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. 643 del 28/07/2025

Oggetto: APPROVAZIONE PROCEDURA PER LA GESTIONE DELLE NOMINE DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL GDPR 2016/679.

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

DIRETTORE AMMINISTRATIVO - DOTT.SSA BARBARA BUONO

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: Primatesta Giuseppina
Il Responsabile del procedimento: Primatesta Giuseppina
Il Dirigente/Funzionario: Priolo Vittoria Maria
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 Regolamento UE 2016/679 (G.D.P.R. - Regolamento europeo in materia di protezione dei dati personali):

- all'art. 4 p.2 identifica l'attività di trattamento come "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";

- all'art. 4 p. 8 definisce il 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".

RILEVATO CHE l'art. 28 del citato G.D.P.R., stabilisce che:

"1. Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
2. Il responsabile del trattamento non ricorre ad altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento".

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

PRECISATO che il Responsabile del trattamento è pertanto un soggetto esterno alla struttura aziendale del Titolare (ASL VCO), al quale quest'ultimo affida l'espletamento di servizi o prestazioni che comportano un trattamento di dati personali, le cui modalità sono disciplinate compiutamente in apposito contratto di nomina.

RITENUTO, pertanto, necessario adottare, in conformità a quanto previsto dall'art. 28 G.D.P.R. 2016/679, idonea procedura per regolamentare i rapporti tra il Titolare e ciascun Responsabile esterno del trattamento dei dati, unitamente al contratto di nomina, nonché alla documentazione ivi allegata.

DATO ATTO 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.

RILEVATO CHE la Funzione Privacy sopra citata ha elaborato in collaborazione con il Responsabile della Protezione Dati aziendale, ed in stretta sinergia e coordinamento con la SOC Logistica e Servizi Informatici, la procedura che descrive il processo di gestione della nomina dei responsabili del trattamento.

EVIDENZIATO CHE tale procedura dovrà essere applicata, per quanto di competenza, da tutte le Strutture aziendali che gestiscono contratti o altri atti giuridici con fornitori e soggetti esterni che trattano dati personali per conto dell'ASL VCO.

RITENUTO pertanto di formalizzare la procedura allegata alla presente deliberazione sotto la lettera A), alla quale risultano uniti i seguenti allegati:
1) Modello di Accordo per il Trattamento dei Dati Personali ai sensi art. 28 GDPR;
2) Modalità operative gestione informazioni privacy da rendere a operatori economici e fornitori;
3) IOP – Informativa per operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere;
4) IFC – Informativa per i Fornitori /contraenti

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

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

DELIBERA

1) **di approvare** la Procedura per la gestione delle nomine dei Responsabili del trattamento dei dati personali ai sensi dell'art. 28 del GDPR 2016/679, allegata alla presente deliberazione quale parte integrante e sostanziale sotto la lettera A), e comprensiva dei seguenti allegati:

   1) Modello di Accordo per il Trattamento dei Dati Personali ai sensi art. 28 GDPR;
   2) Modalità operative gestione informazioni privacy da rendere a operatori economici e fornitori;
   3) IOP – Informativa per operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere;
   4) IFC – Informativa per i Fornitori /contraenti

2) **di dare atto** che la procedura di cui al punto 1) del presente dispositivo deve essere applicata, per quanto di competenza, da tutte le Strutture aziendali che gestiscono contratti o altri atti giuridici con fornitori e soggetti esterni che trattano dati personali per conto del Titolare del Trattamento Dati (ASL VCO).

3) **di disporre** la pubblicazione del presente atto, unitamente alla procedura ed ai suoi allegati, sul sito intranet aziendale – Aree tematiche - Sezione Privacy, a cura della Funzione Privacy aziendale, nonché la notifica alle strutture aziendali interessate.

4) **di dare atto che** le informative (allegati 3 e 4 alla procedura) potranno essere aggiornate a seguito di modifiche normative o regolamentari e che, ai fini della loro validità, sarà sufficiente la mera pubblicazione dell'ultima versione di informativa in uso sul sito web aziendale, nella sezione "Dati personali", e nell'area intranet.

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

6) **di dichiarare** il presente atto immediatamente esecutivo, stante l'urgenza di provvedere in merito.

