattamenti da esaminare.
- ✓ Contattare i Direttori delle strutture di cui al punto precedente per richiedere la documentazione, le informazioni e i dati indicati sulla tabella della gestione del rischio relativa ai processi soggetti a audit.
- ✓ Analizzare la documentazione relativa ai processi sottoposti a verifica.
- ✓ Valutazione della fattibilità dell'audit sulla base degli elementi raccolti ed eventuale loro integrazione anche tramite verifica preliminare sul campo.
- ✓ Costituzione di un apposito gruppo di lavoro che si deve occupare dell'audit sulla base delle competenze necessarie per conseguire gli obiettivi dell'audit. Il gruppo di lavoro sarà così costituito: il RPD e suoi collaboratori, un facilitatore di altra struttura esperto tecnico per area, un esperto tecnico del SIA. Per i componenti del gruppo di lavoro si applicherà il criterio della rotazione del personale chiamato a fornire il dovuto supporto normativo e tecnico; per cui gli stessi si asterranno durante gli audit che interessano la propria struttura (per assicurare l'indipendenza del gruppo di audit dalle attività da sottoporre ad audit e di evitare conflitto di interesse). I facilitatori quindi potranno essere coinvolti in audit di altre strutture. Durante l'audit dovrà essere presente il responsabile della struttura o suo delegato ed il facilitatore della stessa, ove individuato.
- ✓ Predisporre una check – list sulla qualità della gestione del rischio condotto dalle strutture oggetto di audit anche in base alle indicazioni emerse dalla mappatura privacy sui rischi e sulle misure di prevenzione dei trattamenti analizzati.
- ✓ Concordare con i Responsabili delle Strutture coinvolte il giorno in cui ha luogo la verifica "sul, campo" da parte del gruppo di lavoro, in modo da essere certi che nei giorni stabiliti sia presente il personale che abitualmente attende allo svolgimento del trattamento sottoposto ad esame.
- ✓ Gli operatori appartenenti alle strutture coinvolte nella verifica vengano informati sui compiti specifici che svolgeranno.
- ✓ Conduzione di una verifica sul campo, sulla base della pianificazione effettuata (inerente ad esempio: a) gli obiettivi dell'audit; b) i criteri di audit ed ogni documento di riferimento; c) l'ampiezza, compresa l'identificazione delle unità organizzative e funzionali e dei processi-trattamenti da sottoporre ad audit; d) le date ed i luoghi ove si devono effettuare le attività di audit sul campo; e) la stima del tempo e della durata per le attività di audit sul campo, comprese le riunioni con la direzione del valutando e le riunioni del gruppo di audit; f) i ruoli e le responsabilità dei membri del gruppo di audit e degli eventuali accompagnatori; g) l'assegnazione di appropriate risorse per le aree critiche dell'audit; h) l'identificazione del rappresentante del valutando per l'audit; i) le voci del rapporto di audit (compresi eventuali metodi per classificare le non conformità), il formato, la struttura e la data prevista per la sua emissione e distribuzione; 1) gli aspetti soggetti a vincoli di riservatezza, etc.) coinvolgendo il dirigente responsabile oltre che i dipendenti che si occupano del trattamento e quelli coinvolti nell'applicazione delle misure di prevenzione ed offrendo al valutando l'opportunità di porre domande.
- ✓ Guide ed osservatori possono accompagnare il gruppo di audit, ma non sono parte di esso. Questi non dovrebbero influenzare o interferire con l'esecuzione dell'audit. Ove siano assegnate guide, queste dovrebbero assistere il gruppo di audit ed agire su richiesta

del responsabile del gruppo di audit. I loro compiti possono comprendere: a) stabilire contatti e tempistica per le interviste; b) organizzare visite a parti specifiche del sito o dell'organizzazione; c) assicurare che regole concernenti la sicurezza del luogo e le procedure di security siano conosciute e rispettate dai membri del gruppo di audit. Le guide possono anche assistere all'audit per conto del valutando. Dietro richiesta del responsabile dell'audit, le guide possono fornire chiarimenti o aiutare a raccogliere informazioni corrette.

- ✓ Al termine della verifica viene predisposta idonea verbalizzazione datata e firmata, indicando, le conformità rispetto ai criteri degli audit ed eventuali rilievi sulle non conformità e vengono formulate eventuali raccomandazioni relative a proposte di miglioramento, eventuali futuri audit, richiesta di un piano di azioni correttive, etc..
  Le conclusioni dell'audit possono indicare l'esigenza di azioni correttive, preventive e, se applicabile, di miglioramento. Tali azioni a seguire non sono considerate come facenti parte dell'audit e sono usualmente effettuate dal valutando secondo tempistiche concordate. Il valutando deve tenere informato il responsabile dell'audit dello stato di queste azioni a seguire. Il completamento e l'efficacia delle azioni correttive dovrebbero essere verificati in accordo. Questa verifica può costituire parte di un audit successivo.
  Le non conformità dovrebbero essere riesaminate con l'appropriato rappresentante del valutando. Lo scopo del riesame è di ottenere consapevolezza che l'evidenza dell'audit sia accurata e che le non conformità siano comprese. Dovrebbe essere fatto ogni tentativo per risolvere eventuali divergenze di opinione relative alle evidenze e/o ai rilievi dell'audit; ed i punti non risolti dovrebbero essere registrati.

- ✓ Rapporto sull'audit a cura del gruppo, che contiene, anche con riferimento a documenti allegati: a) gli obiettivi dell'audit; b) l'ampiezza dell'audit, particolarmente l'identificazione delle unità organizzative e funzionali o dei processi sottoposti ad audit ed il periodo di tempo interessato; c) l'identificazione dei membri del gruppo di audit; e) le date e i luoghi dove sono state eseguite le attività di audit sul campo; f) i criteri di audit; g) i rilievi dell'audit; h) le conclusioni dell'audit; i) il piano di audit; j) l'elenco dei rappresentanti del valutando; k) una sintesi del processo di audit comprendente eventuali ostacoli incontrati che possono far diminuire l'affidamento che può essere riposto nelle conclusioni dell'audit; l) la conferma che gli obiettivi dell'audit sono stati raggiunti nell'ambito dell'ampiezza dell'audit in accordo con il piano di audit; m) le aree non coperte, sebbene rientranti nell'ampiezza dell'audit; n) le opinioni divergenti non risolte tra il gruppo di audit ed il valutando; o) le raccomandazioni per il miglioramento, se specificato negli obiettivi dell'audit; p) i piani concordati delle azioni a seguire; q) una dichiarazione del carattere riservato dei contenuti; r) la lista di distribuzione per il rapporto di audit; s) data del rapporto.

Il gruppo di audit ed i responsabili della gestione del programma di audit non devono divulgare i contenuti dei documenti, né eventuali altre informazioni raccolte nel corso dell'audit, o il rapporto stesso, ad eventuali altre parti.

Entro il 31.12.2018 sono stati effettuati n. 11 audit interni. Nel corso del 2019 sono stati condotti n. 2 audit di sistema con la sopra riportata metodologia, uno in area tecnico-amministrativa ed uno in area sanitaria territoriale. Nel corso del 2020, stante anche la emergenza sanitaria tuttora in corso, è stato condotto un unico audit di sistema in area tecnico-amministrativa. Alla data del

presente aggiornamento è in corso un audit di sistema sempre nell'ambito dell'area tecnico amministrativa.

Parte Sesta – Le policy aziendali in materia di privacy

Premesse

Premesso che nell'ambito della propria attività istituzionale l'Azienda Sociosanitaria Ligure n. 3 effettua trattamento di dati personali, come di seguito elencati, con il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza organizzative, fisiche e logiche, previste per la tutela dei dati trattati, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati stessi, di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta.

Si forniscono, pertanto, idonee informazioni e prescrizioni riguardanti:

1. Elenco dei trattamenti dei dati personali:

1.1) Tipologie dei dati trattati

1.2) Aree, locali e strumenti con i quali si effettuano i trattamenti

1.3) Sistema di videosorveglianza

1.4) Mappa dei trattamenti effettuati.

2. Autorizzati ed Amministratori di sistema

2.1) Amministratori di sistema

2.2) Autorizzati al trattamento

2.3) Custode della parola chiave

2.4) Procedure applicative gestite dall'Area Sistema Informativo Aziendale

3. Analisi dei rischi a cui sono soggetti i dati

4. Misure adottate e da adottare atte a garantire l'integrità e la disponibilità dei dati

5. Criteri e modalità di ripristino dei dati a seguito di distruzione o danneggiamento

6. Formazione degli autorizzati al trattamento dati

7. Misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno della struttura

8. Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati inerenti lo stato di salute dagli altri dati personali dell'interessato

9. **Consegna dei referti on line**
10. **Autorizzati al trattamento nell'ambito delle sperimentazioni cliniche**
11. **Raccolta consenso al CUP regionale**
12. **Pubblicazioni provvedimenti sul sito Internet aziendale per finalità di trasparenza e per altre finalità**

12 a) Pubblicazioni per finalità di trasparenza

12 b) Pubblicazioni per altre finalità

13. **Trattamento dei dati tramite dossier sanitario elettronico e FSE**
14. **Aggiornamento periodico del Documento programmatico sulla Sicurezza**

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

1.1 Tipologie dei dati trattati

Gli stessi risultano dal registro dei trattamenti aziendale.
In seguito all'analisi compiuta, anche attraverso specifica richiesta alle singole strutture aziendali, sono stati individuati i seguenti trattamenti:

- Dati relativi al personale Dipendente e/o assimilato, sia di natura personale sia particolari categorie di dati personali, conseguenti al rapporto di lavoro ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali o inerenti l'adesione ad organizzazioni sindacali
- Dati personali relativi ai fornitori e terzi ricavati da albi ed elenchi pubblici o comunicati dagli stessi compresi dati sul patrimonio e sulla situazione economica o necessari ai fini fiscali o afferenti alla reperibilità e alla corrispondenza con gli stessi o all'espletamento delle procedure di gara
- Dati personali degli utenti dagli stessi forniti per l'espletamento dei fini e per l'esercizio delle attività istituzionali attinenti le funzioni del Servizio Sanitario Nazionale
- Categorie particolari di dati personali degli utenti.
- Dati personali e categorie particolari di dati personali di dipendenti ed assimilati, visitatori, informatori scientifici e fornitori, accompagnatori, familiari e utenti inerenti le attività di trattamento derivanti dalle diverse disposizioni inerenti l'emergenza ed il contrasto alla pandemia da coronavirus (Covid 19).

L'Azienda ha altresì preso atto con deliberazione n. 1082 del 17/10/2006 del Regolamento Regionale 16/05/2006 n.1 avente ad oggetto il Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20 e 21 del Decreto Legislativo 30 giugno 2003 n. 196 e ss.mm.ii.

Tale Regolamento è stato successivamente abrogato e sostituito dal Regolamento Regionale 9 aprile 2014 n. 2 "Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20 e 21 del Decreto Legislativo 30 giugno 2003 n. 196 e ss.mm.ii." , che viene allo stato mantenuto e fatto proprio dal Titolare , quale policy aziendale contenente l'elenco di trattamenti, tipologie di dati, finalità di trattamento, riferimenti normativi che legittimano i trattamenti e destinatari di comunicazioni afferenti i dati trattati dall'Azienda, nelle aree di afferenza ed a miglior dettaglio del registro dei trattamenti agli atti in formato elettronico sul sito intranet aziendale sezione "Normativa-Privacy", in quanto compatibile con le disposizioni attuative della normativa europea a livello nazionale e/o regionale.

Il Regolamento, pubblicato nella sezione della Intranet aziendale denominata "Normativa/privacy", è costituito da una serie di schede che identificano le rilevanti finalità di

interesse pubblico, le tipologie di dati oggetto del trattamento e le operazioni su di essi eseguibili, e ognuna di esse è completata da una descrizione del trattamento effettuato.

Le Strutture aziendali interessate sono state chiamate a verificare che le procedure di trattamento in essere e riportate nel registro dei trattamenti siano coerenti con quanto previsto nel Regolamento ed apportando gli eventuali aggiornamenti ed adeguamenti nella sottosezione del registro dei trattamenti di afferenza.

1.2 Aree, locali e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati avviene presso la sede dell'Azienda, e presso le singole strutture dislocate sul territorio di competenza della medesima, presso le sedi della società regionale d'informatica, Liguria Digitale S.p.A. e presso altri soggetti esterni debitamente designati responsabili esterni del trattamento dati dalle strutture competenti per materia in base all'atto di autonomia aziendale.
Presso ogni struttura o ufficio aziendale in cui si effettua il trattamento di dati sono impartite apposite istruzioni affinché il medesimo avvenga in locali accessibili solo al personale autorizzato del trattamento. I locali sono forniti di serratura a chiave.
Il trattamento dei dati avviene sia con strumenti elettronici sia con strumenti non elettronici (supporti cartacei tradizionali).
Per quanto concerne questi ultimi sono raccolti in schedari o fascicoli a loro volta custoditi in armadi o cassetti, anch'essi dotati di serratura.
Gli uffici che alla data del presente aggiornamento sono privi di appositi armadi o cassetti per la custodia dei supporti cartacei contenenti dati personali e categorie di dati particolari, devono comunque essere chiusi a chiave dal personale al termine dell'orario di ufficio.
Il trattamento effettuato con strumenti elettronici prevede l'utilizzo di personal computer non in rete (pc stand alone) ed in rete.

Gli strumenti informatici di cui dispone la Rete Aziendale sono costituiti, attualmente, da:
- N. 3642 Personal computer in rete
- N 65 Server fisici e N. 121 server virtuali
- N. 602 pc portatili
- N. 10 pc non in rete

Con Rete Aziendale s'intende l'insieme delle apparecchiature informatiche (server, pc, hub, switch, router, stampanti) interconnesse su Lan e dotate di un indirizzo IP conforme al piano di indirizzamento interno dell'Azienda.

Informazioni di dettaglio in punto sono rinvenibili sul sito intranet aziendale nella sezione "Normativa-Privacy" nella specifiche sottosezioni dedicate alle banche dati aziendali ed alla valutazione del rischio dei singoli trattamenti.

1.3 Sistema di videosorveglianza

Al fine di garantire il controllo degli accessi e la vigilanza a tutela della sicurezza dei pazienti, dei visitatori e dei lavoratori, la salvaguardia del patrimonio aziendale, degli assistiti, dei lavoratori, dei visitatori e la tutela della salute degli assistiti, viene effettuato un trattamento dei dati anche attraverso un sistema di videosorveglianza. Le immagini laddove registrate vengono conservate per 24 ore dalla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, per un periodo comunque non superiore alle 72 ore, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Decorso il termine il sistema provvede in modo automatico alla cancellazione delle immagini registrate.

Qualora una struttura aziendale intenda installare un sistema di videosorveglianza per una delle finalità sopra indicate deve inoltrare una richiesta al R.P.D., alla S.C. Affari Generali, al Dipartimento Tecnico-Amministrativo-Area Tecnica – S.C. Elettromedicali, Impianti ed Automazioni ed alla S.C. Gestione e Sviluppo Risorse Umane, nella quale si devono indicare:

- le finalità perseguite, specificando le motivazioni che rendono proporzionale l'installazione di telecamere rispetto all'effettivo grado di rischio;
- il numero, la dislocazione e la tipologia delle video-camere;
- se le immagini devono essere solo rilevate od anche registrate
- le eventuali necessità di conservare le immagini per un periodo superiore alle 24 ore, specificandone le speciali esigenze.

