A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 728 del 28/08/2025

Oggetto: AGGIORNAMENTO MANUALE PER LA SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI APPROVATO CON DELIBERAZIONE N. 1209 DEL 31/12/2018 ED AGGIORNAMENTO GRUPPO PRIVACY COSTITUITO CON DELIBERAZIONE N. 743 DEL 26/7/2018 .

DIRETTORE GENERALE - DOTT. FRANCESCO CATTEL
(NOMINATO CON DGR N. 25-655/2024/XII DEL 23/12/2024)

DIRETTORE AMMINISTRATIVO - DOTT.SSA BARBARA BUONO

DIRETTORE SANITARIO - DOTT.SSA DANIELA KOZEL

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

DELIBERAZIONE DEL DIRETTORE GENERALE

Struttura proponente: AFFARI GENERALI LEGALI E ISTITUZIONALI

L'estensore dell'atto: Motetta Emanuela
Il Responsabile del procedimento: Primatesta Giuseppina
Il Dirigente/Funzionario: Primatesta Giuseppina
Il funzionario incaricato alla pubblicazione.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

IL DIRETTORE GENERALE

Nella data sopraindicata, su proposta istruttoria del Direttore SOC Affari Generali Legali e Istituzionali – SOS Organi Organismi Collegiali Supporto Strategico - di seguito riportata, in conformità al Regolamento approvato con delibera n. 290 del 12/05/2017 e modificato con delibere n. 65 del 28/01/2020 e n. 555 del 25/06/2025.

"PREMESSO CHE

- il Parlamento europeo ed il Consiglio, in data 27 aprile 2016, hanno approvato il Regolamento UE 679/2016 (GDPR - General Data Protection Regulation), in vigore dal 25/05/2018, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abrogando la direttiva 95/46/CE e mirando a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

- il D.lgs n. 101 del 10 agosto 2018 ha adeguato la normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

DATO ATTO CHE le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del quadro normativo in materia di privacy.

RILEVATO CHE ASL VCO, in qualità di "Titolare del Trattamento", si è dotata di una propria organizzazione interna, al fine di adeguare il proprio "sistema privacy" alla normativa comunitaria .

VISTE

- la deliberazione D.G. n. 743 del 26/7/2018, con la quale, in attesa della formalizzazione degli atti interni di adeguamento al GDPR, venivano adottati provvedimenti transitori e veniva costituito il Gruppo Privacy aziendale, composto dai Direttori delle SOC Affari Generali Legali e Istituzionali, Logistica e Servizi Tecnici e Informatici, Direzione Sanitaria PP.OO. Verbania e Domodossola, Distretto, e dal Direttore del Dipartimento di Prevenzione, con facoltà di integrazione di altre figure professionali;

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

- la deliberazione D.G. n. 1209 del 31/12/2018 con la quale, in fase di prima applicazione del GDPR, veniva adottato il *Manuale per la sicurezza del trattamento dei dati personali* che aggiornava quello precedentemente approvato con deliberazione D.G. n. 738/2005;

- la determinazione dirigenziale SOC Logistica e Servizi Informatici n. 276 del 25/02/2025, con la quale è stato rinnovato il servizio di Responsabile della Protezione dei Dati (DPO), ai sensi dell'art. 37 del Regolamento UE 2016/679 (GDPR), nei confronti della società Global Com Technologies Srl, sino al 30/09/2026.

PRECISATO CHE che, nell'organigramma allegato all'Atto Aziendale vigente, approvato con deliberazione DG n. 602 del 18/08/2022, è presente la Funzione "Corruzione/Trasparenza/Privacy", collocata nell'ambito della SOC Affari Generali Legali e Istituzionali, in staff alla Direzione Generale, a cui afferisce il Referente Privacy aziendale.

PRESO ATTO CHE, a seguito dell'attività di revisione ed aggiornamento della Regolamentazione aziendale in tema di privacy, svolta dalla Funzione Privacy con il supporto del Responsabile della Protezione Dati, sono state recentemente adottate le seguenti deliberazioni:

- n. 643 del 28/7/2025, avente per oggetto: "Approvazione procedura per la gestione delle nomine dei Responsabili del Trattamento dei dati personali ai sensi dell'art. 28 del GDPR 2016/679;

- n. 646 del 28/7/225, avente per oggetto: "Approvazione modello organizzativo privacy per la gestione dei ruoli nel trattamento dati in applicazione del Regolamento UE 2016/679 (GDPR) e D.LGS. 101/2018;

- n. 683 del 7/8/2025, avente per oggetto: "Aggiornamento procedura per la gestione delle segnalazioni di violazione dei dati (Data Breach)".

DATO ATTO CHE , in considerazione degli aggiornamenti al sistema organizzativo privacy apportati con gli atti sopra citati, nonché delle modifiche organizzative e normative intervenute, occorre provvedere altresì alla revisione del *Manuale per la sicurezza del trattamento dei dati personali* di cui a precedente deliberazione DG n. 1209/2018.

EVIDENZIATO CHE, la Funzione Privacy Aziendale ha provveduto ad effettuare la revisione di tale Regolamento, inserendo altresì, all'art. 7.7 del documento (Ruoli privacy), la nuova composizione del Gruppo Privacy, nel quale vengono coinvolte le seguenti ulteriori professionalità: Referente Privacy, Responsabile SOS Supporto legale e assicurazioni, Responsabile SOS ICT, Responsabile SOS Tecnico e Coordinamento aziendale Nuovo Ospedale (in particolare per il settore Ingegneria Clinica).

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

Il Gruppo Privacy potrà inoltre essere integrato da altre figure professionali o altri Direttori/Responsabili di struttura, nonché dal Responsabile della Protezione Dati, qualora se ne ravvisi la necessità ed in base agli argomenti trattati.

RILEVATO CHE il Regolamento in oggetto è stato sottoposto alla valutazione del Responsabile della Protezione Dati, il quale in data 21/08/2025 ha comunicato le modifiche da apportare, che sono state recepite nel documento finale.

PROPONE PERTANTO di procedere alla formalizzazione del nuovo *Manuale per la sicurezza del Trattamento dei dati personali*, che viene allegato alla presente deliberazione quale parte integrante e sostanziale sotto la lettera A), provvedendo altresì alla revoca della deliberazione D.G. n. 743 del 26/7/2028".

Condivisa la proposta come sopra formulata e ritenendo sussistere le condizioni per l'assunzione della presente delibera.

Acquisiti i pareri favorevoli espressi ai sensi dell'art. 3 del d.Lgs. 502/1992 e smi, come formulati nel frontespizio del presente atto

DELIBERA

1°) Di revocare la deliberazione DG n. 743 del 26/7/2018, con la quale, in attesa della formalizzazione degli atti di adeguamento al GDPR, venivano adottati provvedimenti transitori e costituito il Gruppo Privacy aziendale.

2°) Di approvare il nuovo *Manuale per la sicurezza del trattamento dei dati personali,* che viene allegato alla presente deliberazione quale parte integrante e sostanziale sotto la lettera A), al quale risultano uniti i seguenti allegati:

1) Informativa generale sul trattamento dei dati personali
2) Informativa breve sul trattamento dei dati personali
3) Informativa sul trattamento dei dati in ambito sanitario
4) Piano per la sicurezza del sistema di gestione informatica dei documenti
5) Procedura gestione delle segnalazioni di violazioni di dati personali (del.683/2025)

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

3°) Di dare atto che il Gruppo Privacy, così come ridefinito all'art. 7.7 dell'allegato A) alla presente deliberazione, risulta così composto:

- Direttore SOC Affari Generali legali e istituzionali
- Referente Privacy
- Responsabile SOS Contenzioso e supporto Legale – Assicurazioni
- Direttore SOC Logistica e Servizi Informatici
- Responsabile SOS ICT
- Responsabile SOS Tecnico e Coordinamento Aziendale Nuovo Ospedale
- Direttore SOC Direzione Sanitaria Presidi Ospedalieri Verbania e Domodossola
- Direttore SOC Distretto
- Direttore Dipartimento di Prevenzione

Il Gruppo potrà essere integrato da altre figure professionali o altri Direttori/Responsabili di struttura, nonché dal Responsabile della Protezione Dati, qualora se ne ravvisi la necessità ed in base agli argomenti trattati.

L'attività di segreteria e coordinamento viene svolta dal Collaboratore Amministrativo afferente alla funzione Privacy aziendale.

4°) Di dare atto che il Manuale adottato con la presente deliberazione aggiorna e sostituisce quello precedentemente approvato con deliberazione DG n. 1209/2018.

5°) Di notificare il presente atto a tutte le strutture aziendali.

6°) Di disporre, a cura della Funzione Privacy aziendale, la pubblicazione del presente atto, nella sezione Amministrazione Trasparente del sito internet aziendale, nonché nell'area intranet - sezione Privacy.

7°) Di dare atto che il presente provvedimento non comporta alcun onere di spesa a carico del bilancio dell'Azienda.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Allegato A)

MANUALE PER LA SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI

rev. agosto 2025

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

Indice

ART. 1 - PRINCIPI GENERALI

1.1 Il presente Manuale contiene disposizioni attuative del Regolamento UE 2016/679 (nel prosieguo "GDPR") e del D.lgs. n. 196/2003, così come emendato dal D.lgs. 101/2018 (Codice Privacy) nell'ambito delle strutture dell'Azienda Sanitaria Locale V.C.O, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda medesima.

L'Azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi degli artt. 15 e ss del GDPR.

1.2 Ai fini del presente manuale si applicano le definizioni elencate nell'art. 4 del Reg. UE 2016/679, e qui di seguito riportate:

a) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
b) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
c) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

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

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

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

h) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

i) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

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

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

l) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

m) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

n) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

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

p) «stabilimento principale»:

- per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

-con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

q) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

r) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

s) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

t) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

u) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

v) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
-il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
- oppure un reclamo è stato proposto a tale autorità di controllo;

w) «trattamento transfrontaliero»:
-trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
- trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

x) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

y) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

z) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

1.3 Ai fini del presente manuale inoltre si definiscono

i) «Designato»: la persona fisica esplicitamente nominata per iscritto dal titolare ad assolvere a specifici compiti e funzioni connessi al trattamento di dati personali sotto la responsabilità e nell'ambito del proprio assetto organizzativo del titolare stesso, ai sensi dell'art. 2-quaterdecies Codice Privacy;

ii) «autorizzato del trattamento»: la persona fisica autorizzata a compiere operazioni di trattamento dati personali dal soggetto Designato;

iii) «dati comuni» i dati personali non rientranti nelle categorie di cui agli artt. 9 e 10 GDPR;

1.4 Ai fini del presente manuale inoltre l'espressione "Dati Particolari", si intende riferita, alle categorie di dati di cui all'articolo 9 del GDPR e ai dati di cui all'articolo 10 del medesimo regolamento.

ART. 2 - TRATTAMENTO DEI DATI PERSONALI

Con l'espressione "trattamento", ai sensi dell'art. 4, punto 2 del GDPR, deve intendersi qualunque operazione o complesso di operazioni effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Qualunque trattamento di dati personali da parte dell'Azienda è consentito soltanto per lo svolgimento delle funzioni istituzionali (artt. 2-ter e 2-sexies Codice Privacy), al fine di adempiere a compiti ad essa attribuiti da leggi e regolamenti.
E' possibile effettuare trattamenti relativi a dati diversi da quelli particolari anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente, fermo restando l'esercizio di funzioni istituzionali.
Il trattamento delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, ai sensi e per gli effetti di cui all'art. 2-sexies, comma 1 del Codice Privacy.

ART. 3 – PRINCIPI E CRITERI PER L'ESECUZIONE DEL TRATTAMENTO DEI DATI PERSONALI

Ogni trattamento di dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto di ogni tipo di trattamento dovranno essere i soli dati essenziali per lo svolgimento delle attività istituzionali.
Ai sensi dell'art. 5 GDPR, i dati personali devono:

- essere trattati in modo lecito e corretto e trasparente nei confronti dell'interessato (*«liceità, correttezza e trasparenza»);*
- essere raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi *(«limitazione della finalità»);*
- essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (*«minimizzazione dei dati»)*;
- essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati *(«esattezza»);*
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati

esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato *(«limitazione della conservazione»);*

- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali *(«integrità e riservatezza»).*

Il titolare del trattamento è competente per il rispetto dei principi sopra elencati e in grado di comprovarlo *(«responsabilizzazione»).*

Il titolare del trattamento, nel pieno rispetto del principio di responsabilizzazione ("accountability") di cui all'articolo 5, paragrafo 2, del Regolamento UE 2016/679, si impegna al rispetto di tutto quanto sopra riportato – assicurando peraltro di poterne fornire dimostrazione, ove richiesto.
Inoltre, gli adempimenti di cui al presente documento mettono il titolare del trattamento in condizione di garantire il pieno rispetto dei principi di privacy by design e by default – definiti all'art. 25 del GDPR, il quale prescrive quanto di seguito riportato:
"*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica".