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. A)

PROCEDURA PER LA GESTIONE DELLE NOMINE DEI RESPONSABILI DEL TRATTAMENTO DI DATI PERSONALI AI SENSI DELL'ART. 28 DEL GDPR 2016/679

Sommario

INTRODUZIONE....3
1. SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE....3
2. NORMATIVA DI RIFERIMENTO....3
3. TERMINI E DEFINIZIONI....4
4. L'ORGANIGRAMMA DATA PROTECTION....7
5. I SOGGETTI responsabili DEL TRATTAMENTO dei dati personali (criteri di inclusione/esclusione)....7
5.1. GESTIONE DELLE NOMINE DEI RESPONSABILI DEL TRATTAMENTO....8
5.1.1. VALUTAZIONE DEI RESPONSABILI DEL TRATTAMENTO....8
5.1.2 PRIVACY BY DESIGN E PRIVACY BY DEFAULT…… ……9
5.1.3. L'ACCORDO CON IL RESPONSABILE DEL TRATTAMENTO....9
6. AMMINISTRATORI DI SISTEMA....11
6.1. GESTIONE DEGLI AMMINISTRATORI DI SISTEMA....11
7. LA MAPPATURA DEI CONTRATTI....12
7.1. IL REGISTRO DEI RESPONSABILI....13
8. MONITORAGGIO E MIGLIORAMENTO CONTINUO …… 13
9. MODALITA' OPERATIVE ……13
Tabella sintetica del processo ……14
10. GESTIONE DEL DOCUMENTO…… 15
Allegati …… ….15

INTRODUZIONE

La normativa vigente in materia di protezione dei dati personali prescrive ai titolari del trattamento di tutelare la riservatezza dei dati personali, al fine di evitare che ogni eventuale utilizzo non corretto degli stessi possa ledere i diritti e le libertà fondamentali dei soggetti interessati da tale trattamento.

Nell'ambito in cui opera Azienda Sanitaria Locale del Verbano Cusio Ossola (d'ora in avanti, per brevità definita ASL VCO) in qualità di titolare del trattamento, tale onere risulta ancora più importante dal momento che vengono trattate quotidianamente una pluralità di informazioni riferite ad un numero ingente di persone ed inoltre – per loro natura – tali informazioni sono riferite sovente ad aspetti legati alla salute delle persone interessate.

In tali circostanze, considerato altresì il numero elevato di soggetti che effettuano le attività di trattamento di dati personali per conto del titolare, risulta necessario mappare adeguatamente le attività di trattamento di dati personali effettuate dal singolo responsabile del trattamento, nonché da eventuali soggetti sub-responsabili.

Pertanto, al fine di comprovare il rispetto dei principi applicabili al trattamento di dati personali di cui all'articolo 5 del Regolamento UE 2016/679 (GDPR) – in linea con il principio di responsabilizzazione previsto al paragrafo 2 dello stesso articolo – il titolare del trattamento ha adottato la presente procedura per garantire una corretta e dinamica gestione operativa di tutti gli adempimenti inerenti all'affidamento delle attività di trattamento di dati personali a *soggetti esterni all'ASL VCO*.

1. SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE

L'obiettivo principale del presente documento è quello di assicurare al titolare la piena e continua aderenza alla normativa vigente in materia di protezione dei dati personali, tenendo quindi in considerazione tutti i principi applicabili ai sensi dell'articolo 5 del Regolamento UE 2016/679 nelle attività di trattamento di dati personali, effettuate con particolare riferimento a quanto disposto dall'articolo 28 "Responsabile del trattamento" del medesimo GDPR.

La presente procedura si applica alle operazioni di trattamento di dati personali effettuate dal responsabile del trattamento – ivi inclusi tutti i soggetti da questo autorizzati al trattamento, che possano raccogliere, accedere o trattare in qualsiasi modo i dati personali per suo conto o nell'ambito del suo assetto organizzativo – ed inoltre trova applicazione per quanto concerne tutti gli strumenti ("asset") adoperati a tal fine.

Pertanto, avendo ad oggetto tutte le attività di trattamento effettuate dal titolare del trattamento e dai soggetti dallo stesso individuati allo scopo, è responsabilità di tutti i soggetti di cui sopra conoscere ed applicare i contenuti della presente procedura operativa, ovvero garantire un'adeguata conformità con la stessa.