Inoltre ogni volta che viene attivato un sistema di videosorveglianza deve essere redatto dalla struttura aziendale presso cui viene installato tale sistema un apposito documento, con il quale vengono documentate le ragioni delle scelte che hanno determinato l'attivazione della videosorveglianza, ed una copia di tale documento deve essere trasmessa alla S.C. Elettromedicali, Impianti ed Automazioni, al R.P.D., alla S.C. Affari Generali, che lo conserveranno ai fini di eventuali esibizioni in occasione di visite ispettive disposte dall'Autorità Garante per la protezione dei dati personali, oppure ai fini di dare riscontro all'esercizio dei diritti dell'interessato o ancora in caso di contenzioso.

L'elenco delle strutture presso cui sono installati sistemi di videosorveglianza è detenuto dall'Area Tecnica del Dipartimento Tecnico-Amministrativo-S.C. Elettromedicali, Impianti ed Automazioni, che ne deve fornire copia aggiornata al R.P.D ed alla S.C. Affari Generali.

Per ogni altra prescrizione in materia si rimanda al regolamento aziendale sulla videosorveglianza approvato con deliberazione n. 640 del 11 novembre 2013, di cui si prevede la revisione per l'adeguamento alla nuova normativa europea e norme di armonizzazione, nonché le policy aziendali in materia, tra le quali da ultimo la circolare ID 66834472 del 29.5.2019 **(allegato Q, R, S)** e al vademecum videosorveglianza del 3/12/2020 del Garante per la Protezione dei Dati Personali **(allegato T);**

In base alle sopra citate policy aziendali, nell'ambito del Dipartimento Tecnico-Amministrativo, alla S.C. Elettromedicali, Impianti e Automazioni sono stati conferiti compiti e responsabilità specifici nel "Sistema privacy aziendale" in relazione ai trattamenti correlati all'utilizzo dei sistemi di videosorveglianza di cui trattasi:

- garantire il rispetto sia in sede di scelta, attivazione e gestione sia in sede di manutenzione degli impianti di videosorveglianza, delle misure di sicurezza indicate dall'Autorità Garante per la protezione dei dati personali nel Provvedimento in materia di videosorveglianza 8.4.2010 e s.m.i. e delle altre misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio correlato all'utilizzazione di sistemi di videosorveglianza, anche con riferimento al rispetto dei tempi di conservazione delle immagini e dei dati correlati , al divieto di controllo a distanza dell'attività lavorativa, ai limiti al controllo di ambienti sanitari e luoghi di cura ed alla necessità di garantire accessi differenziati agli autorizzati alla semplice visione e/o ad operazioni ulteriori, coordinandosi con i dirigenti responsabili delle strutture richiedenti e con la struttura complessa Programmazione e Gestione delle Forniture e/o S.I.A. per gli ambiti di competenza

- coordinare le fasi di installazione, attivazione e manutenzione degli impianti di videosorveglianza, la cui installazione sia stata autorizzata, ai sensi del regolamento aziendale in ASL 3

- tenere l'archivio della documentazione tecnica afferente gli impianti di videosorveglianza installati e/o di nuova installazione, con indicazione delle modalità di ripresa degli stessi

- collocare adeguate informazioni e cartellonistica nelle immediate vicinanze degli impianti di videosorveglianza, secondo la modulistica e cartellonistica in uso, coordinandosi con i dirigenti responsabili delle strutture aziendali (ove gli stessi sono ubicati) e richiedenti la loro installazione (che mantengono il compito specifico e la responsabilità della vigilanza e garanzia che l'uso dei sistemi di videosorveglianza ed il relativo trattamento di dati ed immagini avvenga, per gli ambiti di competenza della struttura da loro diretta, secondo quanto indicato nel regolamento aziendale, nel D.P.S privacy aziendale e nella normativa vigente in materia)

- impartire specifiche istruzioni ad autorizzati e/o responsabili esterni in modo da garantire che, nel caso di interventi manutentivi, i soggetti preposti alle suddette operazioni possano accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza di credenziali di autenticazione abilitanti alla visione delle immagini

- tenere l'elenco aggiornato degli impianti di videosorveglianza presenti in ASL 3, completo di:

1) indicazione delle strutture in cui sono posizionati,

2) numero delle videocamere, se prevedono o meno registrazione delle immagini e del periodo di operatività nell'arco della giornata nonché del tempo di conservazione delle stesse,

3) nominativi aggiornati degli autorizzati a trattare i dati e/o a visionare e/o a far visionare ai soggetti legittimati per legge le immagini degli impianti afferenti alle singole strutture e/o a funzioni ulteriori, individuati dai direttori responsabili delle strutture in cui sono ubicati gli impianti di videosorveglianza stessa, da rendere disponibile a richiesta del Titolare, del RPD, della S.C. Affari Generali e/o dell'Autorità di controllo

- concorrere alla definizione di misure idonee a prevenire il rischio di violazione privacy, alla valutazione del rischio di violazione privacy e monitoraggio del sistema privacy in relazione all'utilizzazione di sistemi di videosorveglianza in ASL 3 ed a controllare il rispetto da parte dei dipendenti (o assimilati) delle suddette misure, coordinandosi con i dirigenti di riferimento per gli ambiti di rispettiva competenza

- fornire le informazioni richieste dal R.P.D. e formulare specifiche proposte volte alla prevenzione del rischio di violazione privacy a seguito dell'individuazione delle attività nell'ambito delle quali è più elevato il rischio medesimo

- collaborare con il DIRIGENTE di riferimento ed il R.P.D. per l'evasione di eventuali richieste di esercizio di diritti, su istanza dell'interessato, ai sensi del Regolamento UE 679/2016 e norme di armonizzazione e/o per l'effettuazione di valutazione di impatto preventiva al trattamento dei dati particolari (quando necessaria) con sistemi di videosorveglianza, da inviare eventualmente al Garante

- In caso di violazione di dati personali con sistemi di videosorveglianza, di cui si sia venuti a conoscenza, segnalare immediatamente, e comunque entro 24 ore, al referente e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali (e mail segreteria.contratticonvenzioni@asl3.liguria.it) qualsiasi violazione privacy in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati, con le modalità previste dal D.P.S. aziendale e dalla normativa vigente

- sottoscrivere ed aggiornare costantemente, sulla base delle deleghe o subdeleghe di sottoscrizione ricevute dal Titolare le designazioni, per iscritto, degli operatori che agiscono sotto la propria direzione, ad autorizzati del trattamento con l'utilizzazione di sistemi di videosorveglianza, secondo livelli differenziati e profili omogenei ed avendo cura di individuare compiti e mansioni cui sono adibiti al fine di formulare correttamente le istruzioni da impartire per trattare i dati
- tenere la documentazione delle designazioni sottoscritte ed aggiornarla, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento dei sottoposti. La documentazione delle designazioni sottoscritte ed aggiornate, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento, deve essere conservata sotto

la responsabilità del Dirigente-responsabile, presso la struttura-area diretta e presso quella di assegnazione dell'autorizzato e, per quanto possibile, correlata dal Dirigente-responsabile stesso al registro dei trattamenti di afferenza della struttura-area, e pubblicato sul sito intranet aziendale nella specifica cartella condivisa (Normativa/Privacy/Registro Trattamenti/Politiche Privacy) nonché messa a disposizione di RPD aziendale e S.C. Affari Generali, su loro richiesta

- custodire gli atti di designazione, il registro dei trattamenti e tutta la documentazione di cui infra, relativa ai sistemi di videosorveglianza installati in ASL 3, in apposito contenitore e/o cartella informatizzata da esibire in caso di verifica interna ovvero di ispezione del Garante

- curare, fra gli autorizzati al trattamento sottoposti alla propria autorità, la diffusione di norme, linee guida e di ogni altra disposizione impartita dall'Azienda anche organizzando la formazione di struttura mirata all'aggiornamento continuo ed obbligatorio in materia di privacy, previsto per legge

- **In caso di designazione di responsabili esterni del trattamento che collaborano ai trattamenti della struttura-area di afferenza (per competenza tecnico-economico – gestionale), secondo le procedure, tempistiche e modalità previste dal D.P.S., e/o di accordi di contitolarità, per conto del Titolare, che all'uopo abbia delegato il direttore della S.C. Elettromedicali, Impianti e Automazioni alla sottoscrizione stessa, fornire a detti responsabili esterni/contitolari le necessarie istruzioni** circa la corretta gestione e tutela dei dati personali mediante utilizzazione di sistemi di videosorveglianza, anche ai fini della loro integrità e sicurezza, vigilando sull'osservanza delle stesse e della normativa in materia, anche con periodici e sistematici audit e controlli, **ed aggiornando in punto il R.P.D. e la S.C. Affari Generali.**

Tutti i dirigenti responsabili delle strutture aziendali che hanno richiesto ed ottenuto secondo le procedure aziendali ed ove sono ubicati gli impianti di videosorveglianza mantengono i compiti specifici e le responsabilità della vigilanza e garanzia che l'uso dei sistemi di videosorveglianza ed il relativo trattamento di dati ed immagini avvenga, per gli ambiti di competenza della struttura da loro diretta, secondo quanto indicato nel regolamento aziendale, nel D.P.S privacy aziendale e nella normativa vigente in materia ed, in particolare:

- individuare specificamente gli autorizzati a trattare i dati e/o a visionare e/o a far visionare ai soggetti legittimati per legge le immagini degli impianti afferenti alla struttura da loro diretta, fornendo agli stessi adeguate istruzioni, formazione ed informazioni sugli impianti di videosorveglianza di afferenza e vigilando sul loro rispetto
- sottoscrivere ed aggiornare costantemente, sulla base delle deleghe o subdeleghe di sottoscrizione ricevute dal Titolare le designazioni, per iscritto, degli stessi, secondo la specifica modulistica prevista per detta tipologia di trattamento (pubblicata sul sito intranet aziendale Normativa/Privacy/Moduli -**allegato Modello Q**), secondo livelli differenziati e profili omogenei ed avendo cura di individuare compiti e mansioni cui sono adibiti al fine di formulare correttamente le istruzioni da impartire per trattare i dati. In punto si rammenta che la delicatezza di detto trattamento suggerisce l'opportunità di ridurre al minimo il numero di autorizzati allo stesso (direttore della struttura e/o del Dipartimento e/o dello

Stabilimento e/o del Distretto e/o suo delegato autorizzato formalmente, nella logica del raggruppamento ove possibile per edifici di afferenza)
- custodire gli atti di designazione ed il registro dei trattamenti, in apposito contenitore e/o cartella informatizzata da esibire in caso di verifica interna ovvero di ispezione del Garante
- tenere l'elenco aggiornato di dette designazioni specifiche, da trasmettere alla S.C. Elettromedicali, Impianti e Automazioni e da rendere disponibile, a richiesta, del Titolare, del RPD , della S.C. Affari Generali e/o dell'Autorità di controllo
- coordinarsi con la S.C. Elettromedicali, Impianti e Automazioni affinchè siano collocate adeguate informazioni e cartellonistica nelle immediate vicinanze degli impianti di videosorveglianza, secondo la modulistica e cartellonistica in uso e vigilare sulla loro custodia e manutenzione
- esporre nei locali in cui sono collocati gli impianti di videosorveglianza, in prossimità agli stessi, anche **l'informativa estesa specifica** (pubblicata sul sito intranet aziendale Normativa/Privacy/Modelli e sul sito internet aziendale Siti Tematici/Privacy – **allegato Modello R**) e garantire che adeguate informazioni vengano date agli utenti che le richiedano dal personale presente nella struttura
- tenere documentazione del numero di videocamere di afferenza, loro ubicazione, se prevedono o meno registrazione delle immagini e del periodo di operatività nell'arco della giornata nonché del tempo di conservazione delle stesse immagini e vigilare-monitorare sul loro corretto funzionamento; il tutto da rendere disponibile, a richiesta, del Titolare, del RPD , della S.C. Affari Generali e/o dell'Autorità di controllo
- concorrere alla definizione di misure idonee a prevenire il rischio di violazione privacy, alla valutazione del rischio di violazione privacy e monitoraggio del sistema privacy in relazione all'utilizzazione di sistemi di videosorveglianza per l'area di afferenza ed a controllare il rispetto da parte dei dipendenti (o assimilati) delle suddette misure, coordinandosi con la S.C. Elettromedicali, Impianti e Automazioni e/o la S.C. SIA , per gli ambiti di rispettiva competenza

- fornire le informazioni richieste dal R.P.D. e formulare specifiche proposte volte alla prevenzione del rischio di violazione privacy a seguito dell'individuazione delle attività nell'ambito delle quali è più elevato il rischio medesimo

- collaborare con il Referente Dirigente di riferimento ed il R.P.D. per l'evasione di eventuali richieste di esercizio di diritti, su istanza dell'interessato, ai sensi del Regolamento UE 679/2016 e norme di armonizzazione e/o per l'effettuazione di valutazione di impatto preventiva al trattamento dei dati particolari (quando necessaria) con sistemi di videosorveglianza, da inviare eventualmente al Garante

- curare, fra gli autorizzati al trattamento sottoposti alla propria autorità, la diffusione di norme, linee guida e di ogni altra disposizione impartita dall'Azienda anche organizzando la formazione di struttura mirata all'aggiornamento continuo ed obbligatorio in materia di privacy, previsto per legge
- In caso di violazione di dati personali con sistemi di videosorveglianza, di cui si sia venuti a conoscenza, segnalare immediatamente, e comunque entro 24 ore, al referente e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali (e

mail segreteria.contratticonvenzioni@asl3.liguria.it) qualsiasi violazione privacy in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati, con le modalità previste dal D.P.S. aziendale e dalla normativa vigente

- registrare ed aggiornare costantemente, sul registro dei trattamenti di afferenza, il trattamento con sistemi di videosorveglianza e comunicarlo come previsto dal D.P.S. aziendale.

Si ricorda infine che, laddove la normativa preveda l'attivazione di sistemi di videosorveglianza presso strutture di soggetti-enti terzi **che collaborano ai trattamenti della struttura-area di afferenza (per competenza tecnico-economico – gestionale),** affidatari di servizi in forza di specifici accordi contrattuali e/o convenzionali e, pertanto, designati quali responsabili esterni e/o contitolari, **i direttori delle strutture- aree di afferenza (per competenza tecnico-economico – gestionale) devono fornire a detti responsabili esterni/contitolari le necessarie istruzioni** circa la corretta gestione e tutela dei dati personali mediante utilizzazione di sistemi di videosorveglianza, anche ai fini della loro integrità e sicurezza, vigilando sull'osservanza delle stesse e della normativa in materia, **anche con periodici e sistematici audit e controlli**, **ed aggiornando in punto il R.P.D. e la S.C. Affari Generali.**

Come sopra evidenziato tutte le persone fisiche che, nelle singole Strutture, svolgono materialmente le operazioni di trattamento dati mediante utilizzazione di sistemi di videosorveglianza devono essere designate in tal senso come "DIPENDENTI (o assimilati) autorizzati al trattamento dati mediante l'utilizzo di sistemi di videosorveglianza" dal Titolare (con esercizio della delega alla sottoscrizione ricevuta dal Referente/Dirigente/Dipendente con coordinamento competente ad individuarli).

Per la designazione scritta è utilizzata apposita modulistica, da adattare, caso per caso, elaborata anche in ragione di compiti e funzioni proprie di determinate categorie.