ART. 4 - CONSENSO AL TRATTAMENTO DEI DATI – BASI GIURIDICHE DEL TRATTAMENTO

4.1 Ai sensi dell'art. 6 del DGPR (*Liceità del Trattamento)* :

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Nel caso in cui il trattamento trovi base giuridica nel consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato abbia prestato il proprio consenso al trattamento dei propri dati personali. Se tale consenso è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Per quanto riguarda il consenso per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali ("finalità di cura") il Provvedimento dell'Autorità Garante per la protezione dei dati personali del 7 marzo 2019, ha fornito esplicito chiarimento rispetto all'applicazione della disciplina della protezione dei dati in ambito sanitario, confermando che il professionista sanitario soggetto al segreto professionale o altra persona anch'essa soggetta all'obbligo di riservatezza, non devono più richiedere il consenso al paziente per i trattamenti necessari alla cura, indipendentemente dalla circostanza che operi in qualità di libero professionista ovvero all'interno di una struttura sanitaria pubblica o privata.

ART. 5 - DATI GENETICI

Il trattamento dei dati genetici è consentito, previo consenso dell'interessato, nei soli casi previsti dall'articolo 9, paragrafo 2 del GDPR e dalle misure di garanzia approvate dal Garante in attuazione dell'art. 2-septies del Codice.
I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti e accessibili ai soli soggetti autorizzati al trattamento.
Il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti.

ART. 6 - INFORMATIVA

L'informativa è l'elemento necessario e fondamentale per la liceità di ogni forma di trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività specifiche che sono poste in essere.
L'interessato deve essere informato, eventualmente integrando l'informativa scritta con chiarimenti orali, prima del trattamento ed in ogni caso al momento della raccolta dati.
E' comunque opportuno che l'informativa venga data per iscritto. Nei casi di urgenza, per finalità mediche, potrà essere data successivamente al momento in cui è stata data l'informativa orale.
L'informativa deve contenere ai sensi dell'art. 13 del GDPR:

1. i riferimenti all'Azienda, in qualità di titolare del trattamento;
2. i dati di contatto del responsabile della protezione dei dati;
3. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
4. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali ai quali i dati possono essere comunicati, o che possono venirne a conoscenza in qualità di Preposti al trattamento o di Persone autorizzate al trattamento dei dati personali;
5. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
6. l'indicazione dei diritti richiamati all'art. 12 del presente manuale;

7. l'eventuale indicazione per l'interessato dei casi in cui è previsto l'obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli;
8. l'eventuale previsione di trasferimento dei dati personali all'esterno dell'Unione Europea o verso Organizzazioni Internazionali, indicando altresì la misura organizzativa, tra quelle costituenti base valida di liceità del trasferimento, atta a prevenirne il trasferimento illecito.
9. l'indicazione dell'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Quando i dati personali non sono raccolti presso l'interessato, ai sensi dell'art. 14 Reg. UE. 2016/679, l'informativa è data al medesimo interessato entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese; quando è prevista la loro comunicazione, non oltre la prima comunicazione. L'informativa, se i dati sono raccolti presso terzi (ad esempio presso un'altra amministrazione pubblica), non è dovuta nel caso in cui :
- l'interessato disponga già delle informazioni;
-la registrazione o la comunicazione dei dati personali siano previste per legge dal diritto dell'Unione Europea o dello Stato membro in cui è soggetto il titolare del trattamento, ivi inclusi i casi in cui i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge;
- informare l'interessato si riveli impossibile o richieda uno sforzo sproporzionato.

Si allegano al presente documento:
- l'*informativa generale* adottata dall'Azienda (All. 1)
- l'*informativa breve* (All. 2)
- l'*informativa sul trattamento dei Dati in ambito sanitario (e relativi consensi) All. 3,* fornita all'interessato al momento del ricovero nei reparti ospedalieri

L'informativa generale risulta pubblicata nella sezione web aziendale dedicata alla privacy "Dati personali".

L'informativa breve (All. 2) viene affissa presso le varie strutture aziendali (es. centri Unici di Prenotazione, DEA, Pronto Soccorso, Poliambulatori, ecc).
L'Azienda fornisce inoltre altre informative in relazione a specifici trattamenti (es. informativa fornitori, informativa dipendenti, cup telefonico, ecc.).

ART. 7 RUOLI PRIVACY DEFINITI PER L'ESECUZIONE, LA SORVEGLIANZA ED IL MONITORAGGIO DEGLI ADEMPIMENTI PRIVACY.

Visti il GDPR, il D.Lgs. 196/03 e ss.mm.ii e considerata la vigente normativa, il Titolare del Trattamento ha individuato le seguenti figure che costituiscono la parte del modello organizzativo per l'esecuzione, la sorveglianza e il monitoraggio degli adempimenti privacy:

7.1 Il Titolare del Trattamento;
7.2 I Soggetti Designati al trattamento dei dati personali;
7.3 I soggetti autorizzati al trattamento dei dati personali;
7.4 Gli Amministratori di Sistema (AdS);
7.5 I Responsabili del Trattamento dei dati personali;
7.6 Il Responsabile della Protezione Dati (RPD o DPO)
7.7 Funzione Privacy, Referente e Gruppo Aziendale Privacy

7.1. - *Il Titolare del trattamento* è il soggetto che ha il controllo sui trattamenti dei dati personali (in lingua inglese "Data Controller"). Ai sensi dell'art. 4 Definizioni, par. 7) del GDPR è definito come "La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

Il Titolare del Trattamento decide le finalità e le modalità del trattamento ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalle leggi e, comunque, dalla vigente normativa.
Il Titolare del Trattamento è l'Azienda Sanitaria Locale VCO ("ASL VCO"), in persona del legale rappresentante pro-tempore il Direttore Generale.

7.2 - *I Soggetti Designati al trattamento dei dati personali*
Il legislatore, all'art. 2-quaterdecies "Attribuzione di funzioni e compiti a soggetti designati" del Codice in materia di protezione dei dati personali, introdotto dal D.Lgs. 10 agosto 2018, n. 101 (v. art. 2, Modifiche alla parte I, titolo I, del decreto legislativo 30 giugno 2003,

n. 196), ha introdotto la figura facoltativa del "soggetto designato", prevedendo la possibilità di attribuire specifiche funzioni e compiti a soggetti designati dal titolare o dal responsabile.
Alla luce del quadro normativo sopra delineato, considerata la complessità dell'organizzazione dell'ASL VCO, in continuità con l'assetto organizzativo sin qui già progettato, il Titolare ha ritenuto opportuno attribuire specifici compiti e funzioni connesse al trattamento di dati personali a "Soggetti Designati" che rivestono un elevato grado di responsabilità ed autonomia all'interno dell'ASL VCO, al fine di poter efficacemente rispondere alle specifiche necessità operative dei servizi, in modo da rendere più tempestiva e funzionale la vigilanza sui trattamenti e sulla protezione dei dati.

Il Titolare nomina, in coerenza con l'attuale assetto organizzativo, quali Soggetti Designati al trattamento dei dati personali ai sensi dell'art. 2 – quaterdecies del D.Lgs. 196/2003 e ss.mm.ii, i Direttori/Responsabili delle SOC, SOSD, SOS in staff, nonché eventuali Funzioni in staff dalle particolarità organizzative e funzionali delle attività di competenza, non precludendo l'individuazione di altri soggetti secondo necessità.

Al fine di conferire continuità delle suddette responsabilità, la delega si estende ai dirigenti che, nel possibile periodo di vacanza del ruolo di Direttori/Responsabili titolari dell'incarico, assumano la relativa qualifica di facenti funzioni.

7.3 - *I soggetti autorizzati al trattamento dei dati personali.*
Il GDPR prevede espressamente la figura della persona autorizzata al trattamento dei dati personali all'art. 4, n. 10) del GDPR).
In ASL VCO per persona Autorizzata al trattamento dei Dati Personali si intende il personale dell'ASL VCO (nonché il personale non dipendente, es. tirocinanti, borsisti, ecc.) che, nell'espletamento delle proprie mansioni, esegue materialmente le attività che implicano un trattamento di dati personali e che ha ricevuto formale lettera di nomina in conformità agli artt. 29, 32 par. 4) del GDPR e 28 paragrafo 3 lett. B).
La nomina dei soggetti Autorizzati al Trattamento Dati è a carico del Soggetto Designato, il quale provvede agli adempimenti per la nomina del personale ricadente sotto la sua responsabilità organizzativa e istruisce gli Autorizzati assicurandosi, attraverso le attività di monitoraggio previste nei processi aziendali, che forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento.

7.4 - *Amministratori di Sistema (AdS)*

Gli Amministratori di Sistema ("AdS") sono figure previste dal Provvedimento emanato dall'Autorità Garante per la Privacy il 27 novembre 2008 dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" e pubblicato sulla Gazzetta Ufficiale del 24/12/2008 e successive modifiche ed integrazioni.

Ai sensi del Provvedimento sopra citato, gli Amministratori di Sistema sono figure professionali che in ambito informatico si occupano della gestione e della manutenzione di un impianto di elaborazione o di sue componenti con cui vengono effettuati trattamenti di Dati Personali. Vengono inoltre considerate tali anche altre figure, quali gli amministratori di basi dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

In ASL VCO, i compiti affidati all'Amministratore di Sistema, così come l'ambito di operatività di competenza sono analiticamente specificati per iscritto, in ottemperanza a quanto previsto dal Provvedimento del Garante del 27/11/2008 e ss.mm.ii. .

7.5 - *I Responsabili del Trattamento dei Dati personali*

Il Responsabile del Trattamento ai sensi dell'art. 28 del GDPR è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo (ditte/cooperative ed altri enti convenzionati) che, singolarmente o insieme ad altri, in virtù di apposito contratto di servizio, convenzione, o altro atto scritto equivalente, tratta i Dati Personali per conto del Titolare.

Qualora un Trattamento di cui è Titolare ASL VCO debba essere effettuato per suo conto da un soggetto esterno, l'Azienda ricorre a Responsabili del Trattamento sottoscrivendo apposito atto giuridico.

L'atto di nomina a Responsabile del Trattamento ex art. 28 GDPR viene sottoscritto dal Direttore/Responsabile della Struttura che gestisce il relativo contratto. Nel caso di contratti con impatto su più trattamenti di rilevanza aziendale è possibile mantenere la sottoscrizione della nomina in capo al Titolare del Trattamento.

L'azienda, con deliberazione DG N. 643 del 28/7/2025 ha predisposto apposita procedura e relativa modulistica per la gestione delle nomine dei Responsabili del trattamento dei dati personali ai sensi dell'art. 28 del GDPR 2016/679.

7.6 *Il Responsabile della Protezione Dati (RPD o DPO)*

Il responsabile della protezione dei dati, ai sensi dell'art. 39 del GDPR, è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.
Pertanto, il rispetto di tali principi non può prescindere da un'adeguata attività formativa dei soggetti che effettuano dati per conto del titolare; non ultimo, anche l'articolo 29 del GDPR chiarisce come "chiunque agisca sotto l'autorità del titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento".
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile 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;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo 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.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Il RPD/DPO per le attività di sorveglianza e di monitoraggio degli adempimenti privacy è supportato dalla Funzione Privacy di ASL VCO, che con il RPD/DPO collabora e si coordina.

Il RPD (in lingua inglese "DPO" – Data Protection Officer) svolge principalmente funzioni di informazione, consultazione, controllo, sorveglianza dell'osservanza del GDPR, in conformità a quanto disposto dagli artt. 37, 38 e 39 del GDPR e delle Linee Guida del Garante sui Responsabili della protezione dei dati del 14 Luglio 2017.

Il RPD deve assolvere i suoi compiti in autonomia e indipendenza e deve disporre di un supporto adeguato in termini di risorse finanziarie e infrastrutture.