2. NORMATIVA DI RIFERIMENTO

Si elencano di seguito i riferimenti normativi applicabili alla presente procedura:

- Regolamento UE 2016/679 (General Data Protection Regulation) del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101
- Provvedimenti, linee guida e pareri emanati dall'Autorità Garante per la protezione dei dati personali: in particolare, il provvedimento del 27 novembre 2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", per come modificato in base al provvedimento del 25 giugno 2009

- Linee guida adottate dal Comitato europeo per la protezione dei dati (“European Data Protection Board”, EDPB), nonché dal precedente Gruppo di lavoro “Articolo 29” (WP29)
- Regolamenti, policy, istruzioni operative nonché atti organizzativi, ordini di servizio ed ogni altro documento interno all’ASL VCO del titolare del trattamento che risulti funzionale al raggiungimento delle finalità della presente procedura operativa
- Schema internazionale ISDP©10003:2020 per la valutazione della conformità al Regolamento europeo 2016/679
- Registri delle attività di trattamento del titolare e del responsabile, nonché ogni altro registro mantenuto dall’ASL VCO con l’obiettivo di agevolare il rispetto della normativa vigente in materia di protezione dei dati personali

3. TERMINI E DEFINIZIONI

Ai fini di stabilire la terminologia di cui al presente documento, si riportano di seguito le definizioni tratte dall’articolo 4 del Regolamento UE 2016/679:

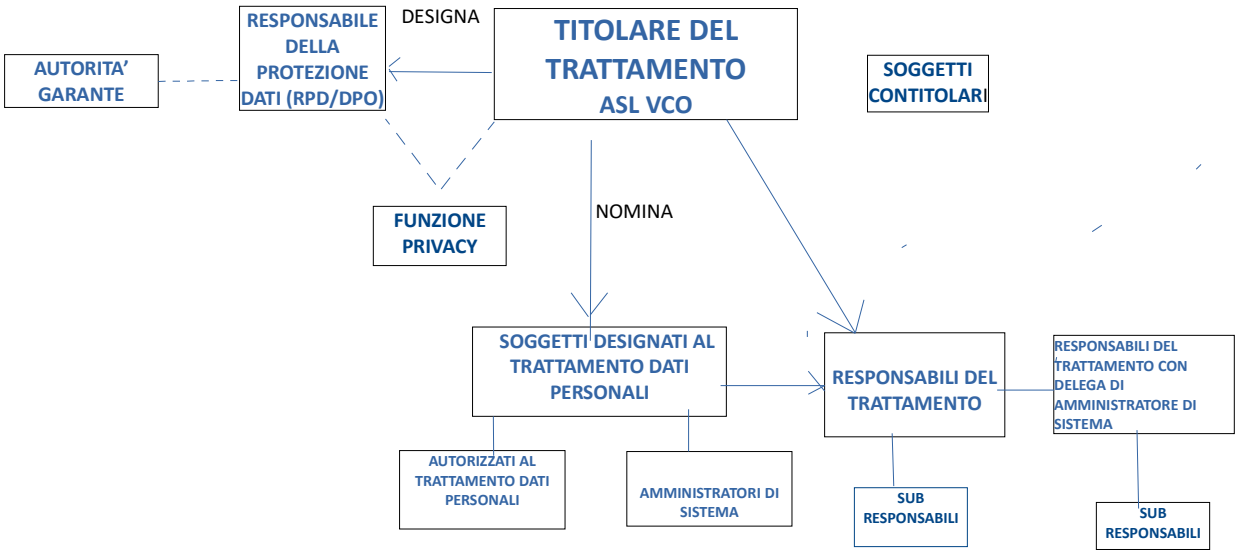
- *dato personale:* qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di 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;
- *trattamento:* qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione;
- *limitazione di trattamento:* il contrassegno dei dati personali conservati con l’obiettivo di limitarne il trattamento in futuro;
- *profilazione:* qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica;
- *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;
- *archivio:* qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- *titolare del trattamento:* la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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;
- *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;

- *destinatario:* la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- *terzo:* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- *consenso dell'interessato:* qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- *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;
- *dati genetici:* i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- *dati biometrici:* i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- *dati relativi alla salute:* 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;
- *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, nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del Regolamento UE 2016/679;
- *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;
- *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;
- *gruppo imprenditoriale:* un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- *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;
- *autorità di controllo:* l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

- *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;
- 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;
- *obiezione pertinente e motivata:* un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del Regolamento UE 2016/679, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme allo stesso 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;
- *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:
    - "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per:
        - «a distanza»: un servizio fornito senza la presenza simultanea delle parti;
        - «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici;
        - «a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale."
- *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;
- *Referente data protection:* soggetto individuato dal titolare del trattamento, tra le persone autorizzate al trattamento dei dati personali sotto la propria autorità diretta ai sensi dell'articolo 2-quaterdecies del D.Lgs. 196/03 e dell'articolo 29 del Regolamento UE 2016/679, al fine di fungere da interfaccia primaria per tutte le questioni inerenti alla protezione dei dati personali all'interno dell'Organizzazione del titolare – ivi incluse le comunicazioni tra il titolare del trattamento ed il responsabile della protezione dei dati, ovvero quelle tra il titolare del trattamento e l'Autorità di controllo competente ai sensi dell'articolo 51 del Regolamento UE 2016/679.