Infatti dovrà essere **chiarito l'ambito di trattamento effettuabile dall'autorizzato** con la specifica credenziale di accesso che allo stesso verrà assegnata tramite la S.C. Elettromedicali, Impianti e Automazioni (trattare i dati e/o a visionare e/o a far visionare ai soggetti legittimati per legge le immagini degli impianti afferenti alla struttura).

Essa deve prevedere:

- ✓ la data di inizio ed eventuale termine dell' attività all'interno della struttura e/o il riferimento al rapporto che lega la persona all'Azienda
- ✓ in modo sintetico, i trattamenti dati autorizzati , gli ambito di autorizzazione, le banche dati e le procedure informatizzate cui si ha accesso in ragione del profilo e delle mansioni assegnate, anche *per relationem* in riferimento al rapporto che lega la persona all'Azienda.
- ✓ specifiche e dettagliate istruzioni operative, riguardo alle corrette modalità di trattamento dati, in ragione del profilo ricoperto ,dell' attività svolta, delle funzioni e delle competenze attribuite con particolare riguardo alle misure di sicurezza da osservare.

Gli Autorizzati possono accedere ai soli dati indispensabili per assolvere alle attività istituzionali cui sono preposti che e debbono trattare in conformità alla vigente normativa, al D.P.S. aziendale ed alle disposizioni impartite dal Referente/Dirigente /Dipendente con coordinamento del "Sistema privacy" di afferenza.

L'atto di designazione ad Autorizzato costituisce l'unico presupposto di liceità per il suddetto trattamento dei dati personali tramite impianti di videosorveglianza.

1.4 Mappa dei trattamenti effettuati

La stessa è desumibile dal registro dei trattamenti pubblicato nella intranet aziendale in specifica sottosezione della sezione "Normativa/Privacy".

2. AUTORIZZATI ED AMMINISTRATORI DI SISTEMA

L'A.S.L. 3 Titolare del trattamento dei dati provvede, ai sensi del **Regolamento UE 679/2016 e norme di armonizzazione**, a designare i Responsabili esterni del trattamento dei dati, ed i soggetti autorizzati al trattamento.
Dette designazioni vengono effettuate dal Titolare A.S.L. 3, nella persona del legale rappresentante pro-tempore direttamente o delegando alla sottoscrizione (direttori e/o responsabili di struttura od articolazione aziendale assimilata nel "Sistema privacy" per area di competenza). Analogamente avviene per la sottoscrizione di eventuali designazioni a Responsabile esterno o accordi di Contitolarità richieste al Titolare A.S.L. 3.
Il Titolare del trattamento o detti delegati alla sottoscrizione per conto del Titolare, individuano, nell'ambito delle strutture-aree aziendali che dirigono, i Dipendenti autorizzati al trattamento dei dati di competenza delle strutture stesse, che verranno designati sempre dal Titolare A.S.L. 3, nella persona del legale rappresentante pro-tempore, con delega di sottoscrizione delle relative designazioni per suo conto a favore dei suddetti direttori e/o responsabili di struttura od articolazione aziendale assimilata nel "Sistema privacy". Dette autorizzazioni al personale hanno efficacia fino a termine degli incarichi – assegnazioni conferiti e/o alla modifica degli stessi e precisano il ruolo nel sistema privacy ricoperto dall'autorizzato, al quale il D.P.S. aziendale correla specifici compiti nell'ambito del sistema stesso.
Sono da designare Autorizzati i dipendenti dell'Azienda ed i collaboratori che, a qualsiasi titolo, prestano la loro opera, anche in via temporanea, all'interno delle strutture aziendali od all'esterno delle stesse ma con funzioni assimilate a quelle dei Dipendenti nel "Sistema Privacy aziendale" (ad esempio: tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti, lavoratori interinali) e che, comunque, agiscono sotto l'autorità di A.SL. 3 .

La S.C. Gestione e Sviluppo delle Risorse Umane, contestualmente alla formalizzazione del conferimento di incarichi, prevede che il Referente/Direttore e/o Responsabile di struttura od assimilata articolazione aziendale delegato e/o sub delegato dal Titolare alla sottoscrizione,

provveda alla sottoscrizione per conto del Titolare dell'autorizzazione al trattamento dati dell'incaricato, utilizzando *i format* pubblicati nella sezione della Intranet aziendale denominata "Normativa/privacy, completa degli **specifici compiti** del Dirigente nel sistema privacy per l'area di afferenza, conservando agli atti della struttura-area copia della designazione e dandone comunicazione al R.P.D. ed alla S.C. Affari Generali.
Analogamente, si provvederà per l'autorizzazione al trattamento dati per gli incarichi di direzione delle strutture-aree aziendali che possano derivare da procedure di affidamento temporanee e/o ad interim, per i quali non interviene la sottoscrizione di specifico contratto di riferimento, conservandosi anche in tale ipotesi copia della designazione e dandone comunicazione al R.P.D. ed alla S.C. Affari Generali.
Parimenti analogamente provvederanno le direzioni delle strutture competenti alla formalizzazione degli incarichi e/o autorizzazioni a collaboratori che, a qualsiasi titolo, prestano la loro opera, anche in via temporanea, all'interno delle strutture aziendali e/o per conto delle stesse e, pertanto, assimilati ai Dipendenti nel "Sistema Privacy aziendale" (ad esempio: tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti, lavoratori interinali) o che, comunque, agiscono sotto l' autorità di ASL3 , prevedendo che il Referente/Direttore e/o Responsabile di struttura od assimilata articolazione aziendale, presso il quale operano detti collaboratori , delegato e/o sub delegato dal Titolare alla sottoscrizione, provveda alla sottoscrizione per conto del Titolare dell'autorizzazione al trattamento dati degli stessi, utilizzando i format pubblicati nella sezione della Intranet aziendale denominata "Normativa/privacy.

Ad ogni autorizzato, all'atto della nomina, sono state fornite idonee e specifiche istruzioni scritte.

In particolare è compito dell'autorizzato al trattamento trattare i dati personali (*qualsiasi informazione riguardante una persona fisica identificata o identificabile «interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*" strettamente necessari allo svolgimento delle mansioni proprie assegnate, ed in particolare:

a) trattarli in modo lecito, corretto e trasparente ed, in generale in conformità ai principi del Regolamento UE 679/2016 (con particolare riguardo agli artt.5-6) e norme di armonizzazione;
b) raccoglierli e registrarli per finalità determinate, esplicite e legittime, e successivamente trattarli in modo che non siano incompatibili con tali finalità;
c) verificare la loro esattezza e, se necessario, aggiornarli;
d) verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare

del trattamento dei dati, anche per il tramite del Dirigente/Direttore responsabile della struttura-area di afferenza;

e) conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali sono stati raccolti o successivamente trattati, rispettando le misure di sicurezza predisposte in Azienda. In ogni operazione di trattamento andrà garantita la massima riservatezza;
f) implementare e/o aggiornare costantemente e tempestivamente i contenuti del "registro dei trattamenti" ed i *format* afferenti le banche dati, la valutazione del rischio di violazione privacy e le misure di sicurezza, nonché il monitoraggio periodico di queste ultime, per la parte di competenza della struttura-area di afferenza, provvedendo alla relativa conservazione, pubblicazione e comunicazione al R.P.D. ed alla S.C. Affari Generali, il tutto con le modalità previste dal D.P.S. aziendale (che mantiene i relativi adempimenti sotto la responsabilità del Dirigente/direttore responsabile della struttura-area di afferenza) e dalla vigente normativa;
g) Attuare le misure di sicurezza predisposte dal Titolare del trattamento e riportate nel presente Documento Programmatico sulla Sicurezza e vigilare sul rispetto delle stesse e, comunque, collaborare con il Titolare ed il R.P.D. per la predisposizione e l'aggiornamento delle stesse in modo conforme ai principi contenuti nel Regolamento UE 679/2016 e norme di armonizzazione (in particolare art.32 del Regolamento UE 679/2016 e norme di armonizzazione) e con le modalità previste dal D.P.S. aziendale;
h) fornire idonea informativa agli interessati ed acquisirne il relativo consenso, laddove necessario ai sensi della vigente normativa, nei casi di raccolta del consenso al trattamento dei dati;
i) collaborare con il Responsabile per la Protezione dei Dati (R.P.D.) aziendale ed il Titolare per ogni eventuale istruttoria o chiarimento dovesse essere disposta in materia di protezione dei dati personali;
j) osservare le disposizioni e/o indicazioni del R.P.D. Aziendale e del Titolare (fornite anche per il tramite del Dirigente/Direttore responsabile della struttura di afferenza) in materia di protezione dei dati personali;

k) osservare le disposizioni e gli obblighi derivanti dal Regolamento Europeo 679/2016 e norme di armonizzazione, in particolare per quelli inerenti la comunicazione e la diffusione dei dati.

l) attenersi alla puntuale adozione delle istruzioni impartite dal Titolare direttamente o tramite delegato alla firma ed anche per il tramite dei Dirigenti/Direttori responsabili della struttura-area di afferenza circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza;

m) Collaborare con il R.P.D. per l'evasione di eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati presentate su istanza dall'interessato ai sensi del Regolamento UE 679/2016 e norme di armonizzazione;

n) Procedere all'individuazione di eventuali dipendenti (od assimilati) sotto propria responsabilità da autorizzare al trattamento dei dati personali o di categorie particolari di dati personali e sottoscriverne per delega del Titolare la nomina, completa di specifiche istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, utilizzando i *format* pubblicati nella sezione della Intranet aziendale denominata "Normativa/privacy, dandone comunicazione al R.P.D. ed alla S.C. Affari Generali . La documentazione delle designazioni sottoscritte ed aggiornate, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento, deve essere conservata sotto la responsabilità del Dirigente-responsabile, presso la struttura-area diretta e presso quella di assegnazione dell'autorizzato e, per quanto possibile, correlata dal Dirigente-responsabile stesso al registro dei trattamenti di afferenza della struttura-area, nonché messa a disposizione di RPD aziendale e S.C. Affari Generali, su loro richiesta

   Nell'ambito delle istruzioni così impartite dal Titolare dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun autorizzato, nonché il Titolare vigilerà, anche con l'eventuale supporto dell'Amministratore di sistema, della rete dei Referenti e Dirigenti aziendali, per gli ambiti di rispettiva competenza, che l'accesso ai dati da trattare da parte degli autorizzati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle pre-

dette autorizzazioni il Titolare avrà anche il compito di verificare, almeno annualmente, con il supporto della rete dei Referenti e Dirigenti aziendali, la sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto di procedere alla revoca delle stesse. La designazione ad autorizzato dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti e/o neo assegnati, assegnati alle singole strutture-aree, che effettuano trattamento dei dati e rientra negli specifici compiti assegnati nel "Sistema privacy" aziendale alla responsabilità del Dirigente-Direttore responsabile della struttura- area di afferenza del neoassunto e/o neo assegnato, che è responsabile anche della **verifica almeno annuale della sussistenza delle condizioni** che hanno determinato la designazione ed in difetto della revoca della stessa.

L'eventuale redazione ed utilizzo di modulistica specifica in materia di trattamento dei dati personali (informative, modelli di acquisizione del consenso, liberatorie per l'utilizzo di immagini, ecc.), diversa rispetto alla modulistica allegata al presente documento, dovrà essere previamente concordato con la S.C. Affari Generali ed il R.P.D.

2.1 Amministratori di sistema

In ottemperanza a quanto prescritto dal provvedimento dell'Autorità Garante per la protezione dei dati del 27 novembre 2008, pubblicato sulla Gazzetta Ufficiale n. 300 del 24 dicembre 2008 "Misure e accorgimenti prescritti ai titolari di trattamento effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i, l'A.S.L.3 ha provveduto al conferimento di incarico di Amministratore di Sistema, da identificarsi nella figura professionale dedicata alla gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, ai seguenti dipendenti:

Sig. Cosolito Vitale Alessandro - Assistente Tecnico Informatico - funzioni attribuite per gli applicativi del settore diagnostica per immagini (RIS/PACS), anatomia patologica, laboratorio analisi interaziendale (LIS), cardiologia, neurologia, CPR (*clinical patient repository*), medicina nucleare, ricetta elettronica, dossier sanitario elettronico, firma digitale e carta nazionale dei servizi, sistema di gestione ospedaliero, sale operatorie, pronto soccorso, vaccinazioni, nefrologia, Gestione ambulatoriale, teleconsulto specialistico intra-interaziendale, screening oncologici, endoscopia, salute mentale, cardiologia, dipartimento prevenzione, allergologia neonatale, ostetricia e ginecologia, diabetologia, dietologia, rianimazione, riabilitazione e rieducazione funzionale, ge-

riatria, reumatologia, pneumologia, centrale monitoraggio DEA, sistema di conservazione sostitutiva legale, prescrizione elettronica aziendale, centro trasfusionale, CUP Liguria, portale Tessera Sanitaria, anagrafe aziendale dei contatti, anagrafe sanitaria regionale, fascicolo sanitario elettronico, funzioni attribuite per infrastrutture/applicativi concernenti attività per piattaforma Windows/VmWare e amministratore di rete; limitatamente per il servizio di reperibilità, Amministratore di sistema

Sig.ra Cassano Maria - Collaboratore Tecnico – funzioni attribuite per gli applicativi di gestione del Personale relativamente alle competenze giuridico – matricolare – economico e per rilevazione presenze e assenze, funzioni attribuite per gli applicativi del settore protocollo, gestione documentale, Dossier sanitario elettronico ,Gestione ambulatoriale, Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, funzioni attribuite per infrastrutture/applicativi concernenti attività per piattaforma Windows/VmWare e amministratore di rete; limitatamente per il servizio di reperibilità, Amministratore di sistema;

Sig. Landi Diego - Assistente Tecnico Programmatore – funzioni attribuite per infrastrutture/applicativi concernenti attività per piattaforma Windows/VmWare e amministratore di rete; limitatamente per il servizio di reperibilità, Ricetta Elettronica, Dossier sanitario elettronico, Sistema di gestione ospedaliero, pronto soccorso, amministratore di sistema; firma digitale e carta nazionale dei servizi

Sig. Rebora Massimo - Assistente Tecnico Programmatore – funzioni attribuite per infrastrutture/applicativi concernenti attività per piattaforma Windows/VmWare, Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, integrazione sistemi dipartimentali, sistemi di prenotazione – Sistema di accesso regionale IAM Ricetta Elettronica, gestione credenziali Fascicolo Sanitario, Amministratore di sistema;

Dott.ssa Ravera Laura - Collaboratore Tecnico – funzioni attribuite per infrastrutture/applicativi per piattaforma Linux – Windows/VmWare – sistemi di RDBMS -, anagrafica ospedaliera, Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, portali informativi web, sistema di accesso regionale IAM, Dossier sanitario elettronico; Integrazione Sistemi Dipartimentali Amministratore sistemi;

D.ssa Daniela Gavaciuto- Collaboratore Tecnico – Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, integrazione sistemi dipartimentali, sistemi di prenotazione – gestione credenziali Fascicolo Sanitario, Amministratore di sistema;

Sig. Lorenzo Guzzinati – Assistente Tecnico Informatico – funzioni attribuite per Libera Professione, Intramoenia, Portali di accesso, applicativi di gestione del Personale relativamente alle competenze giuridico – matricolare – economico e per rilevazione presenze e assenze, ricetta elettronica, specialistica convenzionata, gestione dei trasporti sanitari, portali informativi web, Dossier sanitario elettronico, Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, funzioni attribuite per infrastrutture/applicativi concernenti attività per piattaforma Windows/VmWare e amministratore di rete; limitatamente per il servizio di reperibilità, Amministratore di sistema;

Ing. Manuela Guerisoli – Collaboratore Tecnico Professionale Ingegnere Biomedico - funzioni attribuite per infrastrutture/applicativi concernenti attività per piattaforma Windows/VmWare – Sistema di accesso regionale IAM Ricetta Elettronico, Dossier Sanitario Elettronico, Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, diagnostica per immagini (RIS/PACS), laboratori analisi (LIS), cardiologia, anatomia patologica, neurologia, centri trasfusionali, salute mentale, teleconsulto specialistico intra-interaziendale, screening oncologici, endoscopia, ricetta elettronica, Amministratore di sistema;

Dott.ssa Pareto Luisa - Dirigente Analista – funzioni attribuite per piattaforma Linux – Unix – Windows/VmWare – sistemi di RDBMS – , Anagrafe Sanitaria Web, Sistema di accesso regionale IAM, Dossier Sanitario Elettronico; Sistema di gestione ospedaliero, Sale Operatorie, pronto soccorso, integrazione sistemi dipartimentali, sistemi di prenotazione., gestione documentale, gestione degli asset, referente Pagopa, gestione credenziali Fascicolo Sanitario – Amministratore di sistema;

Sig.ra Patrizia Poli – Assistente Amministrativo - funzioni di amministratore di sistema attribuite relativamente al consenso al trattamento dei dati effettuati tramite Dossier Sanitario, Sistema di accesso regionale IAM Ricetta Elettronico, Anagrafe Sanitaria Web, Amministratore di sistema;

Sig.ra Alba Maggiora – Assistente Amministrativo - funzioni di amministratore di sistema attribuite relativamente al consenso al trattamento dei dati effettuati tramite Dossier Sanitario, Sistema di accesso regionale IAM Ricetta Elettronico, Anagrafe Sanitaria Web, Amministratore di sistema;

Sig. Alessandro Borio – Coadiutore Amministrativo BS - Sistema di accesso regionale IAM Ricetta Elettronico, firma digitale.