7.7 - *Funzione Privacy, Referente e Gruppo Aziendale Privacy*

La Funzione aziendale Prevenzione Corruzione/Trasparenza/Privacy, collocata all'interno della SOC Affari Generali Legali e Istituzionali, annovera tra le sue attività quelle necessarie per supportare il Titolare nella gestione degli adempimenti privacy .

Il Referente privacy è tenuto a supportare il Titolare per la messa a regime di ogni misura che risulti necessaria e/o utile al mantenimento di un buon grado di adeguamento alle norme del Codice privacy ed alle nuove norme contenute nel GDPR.

Inoltre:

- è chiamato a coadiuvare il DPO nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali;
- concorre a promuovere l'osservanza del regolamento aziendale sulla privacy fornendo la necessaria consulenza, in stretta sinergia con il DPO, in ordine alle problematiche in tema di protezione dei dati;
- concorre ad aggiornare le iniziative di formazione interna specifica;
- cura, di concerto con il DPO, l'adeguamento del presente manuale ai provvedimenti del Garante di cui all'art. 2-septies D.lgs. 196/2003 e s.m.i.

Il Referente privacy si avvale della collaborazione del Gruppo Aziendale Privacy, gruppo di lavoro composto da diverse professionalità, portatrici di esperienza e conoscenza specifica dei vari settori di gestione aziendale e conoscenza della complessa organizzazione aziendale, nella sua interezza, e delle relazioni che intercorrono tra le diverse strutture concorrenti ai fini di sanità pubblica.

In particolare il Gruppo Privacy è composto dai Direttori/Responsabili delle seguenti strutture aziendali:

- Direttore SOC Affari Generali legali e istituzionali
- Referente Privacy
- Responsabile SOS Contenzioso e supporto Legale – Assicurazioni
- Direttore SOC Logistica e Servizi Informatici
- Responsabile SOS ICT
- Responsabile SOS Tecnico e Coordinamento Aziendale Nuovo Ospedale
- Direttore SOC Direzione Sanitaria Presidi Ospedalieri Verbania e Domodossola
- Direttore SOC Distretto
- Direttore Dipartimento di Prevenzione

L'attività di segreteria e coordinamento viene svolta dal Collaboratore Amministrativo afferente alla funzione Privacy aziendale.

Il Direttore/Responsabile di struttura, in caso di assenza o di impedimento, può individuare un delegato per partecipare agli incontri.

Il Gruppo potrà essere integrato da altre figure professionali o altri Direttori/Responsabili di struttura, nonché dal Responsabile della Protezione Dati, qualora se ne ravvisi la necessità ed in base agli argomenti trattati.

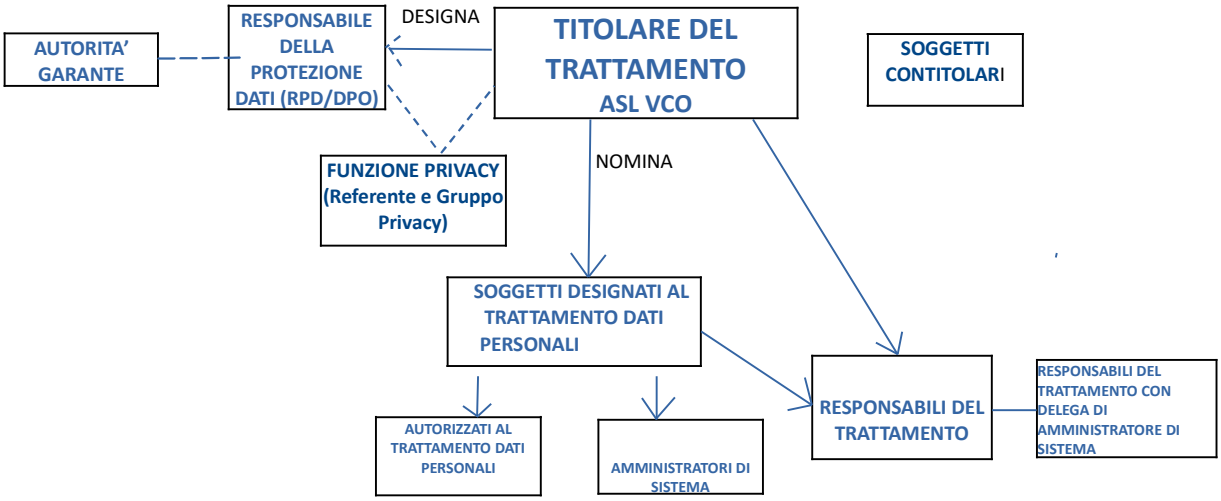
Con riferimento all'art. 7, per il dettaglio delle funzioni dei ruoli ivi indicati, si rinvia:

- alla deliberazione DG n. 646 del 28/07/2025 (*Approvazione Modello Organizzativo Privacy per la Gestione dei Ruoli nel Trattamento Dati in applicazione del Regolamento UE 2016/679 (GDPR) e D.Lgs. 101/2018*) e relativa modulistica;

- alla deliberazione D.G. n. 643 del 28/07/2025 (*Approvazione procedura per la Gestione delle Nomine dei Responsabili del Trattamento dei dati personali ai sensi dell'art. 28 del GDPR 2016/679)* e relativa modulistica.

Organigramma Data Protection

Di seguito si riporta una schematizzazione sintetica dell'*Organigramma Data Protection* che definisce i ruoli organizzativi negli scenari delle attività di trattamento effettuati dal Titolare e le relative interazioni



ART. 8 STRUTTURA AZIENDALE PER LA CYBERSICUREZZA – RESPONSABILE E REFERENTE

La Legge n. 90 del 28 giugno 2024 "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" prevede vari adempimenti in materia di cybersecurity, sia legati alla governance interna, sia in materia di obblighi di notifica degli incidenti e di verifica e correzione di vulnerabilità in alcune tipologie di software. Rientra tra questi adempimenti dotarsi di una struttura di cybersicurezza, in capo alla quale individuare un Responsabile ed un Referente per la gestione dei relativi adempimenti.

Con deliberazione DG n. 877 del 26/11/2024 questa Azienda ha provveduto ad individuare la struttura aziendale per la cybersicurezza nell'ambito della SOS Tecnologia dell'Informazione e della Comunicazione (ICT), ed il Responsabile di tale struttura quale Responsabile della Cybersicurezza.

Inoltre, nell'ambito della stessa struttura è stato individuato il Referente per la Cybersicurezza che risulta altresì ricoprire il ruolo di *Punto di Contatto* per le comunicazioni inerenti gli incidenti informatici ai sensi delle disposizioni della Direttiva UE 2022/2555 (cosiddetta Direttiva NIS 2), come recepita nel D.Lgs 138/2024 .

Il Referente ha il compito di curare l'attuazione delle disposizioni del decreto NIS 2 per conto del soggetto stesso, a partire dalla registrazione, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS.

ART. 9 - CENSIMENTO DEI TRATTAMENTI

9.1 Registro dei trattamenti

L'Azienda predispone e cura l'aggiornamento di un Registro delle Attività di Trattamento secondo il dettato dell'art. 30 GDPR il quale contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare 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 GDPR, 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 GDPR.

Inoltre, nella fattispecie dei trattamenti effettuati in qualità di responsabile del trattamento per conto di un altro titolare, l'art. 30, par. 2, del Regolamento UE 2016/679 prescrive che il cosiddetto Registro del responsabile contenga almeno:

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.

Il Registro delle Attività di Trattamento è aggiornato ai sensi dell'art. 6 ed è sottoposto a verifica periodica, con cadenza almeno annuale in sinergia con il DPO.

L'azienda gestisce il Registro dei Trattamenti con un apposito applicativo informatico (DPM - *Data Protection Manager)*.

9.2 Analisi del rischio – DPIA (Data Protection Impact Assessment)

Ai sensi dell'art. 35 del GDPR 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.
Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati.
L'Azienda, per la redazione della Valutazione di Impatto sulla protezione dei dati (o D.P.I.A Data Protection Impact Assessment), utilizza l'applicativo per la gestione degli adempimenti privacy denominato DPM (*Data Protection Manager)*.

ART. 10 - MISURE DI SICUREZZA

10.1 - Generalità
Nel sistema di gestione informatica dei documenti sono predisposte idonee misure tecniche e organizzative per garantire livelli di sicurezza e di rischio adeguati, in ottemperanza ai principi definiti dalla normativa in materia di tutela e protezione dei dati personali.

Resta inteso che i dipendenti, in quanto funzionari pubblici, sono tenuti a rispettare il segreto d'ufficio e quindi a non divulgare notizie di natura riservata, a non trarre profitto personale o a procurare danno a terzi e all'amministrazione di appartenenza dalla conoscenza di fatti e documenti riservati.

10.2 **Sicurezza dei dati e documenti informatici**

Le risorse strumentali e le procedure utilizzate per la formazione e gestione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'Ente/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il sistema di protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

Le funzionalità del protocollo informatico e dell'ambiente elaborativo garantiscono il rispetto dei requisiti di riservatezza, di integrità, di disponibilità e non ripudio, oltre a quelli sopra richiamati. I documenti informatici e i formati utilizzati per la produzione dei documenti possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto.

Con deliberazione DG n. 128 del 15/02/2024, adottata ai sensi del par. 3.5 delle Linee Guida Agid in tema di formazione, gestione e conservazione dei documenti informatici, ASL VCO ha adottato il Manuale di Gestione Documentale, che fornisce istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

10.3 Adempimenti in materia di protezione dei dati personali – Responsabili del Trattamento Dati

Nei casi in cui il trattamento viene sviluppato, per conto del Titolare, da un responsabile individuato ai sensi dell'art. 28 del Regolamento UE 679/2016 l'adozione delle misure tecniche ed organizzative è in capo anche a quest'ultimo.

I soggetti esterni a cui è delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili di trattamento ai sensi dell'art. 28 Regolamento UE 679/2016.

10.4 Misure organizzative di sicurezza per la protezione e la tutela dei dati nel sistema di gestione informatica dei documenti

Il sistema di gestione informatica del protocollo e dei documenti è conforme alle specifiche previste dalla normativa di settore (scritture di sicurezza e controllo accessi).
In particolare, il sistema di gestione informatica del protocollo e dei documenti, assicura:

- l'univoca identificazione e autenticazione degli utenti che accedono al sistema di gestione informatica dei documenti tramite UserID/password. Le credenziali di autenticazione sono rilasciate dal Responsabile della gestione documentale o suo delegato.

L'allegato 12 alla citata deliberazione 128/2024 (*Piano per la sicurezza del sistema di gestione informatica dei documenti*) individua e descrive le misure idonee per la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e di tutto il patrimonio informativo aziendale (allegato 4 al presente manuale).

10.5 Trattamenti senza l'ausilio di strumenti elettronici

Nel caso di trattamenti di dati personali effettuato con strumenti diversi da quelli elettronici o comunque automatizzati è stato altresì stabilito di:

- Conservare i dati e i documenti ad essi afferenti, in armadi o cassetti dotati di serrature o di altri sistemi di chiusura che ne consentano un accesso selezionato, evitando che gli stessi siano collocati in spazi liberamente accessibili al pubblico (ad es. corridoi, sale d'attesa, sale riunioni ecc.);

- Trattare i dati e le pratiche con diligenza e cautela tali da evitare indebite acquisizioni di notizie ed informazioni da parte di soggetti estranei o non autorizzati;

- Trasmettere dati particolari all'interno dell'Azienda direttamente a mani del destinatario, ovvero in buste o pacchi sigillati riportanti la dicitura "Riservato";

- Comunicare i dati particolari a mezzo telefono solo in situazioni di particolare urgenza e gravità, e comunque previa adozione di tutte le misure ritenute più efficaci per evitare la divulgazione a soggetti estranei e non identificati;

-

- Gli atti e i documenti contenenti dati personali anche particolari sono affidati alle persone autorizzate al trattamento dei dati personali per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dalle persone autorizzate al trattamento dei dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione;

- Le persone autorizzate al trattamento dei dati personali devono controllare l'accesso agli archivi contenenti dati personali anche particolari. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;

- Gli archivi e i registri cartacei devono essere custoditi in locali muniti di serratura ed il personale addetto provvede a far sì che in sua assenza i locali siano sempre chiusi a chiave;

- L'accesso e la permanenza nei locali degli archivi di persone non autorizzate al trattamento devono avvenire sempre in presenza di una delle persone autorizzate al trattamento o del Designato al trattamento;

- Può altresì accedere ai locali, per esigenze strettamente di servizio, personale della segreteria della Direzione. In tal caso l'accesso deve essere segnalato appena possibile alle persone autorizzate al trattamento o al Designato al trattamento.