4. L'ORGANIGRAMMA DATA PROTECTION

Al fine di rappresentare schematicamente il posizionamento dei ruoli all'interno dell'ASL VCO relativa alla protezione dei dati personali, si riporta di seguito una raffigurazione dell'*Organigramma Data Protection (ODP)*, da contestualizzare negli scenari delle attività di trattamento effettuate dal titolare, per come descritte negli appositi registri.



5. I SOGGETTI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI (CRITERI DI INCLUSIONE/ESCLUSIONE)

Il responsabile del trattamento, per come definito all'art. 4 del Regolamento UE 2016/679, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

In via generale, i fornitori che rispetto al contratto principale trattano dati personali (ossia ogni informazione relativa a persone identificate o identificabili) per conto dell'Ente devono essere designati responsabili del trattamento.

La procedura si applica a tutti i contratti/atti giuridici per cui ricorrano i seguenti presupposti:

- il fornitore aggiudicatario dell'affidamento (o altro soggetto esterno) tratta dati personali per conto del Titolare del Trattamento;

- esiste un contratto tra le parti o altro atto giuridico vincolante in essere o in corso di stipula.

Nel contesto organizzativo dell'Ente i dati personali trattati dal fornitore/responsabile del trattamento per conto del Titolare si riferiscono alle categorie di interessati, quali: utenti, pazienti, lavoratori, fornitori dell'ente in quanto soggetti fisici e/o rappresentanti legali e/o altri referenti di fornitori soggetti giuridici.

Nel caso in cui il ricorso ad un soggetto esterno per servizi o approvvigionamenti di prodotti non implichi il trattamento di dati personali di soggetti interessati con riferimento all'organizzazione del Titolare, il fornitore non dovrà essere individuato come responsabile del trattamento.

Il titolare, ai sensi dell'art. 28 del Regolamento, può ricorrere *"unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato"*.

5.1. GESTIONE DELLE NOMINE DEI RESPONSABILI DEL TRATTAMENTO

In virtù della maggiore autonomia decisionale conferita dal titolare del trattamento ai responsabili da questo individuati, il paragrafo 3 del suddetto articolo della normativa europea prevede che:

"I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a. *tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;*

b. *garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;*

c. *adotti tutte le misure richieste ai sensi dell'articolo 32;*

d. *rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;*

e. *tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;*

f. *assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;*

g. *su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;*

h. *metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.*

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati."

5.1.1. VALUTAZIONE DEI RESPONSABILI DEL TRATTAMENTO

Al fine di individuare un fornitore esterno quale responsabile del trattamento dati per conto del titolare, la Struttura che gestisce il contratto deve verificare che il contraente si impegni a rispettare gli obblighi di cui al precedente art. 5.1. e, successivamente, stipulare un contratto con lo stesso al fine di designarlo come Responsabile del trattamento.

Il titolare del trattamento si è dotato di un modello di Accordo di Accordo per la nomina dei Responsabili del trattamento dati ai sensi art. 28 GDPR atto a verificare che il responsabile soddisfi i requisiti della normativa vigente in materia di protezione dei dati personali (allegato 1).

L'utilizzo di questo documento, inoltre, permette di rendere documentabili le garanzie presentate dal singolo responsabile del trattamento.

L'operatore economico/soggetto esterno, in fase di partecipazione alla procedura di affidamento, compila le parti di competenza del citato modello di Accordo ed attesta il possesso dei requisiti di sicurezza ivi previsti all'art. 19, o, in alternativa, dichiara di impegnarsi formalmente, sin dal momento della partecipazione alla procedura, ed in caso di aggiudicazione, ad adeguare la propria struttura in tal senso.

5.1.2. PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Il titolare del trattamento si assicura che i responsabili del trattamento forniscano servizi e/o prodotti in linea con i criteri di Privacy by Design e Privacy by Default del GDPR.