Sig. Gianmarco Paone – Borsista - Portali di accesso, portali informativi Web, gestione dei trasporti sanitari,

La Società Liguria Digitale S.p.A., con la quale A.S.L. 3 ha un contratto per la gestione in outsourcing dei sistemi e strumenti informatici, ha provveduto ad identificare ed incaricare gli amministratori di sistema, predisponendo la piattaforma per la raccolta e conservazione dei log di accesso.

L'elenco dei soggetti designati all'interno di Liguria Digitale S.p.A. a svolgere la funzione di amministratore di sistema per conto di ASL3 è conservato presso la S.C. S.I.A., che ne trasmette copia per conoscenza al R.P.D. ed alla S.C. Affari Generali.

Entro il 31 dicembre di ogni anno la S.C. Sistemi Informativi Aziendali verifica l'operato degli Amministratori di sistema, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati personali, provvedendo altresì a confermare annualmente la designazione degli Amministratori di sistema, ove non si siano modificati i relativi profili di autorizzazione e/o a nominare i nuovi Amministratori di sistema ove necessario, trasmettendo contestualmente al R.P.D. ed alla S.C. Affari Generali copia delle note di conferma o copia delle nuove designazioni.

La S.C. Sistemi Informativi Aziendali provvede, inoltre, a richiedere, sempre entro il 31 dicembre di ogni anno, alla Società Liguria Digitale S.p.A. – l'elenco aggiornato degli Amministratori di sistema che svolgono dette funzioni per conto di ASL 3, nell'ambito del servizio in outsourcing per la gestione dei sistemi e strumenti informatici, comprensivo degli estremi identificativi di detti amministratori, trasmettendone copia al R.P.D ed alla S.C. Affari Generali a loro richiesta.

2.2 Autorizzati al trattamento

- Il trattamento dei dati viene effettuato solo dal personale che ha ricevuto una formale autorizzazione mediante designazione per iscritto, attraverso i *format* pubblicati nella sezione della Intranet aziendale denominata "Normativa/privacy**,** con i quali si individua l'ambito del trattamento consentito (c.d. mansionario), con compiti specifici per i Dirigenti/direttori di S.C.

e S.S.D. o strutture assimilate. Si considera tale anche la documentata preposizione del Dipendente e/o assimilato ad una struttura-area per la quale è individuato per iscritto l'ambito del trattamento consentito ai Dipendenti della medesima struttura-area.

- Oltre alle istruzioni generali sulle modalità di trattamento dei dati personali, agli autorizzati sono fornite esplicite istruzioni relativamente a:
- Procedure da seguire per la classificazione dei dati personali al fine di distinguere quelli denominati come particolari, di cui all'art. 9 del regolamento UE 679/2016, osservando le maggiori cautele che questa tipologia di dati richiedono;
- Modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia ed archiviazione degli stessi;
- Modalità per elaborare e custodire le password necessarie per accedere agli strumenti elettronici ed ai dati in essi contenuti;
- Prescrizioni di non lasciare incustoditi ed accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro, né i documenti contenenti dati personali qualora si stia operando un trattamento con supporti di tipo cartaceo;
- Prescrizioni inerenti l'obbligo di assoluta riservatezza e di divieto di divulgazione delle password di accesso al sistema;
- Procedure per il salvataggio dei dati;
- Procedura in caso di assenza prolungata od impedimento dell'incaricato che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema;
- Modalità di utilizzo, custodia ed archiviazione dei supporti rimovibili contenenti dati personali;
- Aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare del trattamento, sulle misure di sicurezza;
- Modalità di utilizzo di posta elettronica ed internet (come da vigente Regolamento aziendale pubblicato sul sito intranet sezione "Normativa/Privacy)

- Prescrizioni sulle modalità di informativa ai terzi (pazienti, utenti, etc.) in merito al trattamento dei loro dati ed all'acquisizione del relativo eventuale consenso, ove previsto dalla vigente normativa, utilizzando i modelli generali allegati al presente documento (**ALLEGATI 11, 11.1, 12, 13, 14, 18, 19, 20, 21, 22, 22.1, 22.2, 23, 24, 25, 26, 26.1, 26.2, 26.3, 26.4, D, E, G, H, I, J, L, M, N, O, U e V**) o specifici modelli integrativi definiti di concerto con la S.C. Affari Generali ed il R.P.D. e/o predisposti a livello regionale (ad es. tramite A.Li.Sa. ex L.R. 17/2016 e ss.mm.ii).

Per i Dirigenti responsabili di struttura complessa-Direttori, SSD ed assimilate l'autorizzazione ricomprende la designazione all'espletamento di specifici compiti infra precisati per la gestione del "Sistema privacy" nella struttura-area diretta. Limitatamente all'area di competenza della struttura-area che dirigono e delle funzioni e competenze correlate, gli stessi dovranno:

1. collaborare con il R.P.D. Aziendale e con il Titolare ed il Referente per l'attuazione delle prescrizioni in materia di privacy;

2. individuare *i Dipendenti (o assimilati), afferenti alla struttura-area diretta da autorizzare al trattamento dei dati di competenza e sottoscrivere le relative autorizzazioni al trattamento dati personali e categorie particolari di dati personali* (**modelli allegati 15, 16, 17, A, A1, A2, P)** per conto del Titolare, che all'uopo delega (o subdelega per il tramite del direttore-Dirigente dell'area di afferenza) alla sottoscrizione, fornendo a detti Dipendenti (o assimilati) le necessarie istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, con le modalità previste dal DPS aziendale. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun autorizzato, nonché si dovrà vigilare, che l'accesso ai dati da trattare da parte degli autorizzati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni bisognerà anche verificare la permanente sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto procedere alla revoca delle stesse. La designazione quale autorizzato dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti-neo assegnati alla struttura-area, che effettuano trattamento dei dati. Dette attività sono sotto la responsabilità dei suddetti Dirigenti-Direttori responsabili;

3. sottoscrivere la designazione dei responsabili esterni del trattamento che collaborano ai trattamenti della struttura-area (individuata sulla base della competenza tecnico-economico-gestionale sul trattamento), secondo le procedure, tempistiche e modalità previste dal D.P.S., per conto del Titolare, che all'uopo delega detti Dirigenti alla sottoscrizione stessa, fornendo a detti responsabili esterni le necessarie istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, effettuando audit e controlli periodici sul rispetto delle stesse ed aggiornando in punto il R.P.D. e la S.C. Affari Generali. Analogamente sono delegati alla sottoscrizione per conto del Titolare delle designazioni a responsabile esterno effettuate da altri nei confronti di ASL 3 o degli accordi interni di contitolarità inerenti i trattamenti di competenza (individuata sulla base della competenza tecnico-economico-gestionale sul trattamento) della propria struttura-area;

4. *garantire,* per la parte di competenza della struttura-area diretta, *l'*implementazione e/o aggiornamento costante e tempestivo dei contenuti del "registro dei trattamenti" e dei format afferenti le banche dati, la valutazione del rischio di violazione privacy e le misure di sicurezza, nonché il monitoraggio periodico di queste ultime, provvedendo alla relativa conservazione, pubblicazione e comunicazione al R.P.D. ed alla S.C. Affari Generali, il tutto con le modalità previste dal D.P.S. aziendale (che mantiene i relativi adempimenti di responsabilità del Dirigente/direttore responsabile della struttura-area di afferenza) e dalla vigente normativa;

5. *concorrere alla definizione di misure idonee a prevenire il rischio di violazione privacy, alla valutazione del rischio di violazione privacy e monitoraggio del sistema privacy per la struttura-area diretta ed a controllare il rispetto da parte dei Dipendenti (od assimilati) della struttura-area stessa delle suddette misure, coordinandosi con il Referente di area ed il R.P.D.;*

6. *provvedere al monitoraggio delle attività svolte nella struttura-area con particolare attenzione a quelle nell'ambito delle quali è più elevato il rischio privacy;*

7. *fornire le informazioni richieste dal R.P.D. a seguito dell'individuazione delle attività nell'ambito delle quali è più elevato il rischio di violazione privacy e formulare specifiche proposte volte alla prevenzione del rischio medesimo;*

8. curare il processo della gestione del rischio nella struttura-area diretta ed il suo aggiornamento, attraverso un'attività di analisi meditata e partecipativa;

9. individuare un proprio Facilitatore della prevenzione del rischio privacy come previsto dal D.P.S. aziendale;

10. verificare la presenza, la correttezza, la completezza, l'aggiornamento, la semplicità di consultazione, l'omogeneità di tutte le informazioni ed i dati della struttura-area, necessarie per la concreta applicazione delle misure di prevenzione del rischio in materia privacy;

11. accertare che l'aggiornamento e trasmissione dei dati al R.P.D. avvenga secondo la procedura e le tempistiche prevista nel D.P.S. aziendale;

12. garantire un adeguato sostegno ai Referenti riguardo a tutti i compiti loro assegnati, sulla prevenzione del rischio, come indicato nel D.P.S. Aziendale;

13. trasmettere tempestivamente (e comunque entro 15 giorni dalla variazione) al Referente ed al R.P.D. e per conoscenza alla S.C. Affari Generali i dati di gestione del rischio privacy della propria struttura ed i relativi aggiornamenti;

14. promuovere ed accertare la conoscenza della normativa privacy e del D.P.S. aziendale, da parte del proprio personale, relazionando il Referente di area ed il R.P.D. sulle criticità accertate;

15. Collaborare con il Referente ed il R.P.D. per l'evasione di eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati ed ulteriori esercizi di diritti su istanza dall'interessato ai sensi del Regolamento UE 679/2016 e norme di armonizzazione **(ALLEGATO 3 policy aziendale per l'esercizio dei diritti degli interessati-utenti ex artt.15-22 GDPR);**

16. presentare al Referente e, per conoscenza al R.P.D ed alla S.C. Affari Generali, ogni richiesta di valutazione di impatto preventiva al trattamento dei dati sensibili (quando necessaria) da inviare eventualmente al Garante e gestire in collaborazione con il Referente la sua effettuazione, sottoponendone i risultati preventivamente al RPD;

17. In caso di violazione di dati personali di cui si sia venuti a conoscenza, segnalare immediatamente, e comunque entro 24 ore, al referente e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali qualsiasi violazione privacy in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati, con le modalità previste dal D.P.S. aziendale e dalla normativa vigente (**ALLEGATO 4 Policy aziendale in caso di violazione privacy – data breach**);

18. Vigilare sull'attuazione da parte dei *dipendenti (od assimilati) afferenti alla struttura-area diretta* degli obblighi di informazione ed acquisizione del consenso, quando richiesto dalla normativa vigente, nei confronti dell'interessato, secondo i format e le modalità previste nel D.P.S. aziendale e policy aziendali attuative e sull'adozione delle cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo pornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari.

La Struttura Complessa Gestione Organizzazione e Sviluppo delle Risorse Umane, contestualmente alla sottoscrizione del contratto di lavoro individuale o al conferimento dell'incarico a qualsiasi titolo, anche in assenza di sottoscrizione di contratto, con il Dipendente e/o assimilato, rende allo stesso le informazioni di cui al modello allegato al presente documento (**Allegati F e J**), pubblicato anche sul sito intranet aziendale, nella sezione "N*ormativa-Privacy".*

Altresì la Struttura Complessa Gestione Organizzazione e Sviluppo delle Risorse Umane rende le informazioni di cui al modello allegato al presente documento (**Allegato 20**) agli utenti/candidati di concorsi e selezioni del S.S.R. unificate su base regionale di relativa afferenza.

Parimenti fa la struttura-area aziendale che conferisce l'incarico e/o alla quale afferisce per competenza il trattamento dati correlato per i consulenti, i partecipanti a gare e a concorsi (**ALLEGATO 18**).

2.3 Accessibilità ai dati per interventi e trattamenti indispensabili ed indifferibili

A.S.L. 3 ha predisposto la seguente procedura operativa al fine di garantire l'accessibilità ai dati necessari per l'espletamento delle funzioni e compiti istituzionali atta a garantire ~~e~~ che, in caso di prolungata assenza o impedimento dell'autorizzato, possa assicurare ai soggetti debitamente autorizzati la disponibilità dei dati o degli strumenti elettronici, per gli interventi indispensabili ed indifferibili che si dovessero rendere necessari per ragioni di operatività o di sicurezza del sistema.

Secondo la procedura in essere per regolamentare detta attività, la Struttura Complessa Sistemi Informativi Aziendali, attraverso i propri Amministratori di Sistema ed a seguito di richiesta scritta del Direttore della Struttura/Dipartimento (o suo sostituto) cui afferisce o del Direttore della Direzione Strategica dell'area di afferenza, nel caso di documentata necessità di accedere ai dati gestiti da un autorizzato, è in grado di rimuovere la password di quell'utente, generandone una nuova che viene consegnata al Direttore della Struttura /Dipartimento (o suo sostituto) cui afferisce o del Direttore della Direzione Strategica dell'area di afferenza, esclusivamente per effettuare l'accesso straordinario. In ogni caso, gli Amministratori di Sistema non possono utilizzare la password originale dell'utente in sua vece. L'accesso straordinario sarà, quindi, effettuato, dopo la rimozione delle credenziali dell'utente, con nuove credenziali. Di detta procedura sarà tenuto uno specifico verbale che dovrà essere conservato presso la struttura nella quale si è reso necessario l'accesso. Il Direttore che ha richiesto la procedura di accesso straordinario è tenuto ad avvertire tempestivamente l'autorizzato che è stata attivata la procedura di generazione di nuove credenziali d'accesso.