- I documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per il loro trattamento se non in casi del tutto eccezionali e, nel caso in cui questo avvenga, l'asportazione, autorizzata dal responsabile del trattamento di competenza, deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;

- Quando i dati personali devono essere portati al di fuori dei locali individuati per il loro trattamento, l'incaricato del trattamento deve sempre portare con sé la cartella o la borsa nella quale i documenti sono contenuti e deve evitare che un soggetto terzo non autorizzato possa esaminare anche solo la copertina della cartella in questione, qualora essa riporti l'indicazione del contenuto;

- Per tutto il periodo in cui i documenti contenenti dati personali sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà mai lasciarli incustoditi;

- L'incaricato del trattamento deve controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.

Tutti i Dirigenti di Servizio, Struttura Amministrativa e Sanitaria dovranno attenersi, per quanto di propria competenza, alle suddette misure di sicurezza nel trattamento di dati personali in qualunque modo questi siano raccolti disponendone e verificandone l'osservanza anche da parte dei propri collaboratori.

ART. 11 – LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

Ai sensi dell'art. 4 punto 12 del GDPR per "Violazione di dati personali" (Data breach) si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

L'articolo 32 del GDPR stabilisce che devono essere approntate misure tecniche e organizzative adeguate a garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente una violazione dei dati, è espressione dell'adeguatezza delle misure implementate dal titolare – e quindi del rispetto del principio di accountability da parte dello stesso.

L'art. 33 del GDPR recita che: "*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

Con specifico riferimento all'obbligo di cui all'articolo 33 del Regolamento UE 2016/679, il titolare del trattamento, con deliberazione n. 683 del 7/8/2025, ha adottato apposita procedura per la gestione dei data breach, atta ad individuare quali siano le violazioni che ricadono nell'ambito della suddetta normativa, nonché i casi in cui lo stesso titolare deve notificare le violazioni all'Autorità Garante per la protezione dei dati personali ed eventualmente agli interessati, ed infine le misure atte a trattare il rischio e la documentazione da produrre (Allegato 5).

ART. 12 - DIRITTI DELL'INTERESSATO

Secondo quanto disposto dal Capo III del GDPR, l'interessato ha diritto di ottenere a cura del Titolare o del Preposto al trattamento, senza ritardo:

- la conferma che sia o meno in corso un trattamento dei Suoi dati personali e, in tal caso, di ottenerne l'accesso (diritto di accesso, ex art. 15 Reg. UE 2016/679);
- la rettifica dei Suoi dati personali inesatti, o l'integrazione dei Suoi dati personali incompleti (diritto di rettifica, ex art. 16 Reg. UE 2016/679);
- la cancellazione dei Suoi dati, se sussiste uno dei motivi previsti dal Regolamento (diritto all'oblio, ex art. 17 Reg. UE 2016/679);
- la limitazione del trattamento dei Suoi dati quando ricorre una delle ipotesi previste dal Regolamento (diritto di limitazione, ex art. 18 Reg. UE 2016/679);
- qualora il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) e il trattamento sia effettuato con mezzi automatizzati, l'interessato ha diritto a ricevere dall'Azienda in un formato elettronico di uso comune la trasmissione dei dati personali che lo riguardano senza impedimenti da parte del titolare del trattamento cui li ha forniti (diritto alla portabilità dei dati ex art. 20 Reg. UE 2016/679);

L'interessato ha inoltre diritto di esercitare nei confronti del Titolare i seguenti diritti, nelle forme e nei modi del paragrafo che precede:

- il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano qualora il trattamento sia fondato sul legittimo interesse del Titolare, o su ragioni di pubblico interesse, qualora la tutela delle sue libertà individuali debba ritenersi prevalente su detti interessi legittimi e/o pubblici (diritto di opposizione ex art. 21 Reg. Ue 2016/679).

  Si rammenta che l'esercizio del diritto di opposizione dell'interessato è soggetto al giudizio di bilanciamento tra l'interesse pubblico di cui è portatrice l'Azienda ed i diritti individuali dell'interessato. A tale fine, il personale inviterà l'interessato a voler indicare la motivazione della propria opposizione, ove possibile, in modo possibilmente chiaro, ancorché in forma sintetica.

- Il diritto di presentare reclamo al garante della privacy o di ricorrere all'autorità giudiziaria.

- il diritto di ottenere l'elenco completo ed aggiornato di tutti soggetti Responsabili e autorizzati al trattamento dei Suoi dati personali.

L'interessato, nell'esercizio dei diritti sopra riportati, può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

L'Azienda con deliberazione D.G. n. 641 del 2/8/2019 ha approvato apposita procedura e relativa modulistica per l'esercizio dei diritti degli interessati.

ART. 13 - SEGRETO D'UFFICIO, SEGRETO PROFESSIONALE

Ai sensi dell'art. 9, comma 3, Reg. UE 2016/679 i dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

A questi fini, sono soggetti a segreto professionale o d'ufficio tutti gli esercenti la professione medica e le professioni sanitarie, nonché gli impiegati civili dello Stato e degli Enti pubblici territoriali.

Art. 14 - REDAZIONE DEGLI ATTI E PUBBLICAZIONE

14.1 - I responsabili delle strutture organizzative che propongono una deliberazione o che adottano una determinazione dirigenziale, con il supporto tecnico dei relativi responsabili del procedimento, verificano, alla luce dei principi di necessità, pertinenza e non eccedenza sanciti dalla normativa, che l'inclusione nel testo e nell'oggetto di dati personali sia realmente necessaria per perseguire le finalità dell'atto stesso.

In ogni caso devono essere privilegiate modalità di redazione degli atti che prevedono l'utilizzo di dati anonimi o non direttamente identificativi, quali codici o altri riferimenti, se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.

I soggetti cui si riferiscono dati particolari ai sensi degli artt. 9 e 10 del G.D.P.R. devono essere individuati attraverso l'utilizzo di codici alfanumerici; ogni dato appartenente a categorie particolari di dati personali ai sensi dell'art. 9 del GDPR, che possa essere isolato dal contesto del provvedimento, senza comprometterne la necessaria motivazione, è riportato con il solo riferimento alla registrazione di protocollo.

14.2 - L'Azienda garantisce la riservatezza dei dati personali in sede di pubblicazione all'Albo on-line delle deliberazioni o di altri atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati.

Ai fini dell'individuazione degli interessi pubblici cui il trattamento dei dati è finalizzato, si applica l'art. 2-sexies, comma 2, Codice Privacy.

ART. 15 FORMAZIONE

L'ASL VCO organizza, anche su indicazione e con l'ausilio del DPO, di norma nell'ambito del piano annuale di formazione del personale, interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla

conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

ART. 16 – NORME FINALI

Per quanto non espressamente disciplinato nel presente atto si rinvia alla normativa dell'Unione Europea, la legislazione nazionale e regionale in materia di tutela dei dati personali, nonché le disposizioni emanate dal Garante per la Protezione dei Dati Personali.

Allegati:
1) – Informativa generale sul trattamento dei dati personali
2) – Informativa breve sul trattamento dei dati personali
3) - Informativa *sul trattamento dei Dati in ambito sanitario*
4) – Piano per la sicurezza del sistema di gestione informatica dei documenti.
5) – Deliberazione DG n. 683/2025 (Procedura per la gestione delle segnalazioni delle violazioni di dati personali).

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale: Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
P.I./Cod.Fisc. 00634880033

e-mail: protocollo@pec.aslvco.it - www.aslvco.it

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PER GLI UTENTI (ai sensi degli articoli 13-14 del Regolamento UE 2016/679)

Gentile paziente,

La presente Informativa in merito al trattamento di dati personali viene resa dall'Azienda Sanitaria Locale VCO (di seguito ASL VCO) ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679.

TITOLARE DEL TRATTAMENTO:

La ASL VCO, con sede legale in Via Mazzini n. 117 – 28887 Omegna - VB – CF e PIVA 00634880033 – www.aslvco.it – protocollo@pec.aslvco.it - in qualità di TITOLARE del trattamento, determina finalità e mezzi del trattamento ed è responsabile nei Suoi confronti del legittimo e corretto uso dei dati personali e particolari da Lei direttamente forniti e occasionalmente forniti da terzi.
Tali dati verranno trattati dagli operatori di questa Azienda nel rispetto del segreto professionale, del segreto d'ufficio e secondo i principi della vigente normava nazionale ed europea in materia di protezione dei da personali, in particolare alla luce della disciplina dettata dal Regolamento (UE) 2016/679 del 27 aprile 2016 (nel prosieguo denominato "Regolamento" o "GDPR"), dal D.lgs. 30 giugno 2003, n. 196 (c.d. "Codice Privacy") e dal D.lgs. 10 agosto 2018, n. 101.

SOGGETTO CHE VIGILA SUL RISPETTO DELLE DISPOSIZIONI SULLA PROTEZIONE DEI DATI:

Il Titolare ha nominato **il Responsabile della Protezione dei Dati** (RPD o DPO), ai sensi dell'art. 37 del GDPR, contattabile al seguente indirizzo email: dpo@aslvco.it .

FINALITÀ DEL TRATTAMENTO E BASE GIURIDICA

Il trattamento dei Suoi dati personali e di quelli appartenenti a categorie particolari (ad esempio, i dati relativi alla salute) avviene da parte della Azienda ai sensi dell'art. 9, par. 2, lett. h) del Regolamento, per le seguenti finalità di cura e per motivi di interesse pubblico rilevante ai sensi dell'art. 9, par. 2, lett. g) del Regolamento, individuati dall'art. 2-sexies del Codice (decreto legislativo 30 giugno 2003, n. 196 e s.m.i), per motivi di interesse pubblico nel settore della sanità pubblica ai sensi dell'art. 9, par. 2, lett. i) del Regolamento dunque, senza necessità del consenso:

- tutela della salute e dell'incolumità fisica (ossia attività di prevenzione, diagnosi, cura e riabilitazione);
- tutela socio-assistenziale e interventi di rilievo sanitario a favore di soggetti bisognosi, non autosufficienti o incapaci;
- attività legate alla fornitura di beni o servizi all'utente per la salvaguardia della

Sede legale: Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
P.I./Cod.Fisc. 00634880033

e-mail: protocollo@pec.aslvco.it - www.aslvco.it

salute (es. fornitura di ausili e protesi);

- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- adempimenti amministrativi, gestionali e contabili, correlati ai compiti istituzionali (attività di prevenzione, diagnosi, assistenza, terapia sanitaria e sociale) delle aziende sanitarie e/o connessi ad obblighi di legge che Le consentono di fruire dei servizi (prenotazioni per attività di screening, controllo dichiarazioni sostitutive, controllo esenzioni ticket, medicina di base etc..) a cura dell'Azienda o delle strutture sanitarie accreditate o dei medici convenzionati;
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria e della qualità del servizio, ivi inclusa la gestione, la pianificazione e il controllo dei soggetti accreditati o convenzionati con il SSR;
- attività di indagine a fini statistici e di ricerca scientifica, biomedica ed epidemiologica nel rispetto dei limiti e delle condizioni dettate dalla legge; gestione di esposti/lamentele/contenziosi;
- attività medico-legale e certificatoria;
- ulteriori motivi di c.d. interesse pubblico rilevante previsti da norma di legge o di regolamento.

Ulteriori trattamenti dei dati personali, che potrebbero presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, saranno effettuati, in conformità alle leggi e ai regolamenti, previa ulteriore nota informativa e, dove richiesto, previo rilascio di specifico consenso manifestato liberamente.
Si tratta ad esempio di trattamenti:

- ai fini della consultazione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico e del dossier farmaceutico;
- per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti;
- nell'ambito della teleassistenza/telemedicina;
- per la fornitura di beni e servizi attraverso rete di comunicazione elettronica;
- ai fini dei sistemi di sorveglianza e dei registri di cui all'art. 12, c.10 del D.L. 18 ottobre 2012 n° 179, convertito con modificazioni dalla L. 17 dicembre 2012 n° 221.

A CHI COMUNICHIAMO I SUOI DATI

I dati relativi al suo stato di salute non sono oggetto di diffusione, cioè non possono essere resi noti ad un numero indeterminato di soggetti. Possono invece essere comunicati, nei casi previsti da norme di Legge o di Regolamento, a soggetti pubblici e

Sede legale: Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
P.I./Cod.Fisc. 00634880033

e-mail: protocollo@pec.aslvco.it - www.aslvco.it

privati, Enti ed Istituzioni per il raggiungimento delle rispettive finalità.