In particolare, si stabilisce di operare secondo le best practices di riferimento per l'impostazione predefinita indicate dalle Linee guida dell'ENISA andando ad analizzare le 4 aree di misura:

- Quantità minima di dati personali
- Estensione minima del trattamento di dati personali
- Minimo periodo di conservazione dei dati personali
- Accessibilità minima dei dati personali

Al fine di poter avere un maggior controllo delle scelte operate e una traccia documentale atta a comprovare il livello di conformità della soluzione disegnata al GDPR ed alle altre previsioni normative applicabili, si chiederà al fornitore la documentazione di solution design attuata, ovvero un documento che descriva le analisi e le scelte di progetto adottate e fornisca delucidazioni riguardo ai seguenti fattori:

- livello di conformità al GDPR
- eventuali customizzazioni e conseguenze all'allineamento al GDPR
- natura, ambito di applicazione, contesto e finalità del trattamento dei dati personali dei processi che ci si prefigge di gestire tramite la soluzione
- rischi di security e rischi per i diritti e le libertà degli interessati
- riferimenti alle attività di risk assessment ed alle eventuali valutazioni di impatto eseguite (DPIA)

5.1.3. L'ACCORDO CON IL RESPONSABILE DEL TRATTAMENTO

Il titolare del trattamento sottoscrive l'idoneo accordo per il trattamento di dati personali ai sensi dell'articolo 28 del Regolamento UE 2016/679 solo dopo che il Fornitore/soggetto esterno ha provveduto ad attestare e documentare l'esistenza delle misure tecniche ed organizzative indicate nel modello del citato Accordo che viene preliminarmente inserito nei documenti di gara, adeguate a garantire la compliance del trattamento affidato al GDPR.

Infatti, la normativa prescrive espressamente al titolare di "stipulare la materia trattata" nell'accordo per il trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679: pertanto, il cosiddetto "Data Processing Agreement" riporterà – oltre, come detto, ai riferimenti contrattuali quanto più dettagliati possibile – anche un insieme di informazioni atte a descrivere in dettaglio, seppur sinteticamente, l'oggetto e le caratteristiche del trattamento effettuato.

A tal proposito, l'accordo per il trattamento adottato dalla ASL VCO (all. 1 alla presente procedura) prevede che il titolare ed il responsabile, prima della sottoscrizione del medesimo, inseriscano negli appositi articoli quanto di seguito descritto:

- L'Art. 15 ha l'obiettivo di descrivere sinteticamente, ed al contempo in maniera chiara ed esaustiva, le caratteristiche delle attività di trattamento effettuate:
  - la natura e le finalità del trattamento di dati personali;
  - le categorie di soggetti interessati dal trattamento (es: dipendenti, utenti del servizio);
  - le tipologie di dati personali coinvolti, specificando ove presenti gli eventuali dati appartenenti alle cosiddette categorie "particolari" di cui all'art. 9 del GDPR;
  - la durata del trattamento, ivi incluso il periodo di conservazione dei dati;
  - le misure di sicurezza tecniche ed organizzative adottate, con particolare riferimento al livello di sicurezza del trattamento di cui all'art. 32 del GDPR;
  - una valutazione sintetica dei rischi del trattamento, con riguardo a quanto prescritto dall'art. 32, par. 2, del Regolamento UE 2016/679;
  - ove applicabile, le categorie di destinatari dei dati (es: soggetti autorizzati sotto la diretta autorità del responsabile, eventuali sub-responsabili): non rientrano in tale definizione "le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine" (art. 4, par. 9, del GDPR);
  - ove applicabile, le informazioni relative all'eventuale trasferimento dei dati al di fuori dei confini dell'Unione Europea, ivi inclusi i Paesi destinatari dei dati personali;
  - ove sussistano le circostanze di cui all'art. 35 del GDPR, tutte le informazioni a disposizione del responsabile che siano necessarie per la valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment, DPIA), ivi inclusa l'eventuale DPIA del Servizio e/o del sistema adottato (art. 28, par. 3, lett. f, del GDPR).
- L'Art. 16 riporta i recapiti del responsabile del trattamento e del Data Protection Officer da questi eventualmente designato ai sensi dell'art. 37 del Regolamento UE 2016/679, al fine di ottenere un punto di contatto per tutte le questioni inerenti alle attività di trattamento disciplinate dall'accordo;
- L'Art. 17 ha l'obiettivo di raccogliere le informazioni essenziali sugli eventuali soggetti individuati quali sub-responsabili ai sensi e per gli effetti dell'art. 28, parr. 2 e 4, del Regolamento UE 2016/679.
- L'Art. 18 prevede la nomina degli Amministratori di Sistema;
- L'Art. 19 riporta i principi di trattamento e diritti degli interessati e le misure di sicurezza garantite dal Responsabile del trattamento.