In ogni caso l'autorizzato non potrà più utilizzare le precedenti credenziali e per accedere al sistema dovrà richiederne di nuove.

In caso di utilizzazione della suddetta procedura per decesso dell'interessato, la stessa verrà espletata previa informativa agli eredi noto del defunto, con possibilità di partecipazione degli stessi all'accesso straordinario effettuato sui supporti informativi aziendali assegnati al defunto.

2.4 Procedure applicative gestite dall'Area Sistema Informativo Aziendale

Nell'ambito del Sistema Informativo di ASL 3 sono gestite applicazioni che comprendono dati personali e particolari categorie di dati personali relativi alle seguenti competenze:

- Personale aziendale e rilevazione presenze
- Protocollo e gestione documentale
- Contabilità e gestione dei magazzini economali e farmaceutici
- Distribuzione e somministrazione dei farmaci
- Compilazione Piani Terapeutici
- Prescrizioni farmaceutiche territoriali
- Conferma delle prestazioni sanitarie specialistiche erogate
- Attività Consultoriale
- Protesi
- Disabili
- Registro Cause di Morte
- Dipartimento di Prevenzione e veterinaria
- Anagrafe Sanitaria e dei Contatti
- Medicina Legale e Invalidi Civili
- Ricettari
- Ricetta elettronica e dematerializzata
- Gestione Reclami
- Pazienti Celiaci
- Assistenza Domiciliare Integrata
- Attività Istituti Accreditati per la specialistica ambulatoriale
- Gestione RSA
- Gestione Sistema Informativo Ospedaliero
- Pronto Soccorso
- Censimento Dati Assistenza Parto – CEDAP

- Sistema Prevenzione e Sicurezza Ambienti di Lavoro
- Lesioni da Decubito
- Sportello distrettuale polifunzionale
- Trasporti sanitari
- Assistenza ospedaliera privata
- Vaccinazioni
- Sistema Trasfusionale
- Anatomia Patologica
- Gestione Pagamenti Esterni
- Calcolo Trattamento Pensionistico
- Registrazione Notizie di Reato
- Sistema di Gestione Informatizzata del Laboratorio di Analisi
- Sistema di Gestione Informatizzata Diagnostica per Immagini
- Cartella clinica neurologia
- Diabetologia
- Cardiologia
- Nefrologia e Dialisi
- Screening oncologici
- Rischio clinico
- Salute Mentale
- Sert
- Anagrafica utenti
- Medicina Nucleare
- Sale Operatorie
- Convenzionati esterni
- Attività Ambulatoriali Intramoenia
- Gestione Richieste Interne
- Cartella clinica ambulatoriale e ricovero ospedaliero
- Riabilitazione
- Dietologia
- Lesioni Difficili

- Cruscotto Sanitario Epidemiologico
- Cruscotto Amministrativo
- Dossier Sanitario Aziendale
- Refertazione Ambulatoriale
- Portale per acquisizione consenso privacy e dossier aziendale
- Portale per la gestione delle richieste Dipartimento Infrastrutture
- Portale Informativo attività intramoenia
- Portale Perla
- Refertazione endoscopica
- Teleconsulto
- Refertazione remota ECG
- Sportello polifunzionale
- Gestione informatizzata deliberazioni e determinazioni
- Flussi COVID.

3. ANALISI DEI RISCHI A CUI SONO SOGGETTI I DATI

In questa sezione del documento sono stati individuati in formato sintetico i principali eventi potenzialmente dannosi per la sicurezza dei dati, rilevando una gradazione del fattore di rischio (basso, medio o alto) ed i riferimenti circa le contromisure adottate nella prima fase di analisi.

Tale analisi viene riportata riassuntivamente e sinteticamente nella tabella seguente e dettagliata per singole strutture aziendali nei format "**TAB_CODICE STRUTTURA_ 03**" (**ALLEGATO 2.2)** pubblicati sul sito intranet aziendale "Normativa-Privacy" nella specifica sottosezione, che riporta anche le misure di sicurezza adottate:

EVENTO	GRAVITA' STIMATA	CONTROMISURE
Furto credenziali autenticazione	BASSA	Disposizioni sulla custodia e segretezza delle credenziali

Carenza di formazione, disattenzione, incuria o errore materiale degli autorizzati	BASSA	Formazione, internal auditing ed Istruzioni agli autorizzati circa l'attenzione da porre durante un trattamento
Comportamenti sleali o fraudolenti	BASSA	Informazione e formazione agli autorizzati al trattamento sulle responsabilità penali, civili e disciplinari ed internal auditing
Azioni di virus informatici o programmi in grado di violare il sistema informativo aziendale	MEDIA	Il sistemi server sono protetti da antivirus aggiornati quotidianamente. I personal computer connessi alla Rete Aziendale e facenti parte del dominio ASL 3 sono protetti da antivirus centralizzato aggiornato quotidianamente. I rimanenti pc acquisiscono l'aggiornamento dell'antivirus a richiesta dell'utente, attraverso il servizio di assistenza, e, comunque, almeno ogni tre mesi.
Spamming o altre tecniche di sabotaggio	BASSA	Utilizzo regolamentato dell'uso di Internet e della posta elettronica. Implementazione su server aziendali di programma antispam, che blocca la ricezione di e-mail indesiderate.
Malfunzionamento o degrado degli strumenti elettronici	BASSA	Aggiornamento programmato del parco macchine e installazione di patch per le applicazioni da parte del servizio di assistenza
Accessi esterni non autorizzati agli strumenti elettronici	BASSA	La Rete Aziendale si configura come una rete privata e l'ac-

		cesso avviene attraverso credenziali di autenticazione personali.
Accessi non autorizzati a locali o reparti ad accesso ristretto	BASSA	Disposizioni sulle procedure di accesso e dispositivi di sicurezza fisici
Asportazione e furto di strumenti contenenti dati	BASSA	Dispositivi di sicurezza fisica e sorveglianza
Eventi distruttivi, naturali o artificiali, dolosi, accidentali	BASSA	Adozione sistema antincendio e sorveglianza
Guasti ai sistemi complementari	BASSA	Gruppi di continuità e gruppo elettrogeno per il CED
Errori umani nella gestione operativa della sicurezza	BASSA	copie di back up – formazione dipendenti - policy aziendali

Nella policy aziendale analisi rischi a cui sono soggetti i dati **(ALLEGATO 2)** viene descritta la metodologia di analisi e come la stessa verrà implementata nel corso del tempo**.**

4. MISURE ADOTTATE E DA ADOTTARE ATTE A GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI E REQUISITI MINIMI DI SICUREZZA

Alla luce dei fattori di rischio vengono descritte sinteticamente le misure adottate al fine di garantire la sicurezza dei dati, in termini di integrità e disponibilità. Per quanto concerne il trattamento dei dati effettuato senza l'ausilio di strumenti elettronici**:**

- Le operazioni di trattamento e di conservazione dei dati sono effettuate presso uffici, locali ed archivi accessibili solo al personale autorizzato del trattamento, mediante l'utilizzo di apposite chiavi a disposizione dei soli addetti;
- Gli autorizzati operano seguendo le procedure e le istruzioni fornite dal presente D.P.S. e dal Titolare o suo delegato;

- L'accesso agli archivi è controllato e consentito al solo personale specificatamente autorizzato. Dopo l'orario di chiusura le persone ammesse a qualunque titolo sono identificate e registrate. Per gli archivi che non sono dotati di strumenti elettronici per il controllo degli accessi o privi comunque di personale incaricato della vigilanza, le persone che vi accedono sono preventivamente autorizzate dal titolare o dal dirigente responsabile dell'archivio.

- Durante le operazioni di trattamento i documenti non devono essere lasciati incustoditi sia in caso di allontanamento temporaneo dalla stazione di lavoro sia al termine della giornata qualora il trattamento non sia ancora terminato.

- Le riproduzioni di documenti contenenti dati personali da eliminare durante le operazioni di trattamento non devono essere lasciate incustodite sia in caso di allontanamento temporaneo dalla stazione di lavoro sia al termine della giornata qualora il trattamento non sia ancora terminato e devono essere distrutte con modalità tali da non rendere intellegibili i dati personali ivi riprodotti.

- L'accesso agli edifici dell'Azienda è monitorato da personale di servizio, per cui non è permesso l'accesso ad estranei non autorizzati.

- Viene verificata, almeno annualmente, con le modalità previste dal presente D.P.S., l'individuazione dei profili di autorizzazione degli autorizzati del trattamento.

Per quanto concerne il trattamento dei dati effettuato con strumenti elettronici:

- ✓ Ciascun computer integrato nella Rete Aziendale accede alle risorse condivise, quali file server, applicazioni transattive e posta elettronica, attraverso credenziali di accesso a norma. L'accesso a tali risorse viene autorizzato dal Direttore della struttura-area aziendale presso cui viene effettuato il trattamento, il quale ha il compito di comunicare alla S.C. Sistemi Informativi Aziendali ogni variazione delle competenze dell'autorizzato che comportino differenze nell'accesso ai dati.
- ✓ Ogni applicazione transattiva di medio-alta complessità e gestita dalla Struttura Complessa Sistemi Informativi Aziendali (piattaforma Oracle, SQL Server, MySQL, etc.) dispone di un sistema di autenticazione specifico. Ulteriori applicazioni di bassa complessità sono realizzate con semplici database, come MS Access, File Maker e altri, sono gestiti direttamente dall'autorizzato con il sistema di autenticazione del prodotto specifico. Altrettanto dicasi per dati gestiti con applicazioni come word processor e fogli di calcolo.
- ✓ Ogni autorizzato è stato edotto che la password deve essere di almeno otto caratteri e cambiata almeno trimestralmente, e che deve essere tenuta assolutamente riservata. I sistemi informatici di autenticazione che lo consentono sono parametrati per la verifica dei requisiti di lunghezza e scadenza delle password. Tali sistemi non concedono l'accesso in deroga alla politica di sicurezza.

- ✓ Sui pc stand alone che non dispongono di un sistema di autenticazione adeguato, è compito del Dirigente responsabile della struttura-area cui appartiene il Dipendente e/o assimilato ricordare le disposizioni date dal Titolare agli autorizzati ai trattamenti della struttura-area diretta, al fine che non siano utilizzati per la memorizzazione di dati personali e categorie particolari di dati personali.
- ✓ E' prevista la cessazione delle credenziali di autenticazione in caso di inutilizzo delle stesse per un periodo superiore ai sei mesi, e comunque in caso di modifica dei profili di autorizzazione che identificano gli autorizzati del trattamento.
- ✓ E' compito della Struttura Complessa Gestione e Sviluppo Risorse Umane e del Dirigente responsabile della struttura-area di afferenza comunicare alla Struttura Complessa Sistemi Informativi Aziendali le variazioni nello stato dei dipendenti ed assimilati che possono comportare cambiamenti nella politica delle autorizzazioni, come a titolo di esempio cessazioni dal servizio e trasferimenti di struttura.
- ✓ La Rete Aziendale è una Rete Privata, dotata di sistema informatico di sicurezza perimetrale.
- ✓ L'accesso ad Internet è rilasciato su richiesta del Dirigente responsabile della Struttura-area a cui appartiene il Dipendente e/o assimilato.
- ✓ All'assegnazione della matricola viene generato un account di posta aziendale per il Dipendente e/o assimilato.
- ✓ E' stata data disposizione di non abbandonare il posto di lavoro durante una sessione in cui si trattino dati personali o categorie particolari di dati personali. In questa eventualità l'autorizzato ha l'obbligo di chiudere la sessione o di attivare lo screen saver protetto da password personale;
- ✓ L'A.S.L.3 ha deliberato un regolamento relativo all'uso appropriato delle risorse informatiche, dell'uso della posta elettronica aziendale, dell'accesso a Internet. Tale provvedimento è pubblicato sul sito intranet aziendale sezione "Normativa /Privacy". Il personale dell'Azienda è stato informato per via gerarchica ed attraverso la Intranet Aziendale dei contenuti del regolamento;
- ✓ Analogamente si è provveduto per l'attività lavorativa con modalità smartworking.

Sempre allo scopo di impedire intrusioni all'interno della Rete Aziendale è vietato a tutto il personale di utilizzare modem su elaboratori appartenente alla Rete stessa. Ogni apparecchiatura di telecomunicazione installata abusivamente in tale configurazione verrà rimossa immediatamente dal personale coordinato dalla Struttura Complessa Sistemi Informativi Aziendali.

La Struttura Complessa Sistemi Informativi Aziendali sovrintende alle risorse del sistema operativo degli elaboratori e dei sistemi di base dati al fine di consentirne l'utilizzazione.

Le strutture tecniche aziendali, che comprendono gli Amministratori di Sistema, intervengono sul Sistema Informativo attraverso propri codici di accesso.

L'autenticazione degli utenti della Rete Aziendale, per l'utilizzo di risorse quali i documenti e la posta elettronica interna, avviene tramite il sistema operativo (Windows 2000, Me e XP, Window 7, Windows 10).

I criteri e le procedure informatiche per assicurare l'integrità e la disponibilità dei dati sono affidati alle applicazioni di gestione dei dati stessi, al RDBMS ed ai suoi meccanismi di backup e recovery. I dati allocati all'interno dei file del RDBMS (Oracle/SQLServer) sono mascherati dal sistema di criptazione tipico del DB.

I Server dei dati sono ospitati nel CED presso la server farm Liguria Digitale e in parte presso il CED del P.O. Villa Scassi.

I backup dei dati residenti sui server di ASL3 ospitati nel CED presso la server farm Liguria Digitale S.p.A., e presso il CED dello Stabilimento Ospedaliero Villa Scassi vengono eseguiti tutti i giorni della settimana; 6 sono di tipo "incrementale" (da lunedì a sabato) più 1 di tipo "full" che viene effettuato nell'arco del week-end.

La "retention" dei backup è di 3 settimane.

Nel primo week-end di ogni mese il "backup full" eseguito presso il CED della server farm Liguria Digitale S.p.A. viene trasferito in altra sede e conservato per un anno in armadio di sicurezza.

I sistemi, le NAS e le librerie utilizzati per i backup sono ubicati in sala diversa da quella dove sono installati i sistemi ASL3 su cui risiedono i dati da salvare.

I dati salvati sono replicati su di un'altra NAS ubicata in una sede Liguria Digitale diversa dalla Server Farm.

Tutto le apparecchiature del Centro Elaborazione Dati sono oggetto di contratto di assistenza e manutenzione che garantisce la sostituzione della componentistica e la reinstallazione del software di base.
Tutte le operazioni di assistenza sono organizzate sulla base di Livelli di Servizio che governano i tempi di intervento.

Lo stato attuale è comunque meglio descritto nello specifico documento redatto secondo lo schema stabilito dalla circolare AGID 2/2017 del 18/04/2017 "Misure Minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del presidente del Consiglio dei Ministri 1 Agosto 2015**)** **Allegato K** (agli atti della S.C. Sistemi Informativi Aziendali e riportato in allegato).

5. CRITERI E MODALITA' DI RIPRISTINO DEI DATI A SEGUITO DI DISTRUZIONE O DANNEGGIAMENTO E DI SEGNALAZIONE DELLE VIOLAZIONI PRIVACY

Qualora, tra i sistemi gestititi dalla Struttura Complessa Sistemi Informativi Aziendali si dovessero verificare situazioni di emergenza derivanti dal danneggiamento di un supporto di memorizzazione (HD, CD, DVD, etc.) o dalla distruzione accidentale delle informazioni memorizzate, si descrive la procedura normalmente attuata:

- ✓ Individuazione del malfunzionamento da parte del personale del CED
- ✓ Attivazione dei servizi di assistenza e manutenzione
- ✓ Ripristino del sistema ed eventuale caricamento del backup.