Ad esempio:

- soggetti pubblici (altre aziende sanitarie) e privati (strutture sanitarie private, es. case di riposo) coinvolti nel Suo percorso diagnostico-terapeutico;
- Comune di residenza;
- Servizio Sanitario della Regione Piemonte o della Regione di residenza (se diversa), per finalità amministrative di competenza regionale (flussi SDO e mobilità);
- Servizi Sociali dei Comuni per le attività connesse all'assistenza di soggetti deboli;
- Medici di Medicina Generale/Pediatri di Libera Scelta, quando previsto;
- soggetti qualificati ad intervenire in controversie in cui è parte l'Azienda (compagnie assicurative, legali e consulenti, ecc);
- Forze dell'Ordine e Autorità Giudiziaria, Istituti penitenziari, nei casi previsti dalla legge;
- INPS/INAIL per gli scopi connessi alla tutela della persona assistita;
- soggetti terzi che effettuino operazioni di trattamento dati personali per conto dell'Azienda, appositamente qualificati "responsabili del trattamento" e tenuti al rispetto degli adempimenti in materia di protezione dati, in virtù di apposito contratto stipulato con l'Azienda;
- altri soggetti nei casi previsti da norma di legge o di regolamento.

In tutti i casi in cui un soggetto esterno nello svolgimento di attività tratti dati personali per conto dell'Azienda Sanitaria, tale trattamento si svolge sulla base di un contratto che ne costituisce la base giuridica e tali soggetti sono individuati "Responsabili del Trattamento" ai sensi dell'art. 28 del GDPR.

In caso di ricovero presso le strutture dell'Azienda Lei ha diritto a rendere o meno nota la propria presenza in reparto a soggetti terzi e a comunicare le informazioni sul Suo stato di salute solo ai soggetti da Lei individuati: tutto ciò compilando apposita modulistica.

TRASFERIMENTO DEI SUOI DATI VERSO UN PAESE TERZO E/O UN'ORGANIZZAZIONE INTERNAZIONALE

È possibile che i Suoi dati personali possano essere trasferiti a soggetti di un altro Paese, anche all'esterno dell'Unione Europea, se previsto da un obbligo di legge oppure in assolvimento di obblighi contrattuali verso un Responsabile del Trattamento. I trasferimenti verso Paesi extra-UE saranno effettuati soltanto nel pieno rispetto del GDPR.

PERIODO DI CONSERVAZIONE DEI SUOI DATI

Per la determinazione del periodo di conservazione dei dati personali, presenti nei

Sede legale: Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
P.I./Cod.Fisc. 00634880033

e-mail: protocollo@pec.aslvco.it - www.aslvco.it

documenti amministrativi e sanitari si fa riferimento al Massimario di Conservazione e Scarto della ASL VCO. In particolare i dati personali e particolari relativi a ciascun episodio di ricovero, che confluiscono nella cartella clinica, sono conservati per un periodo di tempo illimitato.
Il massimario di scarto è disponibile al seguente link: https://www.aslvco.it/azienda/regolamenti/

PROFILAZIONE
In nessun caso verrà effettuata qualsivoglia forma di trattamento automatizzato dei Suoi Dati personali per ottenere informazioni relative alle Sue preferenze personali, alle inclinazioni sessuali, ai comportamenti, alla situazione economica o alla sua ubicazione.

I SUOI DIRITTI IN QUALITA' DI SOGGETTO INTERESSATO
Lei ha il diritto (artt. 15 - 22 del GDPR) di chiedere all'Azienda di accedere ai Suoi dati personali e di rettificarli se inesatti, di cancellarli o limitarne il trattamento, se ne ricorrono i presupposti, nonché di ottenere la portabilità dei dati da Lei forniti, solo se oggetto di un trattamento automatizzato basato sul Suo consenso o sul contratto. Lei ha altresì il diritto di revocare il consenso prestato per le finalità di trattamento che lo richiedono, ferma restando la liceità del trattamento effettuato sino al momento della revoca.
Lei potrà esercitare i diritti sopra indicati inviando una e-mail all'indirizzo protocollo@pec.aslvco.it .
La modulistica per l'esercizio dei diritti è pubblicata nel sito web aziendale www.aslvco.it nella sezione "Dati personali".

Eventuali segnalazioni formali, in caso di presunta violazione dei dati o di immotivata inottemperanza alle richieste di esercizio dei diritti potranno essere inviate al Responsabile della Protezione Dati all'indirizzo dpo@aslvco.it.

Lei ha anche il diritto di proporre reclamo, ai sensi dell'art. 77 del GDPR, al Garante per la Protezione dei dati personali.

Il Titolare del Trattamento Dati

Direttore Generale ASL VCO

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

All. 2

Informativa breve
trattamento dati personali e particolari sulla salute

Il titolare del trattamento dei dati è l'ASL VCO, C.F. e P.I.V.A. 00634880033, via Mazzini, 117 – 28887 Omegna. Il responsabile della protezione dei dati è contattabile scrivendo al suddetto indirizzo o a dpo@aslvco.it.
Il titolare tratta i suoi dati personali in conformità alla normativa vigente in materia di protezione dei dati personali, per finalità di prevenzione, diagnosi, cura, amministrative, di tutela socio assistenziale sanitaria e motivi di interesse pubblico rilevante, come meglio descritto nell'informativa estesa consultabile sul sito aslvco.it al segunte link: https://www.aslvco.it/datipersonali, o mediante il QR Code qui accanto raffigurato.

Il Titolare del Trattamento Dati
Il Direttore Generale ASL VCO

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

All. 3

Informativa sul trattamento dei dati personali in ambito sanitario ai sensi dell'art. 13 del Regolamento UE 2016/679 (c.d. "GDPR")

Gentile Signore/ Signora,

Il titolare del trattamento dei suoi dati personali è l'ASL VCO, C.F. e P.I.V.A. 00634880033, via Mazzini, 117 – 28887 Omegna. Il responsabile della protezione dei dati è contattabile scrivendo al suddetto indirizzo o a dpo@aslvco.it. Il titolare tratta i suoi dati personali in conformità alla normativa vigente in materia di protezione dei dati personali:

A) per finalità di diagnosi, cura, amministrative, di tutela socio assistenziale sanitaria e motivi di interesse pubblico rilevante, ai sensi degli artt. 6 lett. E) e 9 lett. H) ed I) del GDPR; per le suddette finalità non è richiesto il suo consenso. Il Titolare potrà condividere, altresì, per alcune finalità ed in relazione ad alcuni trattamenti i suoi dati con il Contitolare Centro Ortopedico di Quadrante (COQ). L'informativa generale privacy è reperibile presso le sedi della ASL, consultabile sul sito aslvco.it/datipersonali, e mediante il QR Code qui accanto raffigurato.

B) Per il trattamento dei suoi dati genetici ai sensi dell'art. 9, comma 2, lettera "a" del GDPR, dell'art. 2-sexies, comma 2, lett. "u" e 2-septies, comma 6 del Dlgs 196/2003, dell'art. 22, comma 11 del Dlgs. 101/2018, dell'Autorizzazione del Garante al trattamento dei dati genetici n. 8/2016. Per la suddetta finalità è necessario che lei presti il suo consenso. In merito al trattamento dei suoi dati genetici, lo stesso potrà essere effettuato anche per mezzo di Fornitori esterni regolarmente autorizzati ai sensi dell'art. 28 G.D.P.R.;

C) Per comunicare notizie inerenti il suo stato di salute e i suoi referti clinici a soggetti terzi. Anche in questo caso è necessario che lei presti il suo consenso.

Preso atto di quanto sopra, e presa visione dell'informativa estesa, il sottoscritto

NOME ……..COGNOME……..DATA DI NASCITA……..

RESIDENZA…….in qualità di

☐ Paziente
☐ Legale rappresentante del paziente Sig./Sig.ra _____

Nato/a a _____il_____

REGIONE PIEMONTE

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

Per le finalità di cui alla lettera B)

☐ AUTORIZZA □ NON AUTORIZZA Il trattamento dei dati genetici

Per le finalità di cui alla lettera C)

☐ AUTORIZZA ☐ NON AUTORIZZA IL PERSONALE DELL' A.S.L. V.C.O. A COMUNICARE INORMAZIONI DI NATURA SANITARIA CHE LA RIGUARDANO:

(barrare la voce che interessa)

☐ Solo al sottoscritto/a

☐ Ai familiari che ne facciano richiesta, e specificatamente:

□ coniuge; □ figli; □ genitore; □ parente fino al 4° grado; □ affini fino al 2° grado; □ convivente

☐ A chiunque ne faccia richiesta

☐ Solo alle persone di seguito indicate:

_____

N.B. In caso di ricovero, inoltre, Le ricordiamo che il nostro personale del centralino e di reparto confermerà la Sua presenza in ospedale alle persone che chiedono di Lei (per consentire la comunicazione e/o la visita di parenti o conoscenti), **a meno che lei non indichi nella riga che segue, barrando la relativa casella, il diniego a confermare a terzi la Sua presenza**.

□ Non desidero che la mia presenza in ospedale venga comunicata e/o confermata a terzi.

Data ____/_____/_____ Firma leggibile del paziente (o del Legale Rappresentante)

_____

REGIONE PIEMONTE

ALL. 4

PIANO PER LA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Sommario

1. PREMESSA - RIFERIMENTI ED ALLEGATI

Il presente Piano della Sicurezza del Sistema di gestione informatica dei documenti (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) del Azienda Sanitaria Locale VCO (di seguito ASL VCO) per quanto attiene alle attività previste nel Sistema di gestione documentale, con riferimento alle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici, *ex* Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni.

Ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività.

Il PdS si fonda su una serie di documenti, procedure e prassi che, per motivi di sicurezza, non vengono allegati o proposti in estratto, tra cui le Misure Minime di Sicurezza adottate.

Nella stesura del presente Piano di Sicurezza del Sistema di gestione informatica dei documenti si è fatto riferimento alle norme tecniche ISO/IEC 27001 quali linea guida tecniche.

2. NORMATIVA E STANDARD DI RIFERIMENTO

2.1 Normativa di riferimento

- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Regolamento (UE) 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno – Regolamento eIDAS;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Circolare n. 2 del 18 aprile 2017, n. 2/2017 di AGID, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione del Cloud Service Provider per la PA;
- Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA.

2.2 Standard di riferimento

Nella definizione del contesto normativo tramite il quale regolamentare il Sistema di gestione documentale, il legislatore ha provveduto ad identificare alcuni standard tecnologici di valenza internazionale cui riferirsi, al fine sia di recepire ricerche e studi, sia di definire il percorso che consenta agli operatori di rispondere in maniera proattiva alla normativa europea. Segue l'elenco degli standard tecnologici cui si ispira il presente documento:

<u>Conservazione di documenti informatici:</u>

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).

<u>Sicurezza informatica:</u>

- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).
- Regolamento generale per la protezione dei dati personali 2016/679 (General Data Protection Regulation o GDPR) - Normativa europea in materia di protezione dei dati personali.
- ETSI TS 101 533-1 V1.2.1 – Technical Specification, Electronic Signatures and Infrastructures /ESI); Information Preservation Systems Security.

3. ORGANIZZAZIONE DEL SISTEMA DI GESTIONE DOCUMENTALE

Il paragrafo ha ad oggetto la descrizione dell'organizzazione del Sistema di gestione documentale, sotto il profilo dei ruoli, delle responsabilità e della produzione-diffusione di policy e procedure.

3.1 Ruoli e responsabilità del sistema di gestione documentale

Lo svolgimento delle attività legate al sistema di gestione documentale richiede la presenza di più attori, ognuno dei quali ha la responsabilità di specifiche attività da svolgere. Questi ruoli si inseriscono nell'organigramma generale dell'Ente, arricchendo i ruoli e le procedure già previste per la gestione dei processi interni.

Peraltro, così com'è previsto che alcune attività possano essere svolte dal medesimo soggetto è, altresì, previsto che alcune funzioni possano essere delegate ad altri soggetti.

Le attività relative al servizio di gestione documentale coinvolgono vari settori della ASL VCO che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti.

Specificamente, le attività impattano sulle seguenti strutture organizzative:

• *Responsabile del Servizio di gestione documentale*: questi possiede le competenze concernenti la definizione e l'attuazione delle politiche complessive del sistema di gestione documentale, nonché del governo della gestione del sistema.