Le informazioni contenute negli articoli sopra elencati, di fatto, possono subire variazioni durante il periodo di validità dell'accordo: ciò può essere dovuto, a titolo esemplificativo e non esaustivo, ad integrazioni contrattuali concordate tra le parti, a cambiamenti intercorsi in merito ai soggetti sub-responsabili, ovvero a modifiche di ogni natura delle caratteristiche del trattamento effettuato.

In tali circostanze, il titolare del trattamento – ove necessario, con il supporto del responsabile della protezione dei dati – valuta l'opportunità di effettuare le modifiche ai suddetti articoli dell'accordo, oppure di produrre un nuovo documento alla luce delle modifiche apportate alle attività di trattamento, che dovrà essere nuovamente sottoscritto dalle parti.

Alla fine del rapporto di collaborazione tra il titolare e il responsabile, sarà necessario:

- richiedere che siano effettuate le azioni minime per consentire la continuità delle attività aziendali del titolare;

- revocare gli asset aziendali (fisici e digitali) assegnati al soggetto;
- richiedere copia di tutti i documenti contenenti dati personali in possesso del responsabile e trattati per conto del titolare;
- richiedere la distruzione o cancellazione definitiva delle restanti copie di banche dati o altri documenti contenenti dati personali in possesso del responsabile;
- revocare le chiavi di accesso (fisiche e digitali) ai sistemi informativi dell'Organizzazione;
- predisporre la disattivazione di account e caselle di posta elettronica personali.

La gestione delle suddette prescrizioni avviene mediante l'aggiornamento del Registro dei Responsabili del Trattamento: tramite tale documento mantenuto dalla struttura che gestisce il contratto (RPU), il titolare potrà sia verificare in ogni momento le autorizzazioni restituite e sottoscritte per accettazione dai soggetti destinatari, sia dimostrare, in conformità con il principio di accountability, l'adempimento delle normative vigenti in materia di protezione dei dati personali.

6. AMMINISTRATORI DI SISTEMA

Alcune delle attività di trattamento regolamentate dalla presente procedura implicano per loro natura l'affidamento – da parte del titolare – della gestione di sistemi informatici a determinati soggetti autorizzati al trattamento, oppure individuati quali responsabili del trattamento ai sensi dell'articolo 28 del Regolamento UE 2016/679: in tali circostanze, le autorizzazioni e gli accordi al trattamento dovranno prevedere l'assegnazione delle funzioni di *amministratore di sistema*.

Con la definizione di *"amministratore di sistema"* si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo, nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati: attività tecniche quali il salvataggio dei dati, la gestione delle attività di backup e recovery, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware, comportano infatti, in molti casi, un'effettiva capacità di azione sulle informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore di sistema non consulti "in chiaro" le informazioni medesime.

Nel loro complesso, le norme vigenti in materia di protezione dei dati personali – sebbene non definiscano espressamente tali figure – mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta.

Peraltro, la stessa Autorità Garante per la protezione dei dati personali – con il provvedimento del 27 novembre 2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" – ha richiamato l'attenzione dei titolari del trattamento sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche assimilabili a quelle di amministratore di sistema.

6.1. GESTIONE DEGLI AMMINISTRATORI DI SISTEMA

Ai sensi del suddetto provvedimento:

a. L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea

garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

b. La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

c. Gli estremi identificativi degli amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante;

d. Nel caso di servizi di amministrazione di sistemi affidati in outsourcing, il titolare o il responsabile devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche con funzioni di amministratore di sistema;

e. L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

f. Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

A tal proposito, nell'ambito degli adempimenti descritti dalla procedura operativa di cui al presente documento, il titolare del trattamento prevede di:

- Valutare il Responsabile del Trattamento;
- Stipulare un contratto o altro atto giuridico a norma dei diritti dell'Unione o degli Stati membri ;
- Incaricare ulteriormente il responsabile quale Amministratore di Sistema, specificando i sistemi informativi da esso gestiti.

L'art. 18 dell'Accordo per il trattamento predisposto dal Titolare disciplina la nomina e raccoglie i recapiti dei soggetti Amministratori di Sistema, nonché il dettaglio dei sistemi amministrati nell'ambito delle attività di trattamento affidate al responsabile dal titolare. Tali riferimenti sono suscettibili di aggiornamenti durante il periodo di validità dell'accordo medianti .