Qualora si dovessero verificare situazioni di emergenza derivanti dal danneggiamento di un supporto di memorizzazione (HD, CD, DVD, etc.) o dalla distruzione accidentale delle informazioni memorizzate su un pc stand alone, si descrive la procedura normalmente attuata:

- ✓ L'utente che ha verificato l'impossibilità di accedere ai dati di cui è autorizzato, comunica l'evento al dirigente della struttura-area di afferenza e contatta il servizio telefonico di assistenza informatica. Il servizio di assistenza opera all'interno di livelli di servizio definiti
- ✓ Il servizio di assistenza assegna a un tecnico l'intervento
- ✓ Attivazione dei servizi di assistenza e manutenzione
- ✓ Ripristino del sistema, ed eventuale caricamento del backup, messo a disposizione dall'autorizzato al trattamento.

Rimane ovviamente di competenza del dirigente della struttura-area di afferenza valutare e gestire eventuali aspetti correlati ad una violazione di dati personali da perdita di disponibilità come da D.P.S. **(in particolare paragrafo 5.1)** e policy aziendale **(ALLEGATO 4 Regolamento per l'utilizzo della dotazione informatica aziendale, della posta elettronica e dell'accesso a Internet**).

5.1.Policy aziendale in caso di violazione privacy (DATA BREACH)

Il Titolare ha l'obbligo di notificare all'autorità di controllo (Garante Privacy) le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e, comunque, «senza ingiustificato ritardo», soltanto nel caso in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati.

Se i predetti rischi sono valutati dal titolare come elevati, ne dovranno essere informati anche gli interessati a meno che il Titolare:

- Abbia messo in atto misure adeguate di protezione ai dati oggetto delle violazioni, in particolare quelle che rendono incomprensibili i dati (cifratura e/o anonimizzazione)

- Abbia messo successivamente in atto misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e libertà degli interessati.

- La comunicazione potrebbe richiedere sforzi sproporzionati. In questo caso si procede a comunicazione pubblica od a una misura simile.

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati negli artt. 33 e 34 del Regolamento Europeo 679/2016.

In particolare per la notifica il Titolare deve indicare:

- la natura della violazione compresi, ove possibile, le categorie di dati e di interessati coinvolti
- comunicare i dati di contatto del responsabile della protezione dei dati (R.P.D.) o altro punto di contatto per avere ulteriori informazioni
- descrivere le probabili conseguenze della violazione dei dati personali
- descrivere le misure adottate o che si intendono adottare per porre rimedio alla violazione ed attenuarne se possibile gli effetti negativi.

Il Titolare del trattamento, anche laddove ritenga che non ci siano rischi per i diritti e le libertà degli interessati, documenta comunque qualsiasi violazione dei dati personali, che deve contenere gli stessi elementi previsti per la notifica.

In caso di violazione di dati personali di cui si sia venuti a conoscenza ciascun Dipendente e/o assimilato è tenuto a segnalare immediatamente e, comunque, non oltre le 24 ore, al proprio Dirigente responsabile di struttura, al Referente e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali (e mail: segreteria.contratticonvenzioni@asl3.liguria.it) qualsiasi violazione privacy in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati.

La comunicazione deve contenere possibilmente le seguenti informazioni:

- la natura della violazione (es. lettura, copia, alterazione, cancellazione, furto, etc.) compresi, ove possibile, le categorie di dati (es. dati anagrafici, indirizzo di posta elettronica, dati di accesso o identificazione, categorie particolari di dati personali, dati di contatto, dati personali, etc.) e di interessati coinvolti (es. minori, soggetti a particolari tutele, utenti, privati, etc.), indicazioni circa l'eventuale dispositivo oggetto di violazione e la sua ubicazione (es. computer, rete, dispositivo mobile, file o parte di esso, strumento di backup, etc.)
- descrizione delle probabili conseguenze della violazione dei dati personali

- descrizione delle eventuali misure adottate o che si ritiene possano essere adottate per porre rimedio alla violazione ed attenuarne se possibile gli effetti negativi.

In punto si richiama anche la policy aziendale in materia di violazione **(ALLEGATI 4, 4.1).**

La notifica qualora effettuata dovrà contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali.
La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it (solo PEC) oppure tramite posta elettronica ordinaria all'indirizzo protocollo@gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.
L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e opzionalmente la denominazione del titolare del trattamento ASL 3.

Il Garante ha anche fornito uno specifico format, scaricabile dal sito dello stesso, all'indirizzo:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

6. FORMAZIONE DEGLI AUTORIZZATI AL TRATTAMENTO DATI

La formazione degli autorizzati deve essere monitorata dal Dirigente responsabile della struttura-area di afferenza.

La formazione viene predisposta e curata in particolare al momento di ingresso dell'autorizzato al servizio e quando si proceda all'installazione di nuovi strumenti elettronici per il trattamento dei dati o nuovi trattamenti, ma deve accompagnare costantemente, anche on the job, l'attività degli autorizzati.

La formazione ha come obiettivo quello di sensibilizzare gli autorizzati al trattamento sulle tematiche della sicurezza, analizzando i rischi e le responsabilità che tale operazione comporta, anche attraverso un'attenta analisi dei vigenti testi normativi.

Inoltre essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto delle categorie particolari di dati personali e delle modalità per aggiornarsi sulle misure adottate dall'Azienda.

La Struttura Complessa Sistemi Informativi Aziendali svolge costantemente opera di informazione attraverso pubblicazioni sulla rete Intranet aziendale riguardanti le corrette modalità di utilizzo delle strutture tecnologiche ed applicative dell'Azienda.

La S.C. Affari Generali ha provveduto ad organizzare in aula, in collaborazione con la S.C. Aggiornamento e Formazione, corsi di formazione per i Direttori delle Strutture Complesse Amministrative, Tecniche e Sanitarie.

Per quanto concerne la formazione degli altri Dipendenti autorizzati, fermo restando che la stessa deve essere monitorata da ogni singolo Dirigente delle strutture-aree di appartenenza per le relative competenze, dato l'elevato numero degli stessi, la S.C. Affari Generali, di concerto con la S.C. Aggiornamento e Formazione, ha organizzato un corso di formazione on-line (FAD), fruibile anche dai suddetti Direttori.

Il corso di formazione per tutti i Dipendenti e/o assimilati ha come finalità quella di far conoscere i rischi che possono incombere sui dati; le misure a disposizione per poter prevenire eventi dannosi; le disposizioni in materia di trattamento e protezione dei dati personali, le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure adottate dal Titolare.

Nel 2008 il corso sulla privacy è stato accreditato presso la Commissione Regionale ECM per tutte le figure professionali del ruolo sanitario.

A fine giugno 2018 è stato messo a disposizione un aggiornamento del corso FAD sulla base delle nuove norme europee ed aggiornato successivamente sulla base delle disposizioni nazionali di armonizzazione e delle indicazione dell'Autorità Nazionale di controllo (Garante privacy). A detto corso si affiancano, sempre anche con finalità formative le attività di audit interno e gli incontri mirati su specifici argomenti, nonché le istruzioni operative specifiche su singole problematiche legate al trattamento dati.

In particolare durante il periodo di pandemia dal 2020 sono state costantemente fornite linee guida ed istruzioni specifiche e format operativi agli autorizzati per le operazioni di trattamento dati, nel rispetto della vigente normativa, anche emergenziale, di volta in volta vigente, consultabile sul sito intranet e/o internet aziendale dedicato.

7. MISURE DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELL'AZIENDA E DI TRATTAMENTI IN CONTITOLARITA'

Il responsabile (esterno) del trattamento ex art.28 Regolamento U.E. 679/2016 e norme di armonizzazione.

L'A.S.L. 3 attraverso incarichi formali (a titolo meramente esemplificativo convenzione, contratto, ecc.) si avvale di soggetti esterni per lo svolgimento di attività e servizi, correlate alle finalità

istituzionali dell'Azienda, che determinano un trattamento di dati per conto di ASL 3. Tali soggetti operano, pertanto, di norma, quali Responsabili esterni dell'Azienda.

La designazione del Responsabile esterno è effettuata dal Titolare, previa istruttoria delle strutture aziendali competenti per materia, con delega di sottoscrizione dei relativi accordi contenenti la designazione in capo al Dirigente responsabile della struttura-area aziendale con **competenza tecnico-economico – gestionale in materia.** A tale scopo ogni struttura-area aziendale che proceda ad affidare un'attività od un servizio all'esterno della ASL 3 è tenuta a predisporre tempestivamente la designazione del soggetto affidatario quale Responsabile esterno del trattamento, utilizzando il modello allegato al presente documento **(Allegato 9, 9.2 9.3 e per forniture complesse 9.1)** e dandone atto nel provvedimento di affidamento dell'attività o del servizio e/o comunque negli accordi contrattuali-convenzionali conseguenti.

La S.C. Affari Generali, la S.C. S.I.A. ed il R.P.D. collaborano con le strutture aziendali qualora si renda necessario integrare il modello di nomina in relazione allo specifico trattamento di dati affidato all'esterno. Parimenti, in caso di affidamenti di interesse regionale, la S.C. Affari Generali ed il R.P.D. collaborano con gli altri R.P.D. del S.S.R. all'elaborazione congiunta di format specifici.

Nell'ambito degli incarichi affidati, i soggetti esterni assumono l'obbligo di operare secondo quanto previsto dalle vigenti disposizioni in materia di protezione dei dati personali, nonché secondo le istruzioni generali impartite dal Titolare e di fornire al medesimo tutte le informazioni necessarie per consentire l'attuazione di adeguate verifiche periodiche.

Il Responsabile esterno, così designato, si impegna in particolare, a titolo esemplificativo, a garantire:

1. di trattare i dati in ottemperanza ai principi sanciti:
- dall'ordinamento nazionale ed europeo in materia di protezione dei dati;
- dall'articolo 5 del Regolamento UE 679/2016;

2. di inviare, con cadenza annuale, all'Azienda l'elenco aggiornato degli Amministratori di Sistema e degli eventuali terzi affidatari, da designarsi a loro volta Responsabili del trattamento dei dati, per la preventiva autorizzazione;

3. di comunicare il luogo fisico di archiviazione dei dati sottoposto ad allocazione vincolante all'interno del territorio italiano, nonché le modalità di loro conservazione (backup e architetture di *Disaster Recovery*) ovvero, fermo restando quanto precede, le eventuali allocazioni su *cloud*, i relativi dati di sicurezza, declinando le generalità del provider/gestore per la relativa autorizzazione e designazione preventiva a responsabile esterno;

4. di attenersi ai criteri di segretezza e tutela nella gestione dei dati conferiti, utilizzandoli al solo scopo di erogare le prestazioni richieste;

5. di non trattare i dati dell'interessato/utente oltre al tempo strettamente necessario ad espletare l'attività affidata ed i connessi adempimenti amministrativo-contabili inerenti/derivanti;

6. di somministrare all'interessato/utente adeguata informativa e registrarne/acquisirne il consenso, ove previsto dalla vigente normativa nazionale e/o europea, con obbligo di conservazione possibilmente insieme alla documentazione relativa all'interessato/utente.

Il Responsabile esterno è tenuto a rispondere direttamente, a tutti gli effetti di legge, con manleva totale dell'ASL 3 per eventuali violazioni di norme, inadempimenti giuridici, inosservanze regolamentari, nonché per i danni inerenti / derivanti dai trattamenti dati di cui trattasi, per i quali l'ASL 3 possa essere chiamata a rispondere, sia civilmente, sia in punto privacy.

Rendicontazione, audit e collaborazione

Se il Responsabile esterno del trattamento ritiene che alcune delle istruzioni violino una qualsiasi disposizione di legge comunitaria o nazionale lo comunica al Titolare senza ingiustificato ritardo.

Il Responsabile esterno mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'accordo di nomina a responsabile del trattamento, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da quest'ultimo incaricato.

Tenuta del registro delle attività di trattamento

Il Responsabile esterno si impegna altresì a redigere per iscritto, se previsto per legge, un registro delle attività di trattamento effettuate per conto del Titolare, che contenga almeno le informazioni di cui all'art 30.2 del Regolamento UE 679/2016.

Comunicazione a terzi

Il Responsabile esterno non comunica i dati a terzi a meno che non sia espressamente autorizzato a farlo dal Titolare.
Il Responsabile esterno può trasmettere dati ad altri Responsabili per conto dello stesso Titolare, in conformità con le istruzioni da questo fornite. In questo caso, il Titolate identificherà, in anticipo e per iscritto, il soggetto a cui vanno comunicati i dati, i dati da comunicare e le misure di sicurezza da applicare alla comunicazione.

Il Responsabile esterno deve rispettare il divieto assoluto di diffusione, condivisione, comunicazione a terzi e di trasferimento dati a soggetti situati in paesi terzi (extra UE), con particolare attenzione a soggetti giuridici afferenti l'indotto delle prestazioni sanitarie e sociali ovvero la fornitura/commercializzazione di beni e servizi ad essa afferenti;

Se il Responsabile esterno intendesse comunque trasferire tutti o alcuni dati personali oggetto dell'Accordo verso un paese terzo o un'organizzazione internazionale, si impegna ad informare il Titolare prima di procedere al trasferimento, fornendo indicazioni sulla base legale che legittima il trasferimento.

Ricorso ad altri Responsabili e Subresponsabili

Il Responsabile esterno non può ricorrere ad altro o nominare altro responsabile, senza previa espressa e scritta autorizzazione del Titolare.

Requisiti minimi da imporre ad altri Responsabili e Subresponsabili

Qualora il Responsabile esterno nomini, previa espressa e scritta autorizzazione del Titolare, altro Responsabile del trattamento su tale altro Responsabile del trattamento sono imposti mediante atto scritto, gli stessi obblighi in materia di protezione dei dati contenuti nell'accordo di nomina a Responsabile esterno del trattamento.
Qualora il Responsabile esterno nomini altro Responsabile del trattamento e quest'ultimo ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

Per quanto attiene i seguenti aspetti inerenti la protezione dei dati il Responsabile esterno si impegna inoltre a garantire:

A. per quanto attiene alla riservatezza dei dati trattati

- di mantenere la segretezza e riservatezza riguardo a dati e informazioni personali e non ai quali abbia avuto accesso in virtù dell'incarico anche dopo il termine dello stesso incarico;
- che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza od abbiano un adeguato obbligo legale di riservatezza.

B. per quanto attiene gli Autorizzati al trattamento

- individuare tra i propri collaboratori, quelli che compiono operazioni di trattamento dati personali e categorie particolari di dati personali e nominarli quali persone autorizzate al trattamento;
- recepire le istruzioni impartite da Titolari e Responsabili, comunicandole agli Autorizzati al trattamento ed istruendoli circa gli obblighi previsti dalle vigenti disposizioni in materia di privacy;
- adoperarsi al fine di rendere effettive le suddette istruzioni, curando in particolare il profilo della riservatezza, della sicurezza di accesso e dell'integrità dei dati;
- stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli Autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persona fisiche.