In particolare, il Responsabile del Servizio di gestione documentale:

a) predispone lo schema del manuale di gestione;
b) propone i tempi, le modalità e le misure organizzative e tecniche;
c) predispone il Piano della Sicurezza del Sistema di gestione informatica dei documenti relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, in collaborazione con l'U.O. Sistemi informativi;
d) definisce e assicura criteri uniformi di trattamento del documento informatico, di classificazione ed archiviazione, nonché di comunicazione interna.

Questi, nello svolgimento della sua attività, si avvale della collaborazione:

- della SOS ICT*,* che cura l'implementazione, la gestione e la sicurezza dell'infrastruttura ICT;
- dello *Help-desk:* afferente all'ICT, che cura la soluzione di problemi tecnici, user oriented, legati alle infrastrutture digitali telematiche dell'ente;
- *del Provider (fornitore) del Software applicativo del Protocollo Informatico*: soggetto privato che implementa e gestisce il software applicativo su cui poggia il sistema di Protocollo Informatico in uso nella ASL VCO.

3.2 Ruoli e responsabilità della sicurezza informatica del sistema di gestione documentale

Il personale della ASL VCO destinato alla gestione del sistema documentale, per quanto concerne le questioni legate alla Sicurezza informatica, si riferisce alla SOS ICT.

3.3 Procedure di produzione, diffusione e gestione della documentazione di sicurezza

Le procedure di gestione della documentazione di sicurezza riguardano le attività legate all'acquisizione, produzione, archiviazione e diffusione del materiale relativo alla Sicurezza delle Informazioni.

I principi di Gestione Documentale della Sicurezza, propri della ASL VCO, prevedono la produzione di documenti elaborati e la loro diffusione, in seguito alla fase di analisi dei rischi, da parte del Responsabile della gestione documentale in cooperazione con il Responsabile della SOS ICT. Scopo dell'attività è offrire uno strumento di condivisione delle procedure di sicurezza con il personale dell'Azienda.

3.4 Procedure per l'acquisto di prodotti e servizi

Sotto il profilo della sicurezza ICT del sistema di gestione documentale, il processo di acquisto dei prodotti e servizi all'interno dell'Azienda è regolamentato dalla normativa di riferimento e gestito dalle competenti strutture aziendali.

3.5 Procedure per l'alienazione degli asset dell'organizzazione

La protezione dei supporti di memorizzazione dell'Azienda è uno dei presupposti della sicurezza dei documenti informatici, in quanto archiviati in tali supporti. Si tratta di: HD e SSD, supporti mobili (USB) cancellabili, supporti mobili non cancellabili (CD, DVD).

Sotto il profilo della sicurezza ICT del sistema di gestione documentale, il processo di dismissione o alienazione degli asset dell'Azienda viene regolamentato da specifiche procedure:

- procedura di **cancellazione** delle informazioni;
- procedura di **distruzione** dei supporti non riscrivibili utilizzati per la memorizzazione delle informazioni;
- procedura di **cancellazione sicura** dai supporti riscrivibili utilizzati per la memorizzazione delle informazioni;
- procedura di **triturazione** di supporti, quali quelli cartacei e analoghi;
- procedura di custodia e conservazione dei supporti contenenti dati degli utenti (hard disk dei pc) una volta che essi non siano più in servizio presso l'Azienda (es. pensionamenti, dismissioni volontarie, trasferimenti, aspettative, ecc.).

3.6 Piano di formazione del personale

Il Responsabile della gestione documentale, in cooperazione con il Responsabile per il trattamento dei dati personali e il Responsabile della SOS ICT pianifica, organizza, fornisce e gestisce la programmazione della formazione del personale, per quanto concerne i seguenti aspetti:

- *policy* e tecnica per l'utilizzo dei sistemi informatici dell'Azienda e del Protocollo Informatico;
- *policy* e tecnica per la sicurezza dei sistemi informatici dell'Azienda e del Protocollo Informatico;
- *policy* per la gestione delle emergenze informatiche dell'Azienda e del Protocollo Informatico.

3.7 Continuità operativa: *Disaster Recovery* e procedure di attivazione

Le misure adottate per garantire la continuità operativa dell'accesso all'intero sistema di gestione documentale si fondano sulla strutturazione di procedure di *Disaster recovery* e *Backup* delle informazioni, nonché sulla presenza di apparati ridondati, come dettagliato nei paragrafi seguenti.

Le misure concernono:

- il sistema web application per il Protocollo Informatico: mediante *policy*, procedure e prassi del Provider dell'applicazione;
- il sistema informatico della ASL VCO: attraverso policy, procedure e prassi elaborate secondo le norme concernenti la Tutela dei dati, la Sicurezza dei sistemi, il Codice per l'Amministrazione Digitale e la normativa legata al Sistema di gestione documentale.

In particolare *policy*, procedure e prassi concernono:

- il grado di affidabilità dei sistemi hardware/software;
- la programmazione della manutenzione delle apparecchiature e delle infrastrutture di supporto: idrico, elettrico, antintrusione, antifurto, antiallagamento, antincendio, continuità elettrica;
- il controllo sui sistemi al fine di assicurarne la continua disponibilità e integrità.

Il servizio di *Disaster Recovery* viene garantito sulla base dei dati soggetti a *backup* periodici effettuati giornalmente ed è declinato in servizio di *Disaster Recovery* DATI e servizio di *Disaster Recovery* INFRASTRUTTURE applicative, come dettagliato di seguito:

- servizio di *Disaster Recovery* DATI - La soluzione comporta il backup dei dati presso il sito secondario, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un *recovery time* più veloce. Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale e con replica costante dei dati. Il *backup* avviene in modalità elettronica mediante collegamenti fra i siti tenuto dimensionati tenendo conto della tipologia, quantità e periodicità dei dati, con:
  - RPO (tempo massimo di delay tra l'ultima copia e il fault dei sistemi) di 4 ore
  - RTO (tempo necessario per il ripristino dei sistemi) di 1 ora.
- servizio di Disaster recovery INFRASTRUTTURE applicative - la soluzione comporta la replica delle *virtual machine* presso il sito secondario, permettendo un *recovery time* più veloce. Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un sito alternativo sempre disponibile. Il *backup* avviene in modalità elettronica mediante collegamenti fra i siti tenuto dimensionati tenendo conto della tipologia, quantità e periodicità dei dati con:
  - RPO (tempo massimo di delay tra l'ultima copia e il fault dei sistemi) di 24 ore

- RTO (tempo necessario per il ripristino dei sistemi) di 1 ora.

La procedura di *Disaster Recovery* da attivarsi all'occorrenza lato Ente mostra una sua disposizione in fasi, atta ad essere applicata a qualunque evento verificato:

- Fase di reazione all'emergenza: 1) ricevimento della segnalazione dell'evento, attraverso sistemi di rilevamento o indicazioni del personale; 2) pre-valutazione della situazione di pericolo e di rischio; 3) indicazione di misure temporanee di emergenza, con possibilità di sospensione del servizio.
- Fase di gestione dell'emergenza: 1) identificazione dell'area tecnica da coinvolgere nell'attività; 2) indicazione di misure di emergenza da disporre al fine di risolvere l'evento; 3) supervisione delle attività e adattamento al caso concreto.
- Fase di riattivazione dei servizi: 1) osservazione sulle attività svolte in base a principi di buone regole tecniche; 2) test sui servizi soggetti all'evento "off line"; 3) riattivazione graduale dei servizi con controllo dell'efficienza.
- Fase di ritorno alla normalità: 1) test dei sistemi online; 2) apertura al personale dei sistemi riattivati con monitoraggio della fruizione; 3) piena operatività dei sistemi e normalità operativa.

La struttura organizzativa di riferimento preposta alla gestione dello stato di emergenza è la SOS ICT.

4. ARCHITETTURA FUNZIONALE

Il sistema di Protocollo Informatico si basa su quanto di seguito dettagliato:

- presenza di un software applicativo *web-based*;
- infrastruttura centralizzata su *datacenter* certificato AgID;
- diffusione dell'applicativo attraverso rete privata LAN-WAN dell'ASL VCO verso le sedi dell'amministrazione.
- integrazione del sistema e dell'applicativo verso sistema di conservazione sostitutiva;
- accesso in VPN al fornitore del software applicativo per manutenzione e adeguamento normativo ai sensi di legge.

4.1 Componenti logico-fisiche

La soluzione informatica abilitante il Protocollo Informatico dell'ASL VCO è rappresentata da un software applicativo erogato in *cloud* in modalità IaaS/PaaS su *datacenter* di Terze Parti certificato AGID conforme allo standard ISO 27001 e fruibile attraverso l'infrastruttura di rete LAN/WAN dell'Ente.

L'infrastruttura server che ospita il software di gestione documentale è collocato presso il CLOUD TIM SPC.

In via generale, la soluzione software di protocollo e gestione documentale ARCHIFLOW mostra i seguenti profili:

1) Componente logica:

L'ambiente di produzione è un'architettura *three-tier* di tipo MVC e dunque consta attualmente di un server web interno di Front verso gli utenti (presentation), di un application server su cui sono eseguite le logiche di business e di un server di data base (DAMS ORACLE) che contiene anche la base documentale su file system. L'architettura applicativa mira a garantire i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi;

Gli utenti usufruiscono dell'applicazione interagendo con l'interfaccia utente per via telematica dalla propria postazione di lavoro e della rete locale della ASL VCO;

Il software e le informazioni gestite risiedono in un sistema centralizzato costituito da server virtuali;

L'utilizzo dei dispositivi e della rete intranet della ASL VCO è garantito ai soli utenti dotati di apposite credenziali d'accesso al sistema informatico, rilasciate da SOS ICT su indicazione dei ruoli indicati dai Responsabili delle strutture di appartenenza, con l'utilizzo di password di lunghezza e complessità adeguate e con scadenza e necessità di rinnovo prestabilite;

Il sistema di sicurezza consente agli utenti di collegarsi all'applicazione secondo le modalità d'autorizzazione connesse al proprio ruolo e alle proprie responsabilità;

L'accesso al sistema è effettuato attraverso dispositivi e reti, nonché sistemi operativi e browser, rilasciati dalla ASL VCO.

2) Componente fisica:

Gli utenti usufruiscono dei dispositivi dell'ASL VCO per l'accesso e l'utilizzo della piattaforma erogata in *cloud*.

L'infrastruttura di rete dell'ASL VCO include firewall, router e switch sia di core sia di distribuzione ed è soggetta a controlli di sicurezza sia logici sia fisici.

La sicurezza perimetrale sia on-prem sia cloud viene demandata a Next Generation Firewall in grado di attivare funzionalità di IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Antivirus in configurazione di alta affidabilità. L'antivirus è installato su ogni postazione di lavoro ed è soggetto a periodici aggiornamenti.

Il cloud service provider (CSP)* certificato AGID mette a disposizione le risorse della propria piattaforma IaaS/PaaS (risorse computazionali, di rete, di sicurezza, di storage e monitoraggio) implementata dai dispositivi integrati nel proprio cloud (firewall, proxy, web,application e database server, SAN, switch, router,..).

Il datacenter in cui sono sono ospitati tutti i nostri server hanno una procedura di Disaster Recovery per garantire la continuità operativa.

Per ulteriori informazioni su come è implementata la sicurezza dell'infrastruttura che ospita il sistema di gestione documentale, fare riferimento al "DOCUMENTO PROGRAMMATICO DI GESTIONE DELLA SICUREZZA DEI SERVIZI CLOUD TIM SPC Lotto 1".

4.2 Piani di manutenzione delle infrastrutture

L'ecosistema ICT riconducibile nel suo complesso, direttamente o indirettamente, al sistema di gestione documentale, è soggetto a manutenzione ordinaria e straordinaria schedulate dal CSP (*Cloud Service Provider*) e/o dal *Provider* dell'applicativo che comunica preventivamente all'Ente le attività manutentive ordinarie e straordinarie, infine dal Responsabile del Servizio di gestione documentale - in quest'ultimo caso in cooperazione con il Responsabile della SOS ICT - qualora presupponessero impatti limitati all'infrastruttura di LAN/MAN.

4.3 Data Center per l'erogazione del servizio in modalità cloud IaaS/PaaS

I Data Center (primari e di *Disaster Recovery*) sono situati sul territorio nazionale all'interno di strutture altamente industrializzate, dotate dei più moderni sistemi, impianti e risorse professionali.