7. LA MAPPATURA DEI CONTRATTI

Una volta identificati i responsabili del trattamento, come definiti ai paragrafi precedenti, il titolare ha l'onere di raccogliere e documentare le caratteristiche peculiari dei trattamenti di dati personali effettuati. Questo risulta essere un passaggio inevitabile anche per l'implementazione ed il mantenimento del *Registro delle attività di trattamento*, nel rispetto delle disposizioni di cui all'articolo 30 del Regolamento UE 2016/679.

A tal proposito, una panoramica delle attività di trattamento effettuate dal responsabile è senz'altro desumibile dal contratto, convenzione o altro atto giuridico stipulato tra il titolare ed il singolo fornitore che tratta dati personali per suo conto: ne consegue, quindi, che è di fondamentale importanza mantenere costantemente aggiornato l'elenco dei responsabili, documentando altresì il riferimento puntuale al contratto stipulato.

7.1. IL REGISTRO DEI RESPONSABILI

Il *Registro dei responsabili* viene adottato e mantenuto aggiornato dal titolare, al fine di individuare tutti i fornitori ai quali vengono assegnate – a vario titolo – attività di trattamento dei dati personali, essendo pertanto individuati quali responsabili del trattamento ai sensi e per gli effetti dell'art. 28 del Regolamento UE 2016/679; a tal proposito, si rammenta ancora l'importanza di evitare di inserire in tale documento eventuali fornitori che non trattino dati personali per conto del titolare, in quanto ciò non sarebbe coerente con le finalità del documento.

Il Titolare ha predisposto un apposito *Registro dei Responsabili* attraverso l'adozione e l'implementazione del software *Data Protection Manager.*

La sua compilazione è a carico di ciascun RPU (o struttura aziendale che gestisce il contratto), per quanto di propria competenza, con il supporto della funzione privacy aziendale, che, per eventuali dubbi o problematiche nello svolgimento di tali mansioni, può chiedere supporto al Responsabile della Protezione Dati.

8. MONITORAGGIO E MIGLIORAMENTO CONTINUO

Le attività di trattamento effettuate dal titolare, al fine di verificare costantemente l'aderenza alla normativa vigente, necessitano di valutazioni e controlli periodici atti a riesaminare le misure tecniche ed organizzative adottate. Tale monitoraggio, da svolgersi in caso di necessità e comunque con frequenza almeno annuale, mira a verificare l'efficacia e la corretta applicazione delle norme.

A tal proposito, il titolare del trattamento, per il tramite dell'Ufficio Privacy aziendale e del Responsabile per la cyber sicurezza aziendale – di concerto con il consulente per la protezione dei dati ed anche, ove applicabile, con il responsabile della protezione dei dati – effettua periodicamente attività di *audit*, mediante appositi strumenti di valutazione dell'aderenza alla normativa vigente in materia di trattamento dei dati personali e del rischio *cyber*. Tali controlli consentono di valutare, trattare e ridurre i rischi informatici e di sicurezza cibernetica, puntando inoltre ad individuare ed eliminare eventuali trattamenti che risultino potenzialmente lesivi dei diritti e delle libertà fondamentali degli interessati.

9. MODALITÀ OPERATIVE

Le Strutture che gestiscono i contratti di acquisizione di beni e servizi o altri atti giuridici verso soggetti esterni valutano la necessità di procedere alla nomina a Responsabile del Trattamento, applicando i criteri di inclusione/esclusione illustrati nel paragrafo 5.

Nella valutazione si dovranno considerare anche i contratti in corso di svolgimento alla data di adozione della presente procedura, mentre, nell'ottica del principio di privacy by design, la previsione di designazione dovrà essere gestita, per i contratti da stipulare ex novo, nell'ambito delle procedure di affidamento.

In caso di dubbi in fase di verifica dei presupposti di nomina del Responsabile è possibile chiedere il parere al DPO/RPD, inviando una mail, corredata di tutte le informazioni e la documentazione necessaria, alla Funzione privacy aziendale (privacy@aslvco.it) che, effettuate le opportune verifiche e valutazioni, provvederà ad inoltrare la richiesta al DPO, mettendo in conoscenza la struttura interessata.

In via generale, la nomina del Responsabile avviene utilizzando il modello "Accordo per l'Affidamento del Trattamento dati al Responsabile del Trattamento" (cfr. Allegato 1), che, debitamente compilato dalla struttura che gestisce il contratto nelle parti variabili di competenza, dovrà essere allegato alla documentazione della procedura di affidamento in modo che gli operatori economici possano prenderne visione, compilare le sezioni di competenza, ed attestare il possesso dei requisiti di sicurezza richiesti all'art. 19 del citato modello o, in alternativa, dichiarare di impegnarsi formalmente, in caso di aggiudicazione, ad adeguare la propria struttura in tal senso.