Il Responsabile esterno si impegna ad informare l'interessato/utente sulle modalità utilizzate per conservare i dati in modo da consentire la sua identificazione per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e/o successivamente trattati, avendo cura di applicare, in caso di conservazione digitalizzata, le norme vigenti in materia.

Il Responsabile ***inoltre si impegna a garantire:***

- di comunicare, a richiesta dell'Azienda, in caso di esercizio dei diritti di cui e agli artt. da 15 a 21 e 23 del Regolamento UE n. 679/2016, i dati inerenti i *file di log* di accesso in formato intellegibile al fine di consentire la loro esibizione, come previsto all'interno del sopraccitato Regolamento UE.

Su richiesta del Titolare il Responsabile dà seguito direttamente e tempestivamente a dette richieste di esercizio dei diritti, dandone contestualmente comunicazione al Titolare.

In caso di violazione, fuga o perdita di dati personali, il Responsabile esterno del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Nell'informare il Titolare il Responsabile esterno comunica le seguenti informazioni:

- Descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di dati personali oggetto della violazione;
- il nome ed i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere ulteriori informazioni;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi sui diritti e libertà delle persone fisiche;
- descrizione delle probabili conseguenze della violazione dei dati personali.

Valutazione d'impatto

Se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto dell'Accordo di nomina, il Responsabile esterno assiste il Titolare nella redazione della Valutazione d'impatto sulla protezione dei dati.

Consultazione preventiva

Se si rende necessaria la Consultazione preventiva dell'autorità di controllo, in merito alle attività di trattamento oggetto dell'accordo di nomina, il Responsabile esterno assiste il Titolare fornendogli tutte le informazioni necessarie per la Redazione della Consultazione preventiva.

Responsabile della Protezione dei Dati

Il Responsabile designa ai sensi dell'art. 37.1, un Responsabile della Protezione dei Dati (RPD) di cui al capo IV, Sezione 4, qualora rientrante nei casi previsti dall'art. 37.1 e, comunque, un referente Privacy.

Misure di sicurezza

Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, ma anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile esterno del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Il Responsabile esterno deve implementare misure che garantiscano:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi in uso ai fini dello svolgimento delle Attività di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico;
- la verifica e valutazione periodica dell'efficacia delle misure tecniche e organizzative.

Il Responsabile comunque ***si impegna a garantire:***

1. di osservare e applicare, anche per conto di eventuali terzi affidatari, le misure idonee alla sicurezza dei dati a norma del Regolamento UE n. 679/2016, con particolare riferimento all'applicazione del criterio di indispensabilità del dato nella cernita degli stessi;

2. di applicare, anche in caso di trattamento digitale dei dati, misure di sicurezza, volte ad eliminare o, comunque, a ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati personali e delle categorie particolari di dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle disposizioni contenute nel Regolamento U.E. 679/2016 e relative norme di armonizzazione;
3. di adottare le cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo pornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);
4. di comunicare per iscritto, in forma chiara, compiuta e specifica all'Azienda le misure assunte a norma dello stesso, nonché le modalità di conservazione dei dati, del loro ripristino, della gestione dei *data breach* e dei *file di log* relativi alla tracciabilità degli accessi;
5. di garantire il rispetto degli artt. da 32 a 36, con particolare riferimento all'art. 33 par. 2 del Regolamento UE n.679/2016 (*data breach*);
6. di comunicare per iscritto, in forma chiara, compiuta e specifica all'Azienda le misure idonee alla sicurezza del dato, a norma del Regolamento UE n. 679/2016;
7. produrre acconcia documentazione scritta ovvero relazione circa il regolare adempimento di quanto sopra ad ASL e per essa al suo RPD, consentendo eventuali verifiche sul campo.

Termine del rapporto

Al termine della prestazione dei servizi che comportano l'attività di trattamento, il Responsabile esterno dovrà:

- restituire i dati personali al Titolare del Trattamento ed eliminarli dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati;
- eliminarli in maniera permanente dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati.

In caso di inadempimento a quanto previsto dall'Accordo di nomina, l'incarico sarà soggetto a revoca di diritto, con contestuale caducazione del rapporto contrattuale/convenzionale sostanziale per violazione privacy, fatto salvo il ristoro di eventuali danni inerenti e /o derivanti da tali violazioni.

Ciò fatto salvo, la durata della designazione segue il rapporto contrattuale/convenzionale sostanziale di riferimento a decorrere dall'effettiva attivazione dello stesso.

Responsabilità

Se il Responsabile esterno del trattamento viola una delle disposizioni della nomina a responsabile del trattamento, determinando le finalità ed i mezzi del trattamento, è considerato Titolare delle attività di trattamento per le quali ha determinato in autonomia finalità e mezzi del trattamento.

Il Responsabile esterno risponde per il danno causato dal trattamento in solido con il Titolare, il quale si potrà rivalere sul Responsabile esterno nel caso quest'ultimo od un Subresponsabile non abbia adempiuto gli obblighi dell'accordo di nomina od abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

ASL 3 è manlevata da eventuali danni inerenti o derivanti dalla mancata osservanza delle istruzioni date e/o da comportamenti illeciti per fatto del Responsabile esterno o dei soggetti dei quali lo stesso si avvale.

Ogni struttura deve tenere un elenco dei soggetti nominati Responsabili esterni del trattamento, conservando altresì copia dell'avvenuta nomina, che dovrà essere comunicata tempestivamente ed in modalità elettronica, su richiesta, al R.P.D., al Referente privacy di afferenza ed alla S.C. Affari Generali.

In presenza di trattamenti di interesse regionale A.S.L. 3 utilizzerà l'eventuale modello di accordo di designazione predisposto a livello regionale, anche sulle basi delle indicazioni di A.Li.Sa. ed L.R. n.17 del 29.7.2016 e s.m.i.

Eventuali diversi modelli di designazione potranno essere concordati con il responsabile esterno da A.S.L. 3, sentita la S.C. Affari Generali ed il R.P.D.

Il Contitolare del trattamento ex art.26 Regolamento U.E. 679/2016 e norme di armonizzazione

Ai sensi dell'art. 26 Regolamento U.E. 679/2016 e norme di armonizzazione «Contitolare del Trattamento» è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, con conseguente esercizio di potere decisorio, scelte, potere di ordine, di direttiva vincolante e di controllo.

Tramite Accordo interno i contitolari regolano il proprio rapporto in relazione alle attività di trattamento di dati personali e categorie particolari di dati personali, con particolare attenzione alla protezione dei dati (**Allegato 10).**

Eventuali diversi modelli di Accordo potranno essere concordati con il contitolare da A.S.L. 3, sentita la S.C. Affari Generali ed il R.P.D.

In presenza di trattamenti di interesse regionale A.S.L. 3 utilizzerà l'eventuale modello di accordo predisposto a livello regionale, anche sulle basi delle indicazioni di A.Li.Sa. ed L.R. n.17 del 29.7.2016 e s.m.i.

Ciascuna struttura- tiene inoltre costantemente aggiornata la documentazione delle nomine a responsabile esterno ricevute e degli accordi di contitolarità sottoscritti, a cura e sotto la responsabilità del Dirigente responsabile della struttura-area alla quale i relativi trattamenti afferiscono per competenza tecnico-economico-gestionale.

8.INDIVIDUAZIONE DEI CRITERI DA ADOTTARE PER LA CIFRATURA O PER LA SEPARAZIONE DEI DATI INERENTI LO STATO DI SALUTE DAGLI ALTRI DATI PERSONALI DELL'INTERESSATO

I dati contenuti nei database dei server gestiti dalla S.C. Sistemi Informativi Aziendali sono gestiti dalla tecnologia Oracle e SQL SERVER. Tali RDBMS memorizzano i dati e le strutture all'interno di file che non sono leggibili al di fuori dell'architettura stessa, a meno che non siano stati esportati con le procedure previste.

9.CONSEGNA DEI REFERTI ON LINE

La ASL 3 ha messo a disposizione della propria utenza il servizio di consegna on line dei referti relativi agli esami di laboratorio, che consente di accedere e di stampare i propri referti via internet.

Nel rispetto della normativa in materia di riservatezza dei dati sono esclusi dalla consultazione on line i referti relativi a:

- esami per HIV;
- esami colturali;

- esami che ricomprendono analisi genetiche.

Gli autorizzati al trattamento che svolgono l'attività di accettazione dovranno consegnare all'utenza l'informativa sul trattamento dei dati e acquisire di volta in volta lo specifico consenso da parte del richiedente il servizio, laddove ancora previsto dalla vigente normativa, utilizzando i modelli di cui agli **allegati 21 e G** al presente documento, nella versione attualmente definita in Regione Liguria, e pubblicato attualmente nell'apposita sezione del sito Internet aziendale.

In presenza di trattamenti di interesse regionale A.S.L. 3 utilizzerà l'eventuale modello di informativa ed eventuale raccolta consenso predisposto a livello regionale, laddove previsto dalla vigente normativa, anche sulle basi delle indicazioni di A.Li.Sa. ex L.R. n.17 del 29.7.2016 e s.m.i.

10. AUTORIZZATI AL TRATTAMENTO NELL'AMBITO DELLE SPERIMENTAZIONI CLINICHE

L'Azienda tramite le Sue strutture cliniche ospedaliere e non e tramite il proprio personale sanitario è coinvolta nell'ambito delle sperimentazioni cliniche in qualità di centro sperimentatore.
In relazione ai trattamenti di dati effettuato nell'ambito delle sperimentazioni citate l'Autorità garante per la protezione dei dati personali ha adottato con la Deliberazione n. 52 del 24 luglio 2008, in corso di aggiornamento, le "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali", nelle quali sono individuate le disposizioni cui devono attenersi tanto i soggetti promotori delle sperimentazioni quanto i centri individuati per la sperimentazione medesima. Le stesse vengono fatte proprie dal Titolare quale policy aziendale nei trattamenti di dati personali e da intendersi parte integrante del presente documento, in quanto compatibili con la vigente normativa.

In particolare occorre precisare che tutti i Dipendenti coinvolti, a vario titolo, in una sperimentazione devono essere autorizzati ad utilizzare i dati dei pazienti arruolati attraverso una designazione in qualità di autorizzati al trattamento, effettuata ai sensi della vigente normativa e secondo le indicazioni di cui al presente documento.
Quindi, si prevede che le nomine degli autorizzati al trattamento, effettuate secondo i modelli di nomina di cui agli **allegati 15, 16, 17, ed P** al presente documento, siano valide anche come designazioni per il trattamento di dati personali e particolari effettuate nell'ambito delle sperimentazioni cliniche.

Si richiama inoltre il **VADEMECUM SPERIMENTAZIONI CLINICHE A NORMA PRIVACY (ALLEGATO B).**

11. CUP REGIONALE

A partire dal 1/06/2014 è stato implementato sulle postazioni informatiche degli sportelli CUP/Anagrafe sanitaria/Sportelli Unici Distrettuali un programma per la raccolta, gestione ed archiviazione informatizzata dei consensi al trattamento dei dati personali rilasciati dai cittadini/utenti dell'Azienda.
Tale applicativo consentiva la gestione informatizzata dei consensi non solo a livello aziendale ma anche a livello regionale, sulla base di informativa che viene resa attualmente all'utenza ai sensi del TU Privacy, condivisa da tutte le aziende sanitarie ed ospedaliere regionali, ad eccezione dell'Istituto Giannina Gaslini, e allegata al presente documento nella versione attualmente concordata a livello regionale **(ALLEGATO 12)** ed ancora non implementata nel software regionale essendo in corso la sua ulteriore revisione a seguito dell'entrata in vigore del D.lgs. 101/2018.

Come precisato dai "Chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario" intervenuti con Provvedimento dell'Autorità Garante per la protezione dei dati personali n. 55 del 07.03.2019, i dati personali, anche particolari dell'interessato possono ora peraltro essere trattati senza uno specifico consenso dello stesso per finalità di cura e strettamente correlate.
In presenza di trattamenti di interesse regionale (come nel caso di specie) A.S.L. 3 utilizza il modello di informativa ed eventuale raccolta consenso, laddove previsto dalla vigente normativa, predisposto a livello regionale, anche sulle basi delle indicazioni di A.Li.Sa. ex L.R. n.17 del 29.7.2016 e s.m.i. , così come può elaborare informative integrative aziendali per specifici trattamenti, nonché informative semplificate.

12. PUBBLICAZIONE PROVVEDIMENTI SUL SITO INTERNET AZIENDALE PER FINALITA' DI TRASPARENZA E PER ALTRE FINALITA'

L'Azienda, in virtù delle disposizioni in materia di trasparenza contenute nel Decreto Legislativo 14 marzo 2013 n. 33 e s.m.i., cosi come modificato dal Decreto Legislativo 25 maggio 2016 n. 97 e s.m.i., ha l'obbligo di pubblicare una serie di provvedimenti che possono contenere anche dati personali e sensibili dei soggetti destinatari dei provvedimenti o di soggetti terzi.
A questi obblighi di pubblicazione continuano ad affiancarsi altri obblighi di pubblicità c.d. "on line" di provvedimenti contenuti in diverse disposizioni di settore, diverse da quelle in materia di trasparenza, tra cui quelli atti a garantire la pubblicità legale degli atti amministrativi, determinando anch'essi una possibile diffusione di dati personali.
Pertanto, al fine di contemperare le esigenze di pubblicità e trasparenza con i diritti alla riservatezza dei dati e delle informazioni ricompresi nei suddetti provvedimenti, l'Autorità Garante per la protezione dei dati personali, con il provvedimento n. 243 del 15 maggio 2014 avena emanato le "Linee guida in materia di trattamento di dati personali, contenuti in atti e

documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati". Dette Linee guida vengono fatte proprie dal Titolare quali policy aziendali, in quanto compatibili con la vigente normativa.
Le suddette linee guida, contengono una serie di indicazioni a cui attenersi nel momento in cui vengono redatti gli atti che saranno oggetto di pubblicazione nel rispetto delle normative citate.
Di seguito vengono riportati i principali accorgimenti da seguire nella redazione e nella pubblicazione dei provvedimenti in argomento.
Dal maggio 2018 la gestione del procedimento di adozione e pubblicazione delle deliberazioni e determinazioni aziendali è completamente informatizzato, strutturato nel rispetto delle garanzie di protezione dei dati personali ed utilizzabile tramite credenziali di accesso differenziate da parte dei dipendenti autorizzati al relativo trattamento, come da manuale operativo pubblicato sul sito intranet aziendale.

12 a) Pubblicazioni per finalità di trasparenza

Il Decreto Legislativo 14 marzo 2013 n. 33 e s.m.i. ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzione di dati, informazioni, atti e documenti sui siti web istituzionali dei soggetti obbligati, precisando che "oggetto del decreto" è l'individuazione degli obblighi di trasparenza "concernenti l'organizzazione e l'attività delle pubbliche amministrazioni".

Il riferimento è, pertanto, limitato agli "obblighi di pubblicazione concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" contenuti, oltre che nel D.lgs. n. 33/2013 e s.m.i, anche in altre disposizioni normative aventi analoga finalità di trasparenza, con esclusione degli obblighi di pubblicazione aventi finalità diverse, quali ad esempio gli obblighi di pubblicazione a fini di pubblicità legale. I principi e la disciplina di protezione dei dati personali devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.

Pertanto, prima di mettere a disposizione sul sito web istituzionale informazioni, atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, occorre verificare che la normativa in materia di trasparenza preveda tale obbligo. Laddove si riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni. È, quindi, consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto, nel rispetto del cd. "principio di pertinenza e non eccedenza" , adeguatezza, liceità e correttezza , di cui alla normativa vigente in materia di privacy.

È, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute". In particolare è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Il procedimento di selezione dei dati personali che possono essere resi conoscibili online deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni siano relative ad altri dati sensibili o a dati giudiziari. A titolo di esempio si citano quelli idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, l'adesione a partiti e a sindacati oppure quelli idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonché la qualità di imputato o di indagato.

Le suddette informazioni possono, quindi, non essere riportate nel testo dei provvedimenti da pubblicare sul sito Internet aziendale (ad esempio nell'oggetto, nel contenuto, etc.), ma citate solo negli atti a disposizione degli uffici (richiamati quale presupposto del provvedimento). Altro utile accorgimento può essere quello di indicare delicate situazioni di disagio personale (ad esempio sociale, economico o legale) solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici.

L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo "procedendo alla c.d. *anonimizzazione* dei dati personali eventualmente presenti. In proposito, si evidenzia che sostituire il nome e cognome con le iniziali del soggetto interessato dal provvedimento potrebbe non essere sufficiente ad anonimizzare i dati personali, laddove accanto alle iniziali del nome e cognome permangano ulteriori informazioni di contesto che rendono, comunque, identificabile l'interessato (quali ad esempio la residenza, il domicilio, il luogo di lavoro, il numero di telefono, la data di nascita oppure la complessiva vicenda oggetto di pubblicazione sufficiente a individuare univocamente la persona cui le stesse si riferiscono).

Con riferimento ad alcuni specifici obblighi di pubblicazione le linee guida del Garante forniscono tra le altre le seguenti indicazioni:

- *curricula professionali*

l'obbligo di pubblicazione del curriculum comporta di dover operare un'attenta selezione dei dati in essi contenuti, se del caso predisponendo modelli omogenei ed impartendo opportune istruzioni agli interessati (che, in concreto, possono essere chiamati a predisporre il proprio curriculum in vista della sua pubblicazione per le menzionate finalità di trasparenza). In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative (ad esempio, gli incarichi ricoperti), nonché ulteriori informazioni di carattere professionale (si pensi alle conoscenze linguistiche oppure alle competenze nell'uso delle tecnologie, come pure alla partecipazione a convegni e seminari oppure alla redazione di pubblicazioni da parte dell'interessato). Non devono formare invece oggetto di pubblicazione dati eccedenti, quali, ad

esempio, i recapiti personali oppure il codice fiscale degli interessati, ciò anche al fine di ridurre il rischio di c.d. furti di identità.

- *corrispettivi e compensi*

l'entità di corrispettivi e compensi percepiti da alcune tipologie di soggetti è oggetto di pubblicazione secondo le modalità previste dal D.lgs. n. 33/2013 e s.m.i. Tra questi ultimi sono annoverati, ad esempio, i titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza, nonché i dipendenti pubblici cui siano stati conferiti o autorizzati incarichi

Ai fini dell'adempimento degli obblighi di pubblicazione, risulta proporzionato indicare il compenso complessivo percepito dai singoli soggetti interessati, determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione. Non appare, invece, giustificato riprodurre sul web la versione integrale di documenti contabili, i dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun Dipendente e/o assimilato, come pure l'indicazione di altri dati eccedenti riferiti a percettori di somme quali, ad esempio, i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti).

- *provvedimenti amministrativi*

I provvedimenti e le determinazioni rimarranno pubblicati all'albo on line dell'Azienda per i termini di legge previsti per la relativa pubblicità, decorsi i quali rimarrà solo l'indicazione del numero, data di adozione ed oggetto degli stessi.

- *atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici di importo superiore ai mille euro ed elenco dei soggetti beneficiari*

Per le predette pubblicazioni è prevista l'indicazione delle seguenti informazioni: a) il nome dell'impresa o dell'ente e i rispettivi dati fiscali o il nome di altro soggetto beneficiario; b) l'importo del vantaggio economico corrisposto; c) la norma o il titolo a base dell'attribuzione; d)l'ufficio e il funzionario o dirigente responsabile del relativo procedimento amministrativo; e) la modalità seguita per l'individuazione del beneficiario; f) il link al progetto selezionato ed al curriculum del soggetto incaricato.

Non possono, invece, essere pubblicati i dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici, nonché gli elenchi dei relativi destinatari:

a) di importo complessivo inferiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario;

b) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute (ad esempio indicazioni quale "erogazione ai sensi della legge 104/1992");

c) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario, qualora da tali dati sia possibile ricavare informazioni relative alla situazione di disagio economico-sociale.

Non risulta inoltre giustificato diffondere dati quali, ad esempio, l'indirizzo di abitazione o la residenza, il codice fiscale di persone fisiche, le coordinate bancarie dove sono accreditati i contributi od i benefici economici (codici IBAN), la ripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente-Isee, l'indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative, etc.

12 b) Pubblicazioni per altre finalità

Anche per quanto attiene alle pubblicazioni "on line" per altre finalità, prima di mettere a disposizione sul sito internet aziendale atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, occorre verificare se la normativa di settore preveda espressamente tale obbligo e la relativa durata e laddove si riscontri l'esistenza di tale obbligo normativo è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni soprattutto ove si riscontri la presenza di dati sensibili e giudiziari.

Di seguito si riportano alcune fattispecie esplicative.

- *Pubblicazioni all'albo aziendale on line*

I provvedimenti aziendali (deliberazioni e determinazioni dirigenziali, bandi, atti dispositivi e altre tipologie di atti) sono pubblicati in forma integrale per un periodo di 15 giorni consecutivi dalla data di approvazione del medesimo o per un periodo di tempo superiore se espressamente previsto da una specifica norma di settore, a meno che non sia esclusa la pubblicazione all'albo on line per ragioni di riservatezza. In questo caso il provvedimento dovrà riportare l'indicazione *"nel rispetto della vigente normativa in materia di privacy il presente provvedimento non verrà pubblicato".*

Inoltre, anche alle pubblicazioni nell'albo online si applicano tutti i limiti già indicati per le pubblicazioni per finalità di trasparenza (divieto di diffusione di dati idonei a rivelare lo stato di salute e cautele per gli altri dati sensibili e giudiziari; nonché divieto di diffondere dati personali non necessari, non pertinenti o eccedenti).

Una volta trascorso il periodo temporale previsto dalle singole discipline per la pubblicazione nell'albo pretorio, i documenti e gli atti non sono più visionabili integralmente, rimanendo pubblicato all'albo aziendale on line soltanto l'oggetto ed il numero e data di adozione.

Ciò, salvo che gli stessi atti e documenti non debbano essere pubblicati in ottemperanza agli obblighi in materia di trasparenza, in apposita sezione del sito denominata "Amministrazione Trasparente".

- *Graduatorie*

Con riguardo alla pubblicità degli esiti delle prove concorsuali e delle graduatorie finali – nonché, nei casi (e con le modalità) previsti, dei risultati di prove intermedie – di concorsi e selezioni pubbliche e di altri procedimenti che prevedono la formazione di graduatorie devono essere diffusi i soli dati pertinenti e non eccedenti riferiti agli interessati. Non possono, quindi, formare oggetto di pubblicazione dati concernenti i recapiti degli interessati (utenze di telefonia fissa o mobile, l'indirizzo di residenza o di posta elettronica, il codice fiscale, l'indicatore Isee, il numero di figli disabili, i risultati di test psicoattitudinali, né quelli concernenti le condizioni di salute degli interessati, ivi compresi i riferimenti a condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Per ogni altra disposizione in materia di pubblicazione di provvedimenti aziendali sul sito internet dell'Azienda si rimanda alle linee guida dell'Autorità garante per la protezione dei dati personali, pubblicato sulla rete Intranet aziendale, nella sezione "Normativa-Privacy", fatti propri dal titolare quale policy di sicurezza nei trattamenti di dati personali e da intendersi parte integrante del presente documento, in quanto compatibili con la vigente normativa.

13. TRATTAMENTO DEI DATI TRAMITE DOSSIER SANITARIO ELETTRONICO ED FSE

L'Autorità Garante per la protezione dei dati personali, con il **provvedimento n. 331 del 4 giugno 2015** aveva emanato le **"Linee guida in materia di dossier sanitario",** delineando un quadro di riferimento unitario per disciplinare i trattamenti di dati tramite l'utilizzo dei dossier sanitari, che vengono fatte proprie dal Titolare quali policy aziendali, per quanto conformi alla vigente normativa.

In considerazione di tale provvedimento l'Azienda ha intrapreso un percorso al fine di allineare le proprie procedure alle recenti linee guida in argomento, che ha determinato la predisposizione di una informativa specifica in materia di trattamento dei dati tramite dossier sanitario **(Allegato L),** del modello di acquisizione del consenso per la costituzione del dossier **(Allegato M)**, del modello per la richiesta di oscuramento dell'evento clinico **(Allegato N),** del modello per la richiesta di revoca (**Allegato O**), nonché la predisposizione di un portale aziendale per la raccolta e gestione del consenso informatizzato, che è stato implementato a partire dal mese di ottobre 2016. In parallelo sono iniziati i corsi di formazione per il personale Dipendente e/o assimilato autorizzato all'utilizzo del dossier sanitario elettronico, corsi che prevedono una parte di Formazione A Distanza (FAD) ed una parte informatico – operativa in aula. I dipendenti che accederanno al dossier sanitario elettronico dovranno essere individuati quali autorizzati al

trattamento dei dati, utilizzando il modello allegato al presente documento **(Allegato P),** che andrà ad integrare l'autorizzazione conferita con il modello "**Allegato 15**"**.**

Il FSE, istituito dalla Regione Liguria nel rispetto della normativa vigente in materia di protezione dei dati personali, è l'insieme dei dati e dei documenti digitali di tipo sanitario e sociosanitario, generati da eventi clinici presenti e trascorsi, che riguardano l'assistito.

Pertanto il FSE, previo specifico consenso acquisito previa specifica informativa regionale, sulla base delle linee guida del Garante Privacy fatte proprie, in quanto compatibili con la normativa vigente, quali policy regionali ed aziendali, verrà alimentato in maniera continuativa dai soggetti che di volta in volta prenderanno in cura l'utente, anche fuori dalla Regione Liguria, nell'ambito del Servizio Sanitario Nazionale (SSN) e dei Servizi sociosanitari regionali. Previo ulteriore e specifico consenso il FSE potrà essere alimentato anche con i dati ed i documenti digitali, relativi ad eventi di tipo sanitario e sociosanitario pregressi (cioè prima dell'attivazione del FSE) che riguardano l'utente.

Per quel che riguarda ASL 3, l'Azienda si limita a contribuire all'alimentazione del FSE attualmente con i referti di radiologia e laboratorio firmati digitalmente ed in formato strutturato e prossimamente con le lettere di dimissione, verbali di pronto e referti visita specialistica, come da indicazioni del **Titolare regionale** del FSE.

Per ulteriori specifiche **informative** si rimanda al sito regionale **www.fascicolosanitario.liguria.it,** in corso di aggiornamento a livello regionale (A.Li.Sa. ex LR 17/2016).

14. VALUTAZIONE D'IMPATTO (DPIA)

L'Art. 35 GDPR – Regolamento Generale sulla Protezione dei Dati (UE 679/2016) disciplina la "Valutazione d'impatto sulla protezione dei dati".

"1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.".

In punto il Titolare fa propria quale policy di sicurezza nei trattamenti di dati personali e da intendersi parte integrante del presente documento la "WP 248 -linee guida concernenti la valutazione di impatto sulla protezione dei dati 4.10.2017" e le indicazioni dell'Autorità Garante per la Privacy (sito www.cnil.fr: **https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil**).

I parametri utilizzabili per la valutazione possono essere a titolo esemplificativo:

Contesto: trattamento in considerazione; responsabilità legate al trattamento; standard applicabili al trattamento; dati, processi e risorse di supporto (quali dati sono trattati es. dati personali-identificativi e di contatto-di utenti e terzi, dati particolari es. stato di salute, dati genetici, convinzioni religiose; com'è il ciclo di vita del trattamento dei dati: es. come vengono raccolti e trattati ed archiviati; quali sono le risorse di supporto ai dati: es. archivi, applicativi etc.).

Principi fondamentali: proporzionalità, necessità (es. gli scopi del trattamento sono specifici, espliciti e legittimi e quali sono; quali sono le basi legali che rendono il trattamento legittimo; i dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati-minimizzazione dei dati; i dati raccolti sono accurati e mantenuti aggiornati; qual è la durata della conservazione dei dati).

Controlli per proteggere i diritti personali dei soggetti interessati (es. come sono informati del trattamento i soggetti interessati; come si ottiene il consenso dei soggetti interessati; come esercitano i loro diritti di accesso alla portabilità dei dati i soggetti interessati; come esercitano i loro diritti alla rettifica ed alla cancellazione dei dati i soggetti interessati; come

esercitano i loro diritti di restrizione ed obiezione i soggetti interessati; gli obblighi dei responsabili esterni del trattamento sono chiaramente identificati e governati da un contratto; nel caso di trasferimento di dati fuori dall'Unione Europea i dati sono adeguatamente protetti).

Controlli esistenti o pianificati (es. Policy aziendale di gestione dati).

Accesso illegittimo ai dati (es. Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare; quali sono le principali minacce che potrebbero concretizzare il rischio; quali sono le fonti di rischio; quali dei controlli identificati contribuiscono a gestire il rischio; come si può stimare la gravità del rischio, specialmente riguardo i potenziali impatti ed i controlli pianificati; e riguardo le minacce, fonti di rischio ed i controlli pianificati).

Modifiche indesiderate di dati (es. quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare; quali sono le principali minacce che potrebbero concretizzare il rischio; quali sono le fonti di rischio; quali dei controlli identificati contribuiscono a gestire il rischio; come si può stimare la gravità del rischio, specialmente riguardo i potenziali impatti ed i controlli pianificati; e riguardo le minacce, fonti di rischio ed i controlli pianificati).

Scomparsa dati (es. quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare; quali sono le principali minacce che potrebbero concretizzare il rischio; quali sono le fonti di rischio; quali dei controlli identificati contribuiscono a gestire il rischio; come si può stimare la gravità del rischio, specialmente riguardo i potenziali impatti ed i controlli pianificati; e riguardo le minacce, fonti di rischio ed i controlli pianificati).

Piano d'Azione (es. Principi fondamentali; Controlli esistenti o pianificati; Rischi, etc.).

Alla valutazione d'impatto, nei casi previsti e con le modalità previste dal presente documento e dalla normativa vigente, deve procedere preventivamente il Dirigente competente per materia, con il supporto eventuale del Referente privacy.

15. AGGIORNAMENTO PERIODICO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente Documento Programmatico sulla Sicurezza è sottoposto, di norma, ad aggiornamento triennale, a decorrere dal 2021.
Poiché l'organizzazione aziendale è in corso di completa revisione, come da nuovo atto di autonomia aziendale adottato con deliberazione n°239 del 19.4.2018 e sue successive modifiche, la

cui piena efficacia è ancora in corso, vi potrà essere la necessità di revisione, prima di detto termine, in base al nuovo assetto organizzativo, delle denominazioni delle strutture preposte ai trattamenti ed alle funzioni evidenziate dal presente D.P.S.. Parimenti potranno essere necessari aggiornamenti in relazione alla sopravvenuta normativa nazionale di armonizzazione al Regolamento U.E. 679/2016 ed a indicazioni regionali sopravvenute.