La connettività fra i data center stessi è realizzata attraverso accessi ridondati in fibra ottica a 10 Gbit/s e sono dotati di sistemi di condizionamento, gruppi di continuità, generatori elettrici, sistemi antincendio e monitoraggio attivi 24x7. Ciascun Data Center è attrezzato con sistemi e procedure di seguito descritte:

▪ **Rilevazione fumi e spegnimento incendi** - tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. In particolare l'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturale ed il continuo funzionamento del resto dell'impianto;

▪ **Anti allagamento** - sono previste delle sonde di rivelazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuori uscite di acqua saranno opportunamente allontanate mediante convogliamento e scarico verso l'esterno;

▪ **Anti intrusione -** è previsto un sistema di anti intrusione integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di TVCC, con il sistema di controllo accessi e con gli allarmi tecnologici. I sensori del sistema allocati all'interno dell'edificio saranno attivati e disattivati da segnali provenienti dal sistema di controllo accessi;

▪ **Telecamere a circuito chiuso** - le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche. Il sistema TVCC sarà soggetto ad attivazione tramite "motion detection";

▪ **Condizionamento** - Nell'area I/T sono mantenute, sia in estate sia in inverno, le seguenti condizioni ambientali:

- temperatura 18-24° ±1 °C
- umidità relativa: controllata (30 – 70 %)
- ricambi d'aria pari a 0.5 volumi/ora.

▪ **Continuità ed Emergenza** - sono previsti dei gruppi di continuità (UPS) aventi batterie con autonomia di 30 minuti a pieno carico; tale intervallo di tempo consente l'attivazione del sistema di emergenza (costituito da 2 gruppi elettrogeni) che a sua volta garantisce un'autonomia di almeno 24 ore e capacità di asservire tutto il complesso. Gli UPS assicurano la continuità a tutti i dispositivi informatici.

▪ **Controllo degli accessi fisici** - con sorveglianza armata 24 ore su 24, procedure di registrazione degli accessi e identificazione del personale che accede in nome e per conto dei Clienti, accesso alle sale sistemi controllato elettronicamente tramite badge, controllo del perimetro con impianti a raggi infrarossi, test periodici di evacuazione, procedure di sicurezza con identificazione ed assegnazione di responsabilità.

▪ **Servizio di Gestione Remota del Backup** - Il servizio è finalizzato all'esecuzione continuativa giornaliera dei sistemi di backup atti a garantire, in caso di disastro i seguenti indicatori di Livello di Servizio (RTO e RPO) contrattualizzati dall'Ente con il *Provider* dell'applicativo. La piattaforma di *backup* implementa funzionalità di *data protection* garantendo:

- crittografia dei dati di tipo AES-256 integrata nel proprio file system proprietario;
- riduzione dei tempi di backup tramite deduplica globale e backup di tipo incrementale;
- *live mount* per l'avvio delle Virtual Machine e delle basi di dati direttamente dai file di *backup* archiviati sul proprio *file system*;
- motore di ricerca intelligente per la navigazione rapida tra le diverse versioni dei file di backup, a prescindere dalla posizione di archiviazione;
- replica multipla ed archiviazione integrata del dato in geografico anche in modalità „*multicloud*";
- servizio di backup specifico del sistema di gestione documentale Archiflow, con tempistiche e modalità concordate.

5. CONFORMITA' AL REG. UE 679/2016 (GDPR)

In ottemperanza la Reg. UE 679/2016 (GDPR), il *Provider* dell'applicazione, agendo in qualità di Responsabile del trattamento, è tenuto a:

▪ adottare adeguate misure per la sicurezza dei dati personali previste dal GDPR, indicate dal Titolare (ASL VCO, d'ora in avanti "Titolare"), vigilando sulla applicazione delle stesse, in modo da ridurre al minimo i rischi di violazione dei dati medesimi;

▪ individuare le persone autorizzate al trattamento dei dati personali che operano sotto la propria autorità e garantire che le persone autorizzate assumano idonei obblighi di riservatezza di tali dati, fornendo loro adeguate istruzioni per lo svolgimento delle attività di trattamento e verificandone l'osservanza;

▪ conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali "amministratori di sistema" esclusivamente per quanto necessario per lo svolgimento di quanto previsto dal Contratto e all'attività di verifica almeno annuale dell'operato di questi amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza, riguardanti i trattamenti dei dati personali, previste dalle norme vigenti (come previsto dal Provvedimento del Garante sugli "amministratori di sistema" pubblicato in G.U. n. 300 del 24 dicembre 2008 e dalla sua modifica in base al provvedimento del 25 giugno 2009);

▪ assistere il Titolare nel garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di sicurezza, notifica all'autorità di eventuali violazioni di dati personali e, se del caso, loro comunicazione agli interessati, nonché di valutazione d'impatto sulla protezione dati ed eventuale consultazione preventiva, ai sensi degli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione dello stesso Responsabile;

▪ comunicare al Titolare per iscritto, senza indebito ritardo, eventuali violazioni di sicurezza che riguardino i dati personali trattati ai fini della fornitura dei Servizi oggetto del Contratto;

▪ informare tempestivamente il Titolare in caso di ricevimento di richieste di informazioni o documenti, accertamenti ed ispezioni, da parte del Garante per la protezione dei dati personali, quale autorità competente di controllo, o di altre autorità giudiziarie o di polizia giudiziaria, ove attinenti al trattamento dei

dati personali connesso alla fornitura dei Servizi oggetto del Contratto, e collaborare con il Titolare alla predisposizione dei correlati riscontri, atti, documenti o comunicazioni;

- cancellare o restituire al Titolare, su richiesta di quest'ultimo, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che la vigente normativa europea o nazionale preveda la conservazione dei dati da parte del Responsabile che, in tal caso, ne darà contestuale attestazione al Titolare.

Il Responsabile si riserva, per la esecuzione di alcune parti delle attività commissionate, di nominare "Altri Responsabili" scelti nel proprio Albo dei Fornitori qualificati e che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente Normativa sulla "Privacy" e si impegna a vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dalla Società nei confronti del Titolare.

Al Titolare è riservata la facoltà di richiedere l'elenco degli "Altri Responsabili" incaricati e la relativa documentazione di incarico e di idoneità tecnico professionale.

Al Titolare è altresì riservata la facoltà di richiedere le modificazioni e/o integrazioni degli obblighi previsti in capo alla Società quale Responsabile del trattamento che si rendano necessarie a seguito dell'eventuale entrata in vigore di nuove disposizioni di legge, di regolamento ovvero di provvedimenti adottati da autorità amministrative o giudiziali in materia di tutela dei dati personali.

Il Titolare si è avvalso della facoltà prevista dall'art. 37 punto 2 del GDPR per procedere alla nomina di un "Responsabile unico della protezione dei dati" (RPD oppure DPO).

Al fine di recepire quanto previsto dal GDPR, il Responsabile, congiuntamente alle altre aziende del Gruppo di appartenenza, ha adeguato la propria politica della sicurezza delle informazioni e i relativi obiettivi aggiornando il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI), riferimento per tutte le procedure e le istruzioni inerenti alla sicurezza delle informazioni e alla protezione dei dati personali. Questa nuova versione del SGSI tende ad una maggiore conformità rispetto alla ISO/IEC 27002:2013.

5.1 "Privacy by design" e "Privacy by default"

In ottemperanza al principio di "responsabilizzazione" ("*accountability*") previsto nell'art. 5 del Regolamento, devono essere poste "in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento", tra cui quelle previste dall'art. 25, cioè:

- la Privacy by design per rispondere ai principi di protezione dei dati con "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita…tenendo conto dello stato dell'arte e dei costi di attuazione" oltre che del contesto (tipo di dati, finalità, ecc.);

- la Privacy by default per limitare il trattamento ai soli "dati personali necessari".

Il Responsabile, inoltre, in ottemperanza al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (pubblicato nella Gazzetta Ufficiale n. 300, 24 Dicembre 2008), modificato in base al provvedimento del 25 giugno 2009, rende disponibile la verifica delle attività degli "Amministratori di Sistema" a beneficio dei Titolari del trattamento dei dati. Il provvedimento richiede - oltre alla valutazione delle caratteristiche soggettive dell'amministratore di sistema, alla sua designazione individuale, al suo inserimento in un elenco e alla verifica del suo operato - anche la registrazione dei suoi accessi (autenticazione informatica) ai sistemi ed agli archivi che contengono dati personali, mediante:

- monitoraggio delle attività di *login* e *logout* degli utenti da sistemi operativi ed ai database;
- registrazione in maniera intellegibile ed estrazione su un apposito database per permetterne l'inalterabilità richiesta dal Garante

Gli archivi sono conservati e tenuti a disposizione del Titolare del trattamento per almeno sei mesi.

5.2 Identificazione dei rischi

L'infrastruttura ICT sottesa al Protocollo Informatico, nella sua componente legata al software applicativo e all'intera infrastruttura della ASL VCO, può essere così descritta per macro aree:

- reti e apparati di rete;
- elaboratori e software di sistema;
- software applicativo;

- supporti informatici di memorizzazione;
- infrastrutture;
- contenitori/archivi cartacei, archivi informatici di Backup.

Scopo dell'infrastruttura è la gestione del sistema di gestione documentale, garantendo i dati attraverso loro:

- **Riservatezza**: in modo che l'informazione sia resa disponibile solamente ai processi che la devono elaborare ed all'utilizzatore che ne è autorizzato all'uso;
- **Integrità**: in modo che ogni informazione sia realmente quella originariamente immessa nel sistema informativo, ovvero successivamente legittimamente modificata;
- **Disponibilità**: in modo che la reperibilità delle informazioni in funzione delle esigenze di continuità dei processi aziendali ed al fine del rispetto delle norme, tecniche e giuridiche, che ne impongono la conservazione storica.

I rischi cui è esposta l'infrastruttura ICT suindicata, per sua tecnicità e scopo, possono essere ricondotti a cinque macro categorie:

- rischio d'area legato all'accesso non autorizzato nei locali tecnici (cloud e on-prem);
- rischio di guasti tecnici hardware, software, supporti;
- rischio di penetrazione in reti di comunicazione, device e servizi;
- rischio legato ad errori umani;
- rischio d'area per possibili eventi distruttivi.

5.3 Definizione dei rischi

La definizione dei rischi si propone di mostrare i rischi identificati in forma strutturata.

Il **Rischio d'area legato all'accesso non autorizzato nei locali** può essere definito come la possibilità che soggetti non autorizzati accedano ai locali tecnici presso l'Ente (CED) piuttosto che DataCenter (del Cloud Service Provider). In via indicativa, i rischi possono essere i seguenti:

- accesso ad uffici con collegamento telematico al sistema di gestione documentale;
- accesso al CED e alle aree di Backup;
- accesso alle aree informatiche per la connessione di rete, LAN/MAN e Internet.

Il **Rischio di guasti tecnici hardware, software, supporti**, può essere definito come la possibilità che strumenti fisici e logici si deteriorino o si danneggino, per caso fortuito, incuria o dolo, attraverso attività fisiche e logiche, in modo tale da non consentire la fruizione del sistema di gestione documentale. In via indicativa, i rischi possono essere i seguenti:

- danneggiamento/deterioramento logico/fisico di supporti di memorizzazione, infrastrutture di rete, device;
- danneggiamento/deterioramento logico/fisico dei device presenti nel CED/DataCenter;
- danneggiamento/deterioramento logico/fisico dei device per il Disaster Recovery e la continuità di accesso ai servizi.

Il **Rischio di penetrazione in reti di comunicazione, device e servizi**, può essere definito come la possibilità che un soggetto non autorizzato abbia accesso alle reti di comunicazione dell'ente, sotto un profilo sia logico sia fisico. In via indicativa, i rischi possono essere i seguenti:

- accesso alla rete telematica senza autorizzazione;
- violazione di reti e device attraverso attività fisiche;
- attacchi informatici, hacking e cracking;
- interruzione o sviamento del servizio di rete e/o web.

Il **Rischio legato a errori umani** può essere definito come la possibilità che, a causa di incuria o distrazione, il sistema di gestione documentale, o le sue attività, siano messe a rischio sotto il loro profilo logico e fisico. In via indicativa, i rischi possono essere i seguenti:

- Accesso a device e punti rete incustoditi;
- attacchi d'Ingegneria sociale;
- sovraccarico della rete e dei servizi per utilizzo anomalo delle console;
- interruzione prolungata di servizi elettrici, incendio e allagamento dei locali tecnici.

Il **Rischio d'area per possibili eventi distruttivi**, infine, può essere definito come la possibilità che, a seguito di eventi naturali di tipo distruttivo, il sistema di gestione documentale possa subire danni od interruzioni del servizio, non dipese dalla volontà della ASL VCO o del fornitore del software applicativo. In via indicativa, i rischi possono essere i seguenti:

- danneggiamento/distruzione degli edifici e delle connessioni di rete;
- danneggiamento/distruzione dei device, di rete e forniti agli utenti, e dei software applicativi;
- danneggiamento/distruzione delle sale CED e Backup;
- danneggiamento/distruzione degli archivi per la conservazione dei dati in remoto.

5.4 Stima della criticità dei rischi

La stima della criticità dei rischi è effettuata attraverso una ponderazione composta da criteri di probabilità e livello del rischio. In particolare:
Criteri di probabilità:

- basso: improbabile
- medio: possibile
- elevato: altamente possibile

Livelli di rischio:

- lieve: evento a basso impatto fisico-logico
- medio: evento a rilevante impatto fisico-logico
- grave: evento ad alto impatto fisico-logico.

5.5 Sviluppo di strategie

In base all'identificazione e alla definizione dei rischi, a seguito di loro stima per criteri di probabilità e livelli di rischio, la ASL VCO sviluppa strategie di contrasto e di mitigazione all'evento, atte a ridurre, eliminare o accettare i rischi individuati.

Le strategie sono elaborate dal Responsabile della gestione documentale in cooperazione con il Responsabile dell'U.O. Sistemi Informativi.

5.6 Mitigazione

Il piano di mitigazione del rischio, ovvero della soluzione prevista, in base alle prerogative di sicurezza della ASL VCO, si fonda su una sua valutazione. In particolare:

- se il rischio è considerato accettabile: stante le misure di sicurezza minime in essere e le mitigazioni generali performanti, la ASL VCO procede ad un suo monitoraggio;
- se il rischio non è considerato accettabile: stante le misure di sicurezza minime in essere e le mitigazioni generali performanti, la ASL VCO procede alla revisione delle strategie di sicurezza al fine di individuare mitigazioni ulteriori e sanare il rischio.

5.7 Gestione dei rischi

La gestione dei rischi ICT ha come obiettivo l'analisi circa l'elaborazione di misure atte a modificare il livello di rischio e le strategie di mitigazione, migliorando la sicurezza e la performance dell'infrastruttura ICT. La gestione del rischio è affidata al Responsabile della SOS ICT.

Il rischio, in base a policy e procedure della ASL VCO, è differenziato in base al livello di criticità, al fine di affrontare in via principale i rischi più critici e, in via secondaria, i rischi meno critici.

Le misure atte a modificare il livello di rischio e le strategie di mitigazione sono elaborate dal Responsabile della gestione documentale, in cooperazione con il Responsabile della SOS ICT.

6. POLITICHE DI SICUREZZA

Il presente paragrafo ha ad oggetto la descrizione delle politiche di sicurezza concernenti il sistema di gestione documentale, in particolare sotto il profilo della gestione dei sistemi, del controllo degli accessi fisici e logici, delle postazioni di lavoro, dei contenuti applicativi, degli apparati e supporti mobili, nonché della rete di comunicazione.

6.1 Politica di gestione della sicurezza dei sistemi

La gestione in sicurezza delle infrastrutture informatiche – recata da *policy*, procedure e prassi della ASL VCO – ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi di elaborazione forniscano le prestazioni tecniche ai livelli e con i requisiti di sicurezza definiti.
I principi generali applicati per la gestione della sicurezza sono così sintetizzabili:

- gestione ed aggiornamento dell'inventario di asset hardware e software;
- applicazione di regole standard per l'installazione e la configurazione dei sistemi;
- configurazioni dei sistemi disegnate tenendo in considerazione le esigenze informatico giuridiche attuali e le possibili attività future;
- configurazioni dei sistemi indirizzate alla sicurezza built-in, atte a facilitare l'installazione di ulteriori misure di sicurezza;
- adozione di procedure standard per la configurazione dei sistemi
- attività regolari di monitoraggio sulle prestazioni dei sistemi per gestire adeguatamente eventi, problemi e incidenti.

6.2 Politica per il controllo degli accessi fisici

La politica per il controllo degli accessi prevede di consentire un accesso ai locali tecnici limitato al personale strettamente necessario autorizzato dal Responsabile della SOS ICT (personale della ASL VCO, personale di fornitori esterni se accompagnati).

6.3 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

La creazione dell'utenza è effettuata dalla SOS ICT su comunicazione della SOC Personale attraverso software applicativo dedicato collegato al database degli accessi al dominio. Il flusso di creazione dell'utenza mostra i seguenti profili:

- indicazione di nuovo componente organico PA alla SOS ICT;
- inserimento nel dominio ad opera della SOS ICT;
- inserimento nel programma di gestione del personale ad opera della SOC Personale;
- attribuzione dei ruoli specifici per l'applicativo protocollo ad opera della SOS ICT, previa autorizzazione del competente dirigente.

Sono previste altresì dall'Ente procedure di cancellazione su comunicazione della SOC Personale e/o di cambio di autorizzazione su comunicazione dei Dirigenti dei servizi competenti.

Il sistema di gestione documentale permette l'assegnazione differenziata dei profili di abilitazione, intervento, modifica e visualizzazione dei documenti in rapporto alle funzioni e al ruolo svolto dagli uffici/utenti, garantendo la tutela dei dati personali.

Le abilitazioni dei singoli utenti sono estraibili dal sistema di gestione documentale in qualsiasi momento.

Le modalità di rilascio delle abilitazioni di accesso degli utenti al sistema di gestione informatica dei documenti, e la relativa profilazione, avviene secondo i criteri individuati dalla AOO.

Tramite la procedura Cred.Net, sistema aziendale per la richiesta di autorizzazione all'accesso alle banche dati aziendali, per ogni funzione specifica del sistema viene individuata una voce apposita. Le tipologie di ruoli sono quelle sotto indicate:

<u>ARCHIFLOW:</u>
- Consultazione
- Protocollazione + invio PEC
- Delibere Estensore
- Delibere Responsabile del procedimento
- Delibere Responsabile di Struttura-sostituto-funzionario
- Determinazioni Responsabile del Procedimento
- Determinazioni Responsabile di Struttura-sostituto-funzionario
- Determinazioni Estensore

6.4 Politica di gestione delle postazioni di lavoro

La politica concernente la gestione delle postazioni di lavoro - disposta attraverso differenti policy, procedure e prassi della SOS ICT – mostra i seguenti elementi essenziali:

- fornitura delle postazioni di lavoro;
- regole per l'installazione del software sulle postazioni di lavoro;
- regole per gli aggiornamenti;
- regole per la limitazione della connettività a supporti esterni;
- regole per la modifica delle impostazioni;
- regole tecniche per l'accesso alla rete;
- regole per la creazione dei documenti informatici.

6.5 Politica di gestione del parco applicativo

La politica di gestione del Software si fonda sull'utilizzo di prassi che riguardano:

- la manutenzione dei sistemi;
- il controllo sul contenuto software dei client al fine di verificare la non presenza di codice malevolo sulle postazioni di lavoro;
- la conformità a quanto autorizzato e previsto dalle licenze d'uso.

L'attività è svolta attraverso utilizzo di antivirus/antispam/antimalware costantemente aggiornati, monitoraggio di flussi di rete e analisi preventiva di device, nonché schedulazione di interventi di manutenzione e osservazione delle prestazioni dell'hardware.

6.6 Politica di gestione, dismissione e smaltimento degli apparati e dei supporti

Le politiche di sicurezza della ASL VCO pongono particolare attenzione alla gestione degli apparati mobili, in particolare:

- dispositivi: portatili, tablet, smartphone, cellulari, ecc.
- supporti di memoria esterni: HD esterni/CD/DVD/Pen Drive/DAT/LTO, ecc.
- carta stampata: utilizzata e/o prodotta nell'ambito delle attività di protocollazione.

Per quanto concerne dispositivi e carta stampata, l'utilizzo è consentito, secondo policy, procedure e prassi dell'Ente pubblico, tali da indicare le modalità di utilizzo e conservazione dei dispositivi, nonché le politiche atte alla loro dismissione/distruzione.

6.7 Politica di gestione dei canali di comunicazione

I canali di comunicazione elettronici che attraversano il confine periferico dell'Ente vengono filtrati da apparati di *Next Generation Firewall* con funzionalità di *Intrusion Prevention* e *Attack Detection* per preservare la confidenzialità, e l'integrità, delle informazioni in transito, ed allo stesso tempo evitare abusi del canale elettronico e tentativi di intrusione.

6.8 Manutenzione delle politiche di sicurezza

La ASL VCO dispone il perfezionamento, la divulgazione e il riesame delle politiche di sicurezza al verificarsi dei seguenti eventi:

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;

- risultati delle eventuali attività di audit interni ed esterni.

7. GESTIONE DEGLI INCIDENTI

Si definisce “incidente di sicurezza” qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell’organizzazione o l’integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore. Ciò con particolare riferimento al Dlgs. 196/2003, alla L. 547/1993 ed alla L. 38/2006, al D.P.C.M. 03/12/2013 e al D.L. 2005/82.

La ASL VCO classifica gli incidenti, definendone la codifica preventiva e la gestione degli stessi.

Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- **Rilevazione/identificazione/classificazione**: sono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell’amministrazione;
- **Contenimento**: sono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il *roll-back* dopo la successiva fase di eliminazione;
- **Eliminazione**: sono eliminate le cause che hanno portato al verificarsi dell'incidente;
- **Ripristino**: sono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il *roll-back* delle contromisure di contenimento;
- ***Follow-up***: è verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Le procedure di gestione degli incidenti sono demandate, per quanto concerne il sistema di gestione documentale, alla SOS ICT.

7.1 Processo di gestione degli incidenti

Più in dettaglio, il modello generale che governa il processo di gestione degli *incident* deriva dalle migliori pratiche del *framework* ITIL secondo la seguente metodologia, suscettibile di miglioramenti ed ottimizzazioni in fase di esercizio in funzione di nuove tipologie di minacce nonché della disponibilità di nuove tecnologie e/o evoluzione di quelle presenti atte a contrastarle e mitigarle:

- analisi del contesto;
- ricezione richiesta/segnalazione da parte dell’utente interno all’Ente, oppure rilevazione non sollecitata di una necessità a seguito di controlli periodici o segnalazioni automatiche *real-time* da strumento di monitoraggio;
- inserimento nel sistema di *ticketing* della richiesta/segnalazione/necessità;
- analisi preliminare della richiesta/segnalazione/necessità al fine di limitare inefficienze e problemi per non corrette interpretazioni e/o falsi positivi;
- assegnazione all’intervento di un livello di priorità;
- assegnazione dell’intervento ad un tecnico o gruppo di tecnici in base a complessità;
- pianificazione dell’attività analizzando tutti i fattori ritenuti utili e/o critici (interdipendenze, sinergie tra risorse *on-site* e/o remote, tempistiche, *leveraging* esperienziale sulla base di attività analoghe pregresse e di *best practice* comprovate);
- preparazione dell’intervento attraverso l’analisi di quanto verificatosi in caso di *incident/problem*, identificazione degli ambiti e degli stakeholder anche esterni, monitoraggio degli SLA, effettuazione di *backup* delle configurazioni prima dell’intervento;
- attuazione di processi autorizzativi a vari livelli durante l’esecuzione delle attività in base alle classi di intervento concordate e gestione del processo di escalation;
- esecuzione dell’intervento (in loco, o da remoto, etc.) con particolare attenzione alla definizione concordata dei tempi di intervento e minimizzazione dei tempi di disservizio, completezza, efficienza ed efficacia dell’intervento, comunicazione dell’avvenuta esecuzione all’Ente e relativi *stakeholder* definiti in fase di pianificazione e altri rilevati nel corso dell’intervento, inserimento dello stato avanzamento nel sistema di *ticketing*, compilazione della documentazione della base di conoscenze quando necessario;

- esecuzione reiterata dell'intervento in caso di mancata risoluzione al primo tentativo con eventuale *escalation* verso fornitori esterni e/o l'eventuale supporto di figure tecniche specialistiche fino alla completa risoluzione;
- chiusura del caso con comunicazione ai soggetti interessati.