Per informazioni sulla gestione della documentazione privacy verso operatori economici e fornitori si rinvia alle istruzioni operative "*Modalità operative di gestione informazioni privacy da rendere a operatori economici e fornitori*" (cfr. Allegato 2).

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.

In casi particolari (ad es. contratti derivanti da acquisizioni tramite centrali di committenza) è possibile adottare format di designazione ad hoc, previa acquisizione del parere del DPO/RPD.

In sede di stipula del contratto/atto giuridico, la Struttura procede alla redazione definitiva dell'Accordo di designazione, alla sottoscrizione del Direttore/Responsabile della Struttura o del Titolare ed all'acquisizione della sottoscrizione da parte del fornitore**.**

L'atto di designazione viene conservato con la documentazione di affidamento.

Il RPU dovrà quindi procedere a censire il fornitore ed il relativo trattamento nel software Data Protection Manager allegando poi l'atto di nomina a Responsabile debitamente sottoscritto. Per tale adempimento potrà avvalersi del supporto del DPO per il tramite della funzione privacy aziendale .

Tabella sintetica del processo:

AZIONE	CHI	COME	QUANDO
Valutare la necessità di designazione del Responsabile del Trattamento	Struttura che gestisce il contratto o l'atto giuridico	Applica i criteri di inclusione/esclusione	In sede di istruttoria della procedura di affidamento.
Analizzare i contratti/atti precedenti	Struttura che gestisce il contratto o l'atto giuridico	Verifica la presenza degli elementi indispensabili nella precedente nomina: natura, durata e finalità del trattamento o dei trattamenti assegnati, categorie di dati oggetto di trattamento, adeguate misure tecniche e organizzative.	Tempestivo
Richiedere parere al DPO/RPD	Struttura che gestisce il contratto o l'atto giuridico, tramite la SOC Affari Generali Legali e Istituzionali (Funzione Privacy)	In caso di dubbi sui presupposti della designazione, o qualora sia necessario supporto per la valutazione di impatto (DPIA), chiede il parere al DPO/RPD per il tramite della Funzione Privacy inviando una mail ad privacy@aslvco.it (nella quale deve essere descritto chiaramente il trattamento per il quale si chiede parere ed allegata tutta la documentazione necessaria). La SOC Affari Generali Leg. Ist. (Funzione Privacy) effettuate le opportune verifiche, inoltrerà la richiesta alla casella dedicata del DPO e, per conoscenza, alla struttura interessata.	In base a necessità
Compilare il modulo "*Accordo per l'Affidamento del Trattamento dati al Responsabile*" (cfr. Allegato 1)	Struttura che gestisce il contratto o l'atto giuridico	Compila il modulo di Accordo con le parti variabili di competenza (in base alle caratteristiche del bene/servizio da acquisire) e lo include nei documenti di gara. L'operatore economico/soggetto esterno, in fase di partecipazione alla procedura di affidamento, compila le parti di competenza del citato modello di Accordo ed attesta il possesso dei requisiti di sicurezza ivi previsti all'art. 19, o, in alternativa, dichiara di impegnarsi formalmente, sin dal momento della partecipazione alla procedura, ed in caso di aggiudicazione, ad adeguare la propria struttura in tal senso.	Nell'ambito delle attività di predisposizione degli atti per la procedura di affidamento.

AZIONE	CHI	COME	QUANDO
Gestire la sottoscrizione	Struttura che gestisce il contratto o l'atto giuridico	Dopo aver verificato che l'Accordo di nomina del Responsabile del Trattamento è completo di tutte le informazioni richieste lo sottopone alla sottoscrizione del Direttore/Resp. di Struttura e lo trasmette al fornitore/soggetto esterno per la firma.	In sede di stipula del contratto principale
Archiviare l'Accordo sottoscritto	Struttura che gestisce il contratto o l'atto giuridico	Archivia l'Accordo firmato pervenuto dal fornitore/soggetto esterno nel fascicolo relativo all'affidamento/atto giuridico	Alla ricezione
Aggiornare l'elenco dei Responsabili e il Registro dei Trattamenti	Struttura che gestisce il contratto o l'atto giuridico (RPU)	Accede al programma DPM e provvede, tramite la specifica funzionalità, a censire il Responsabile del Trattamento ed il relativo accordo ex art. 28, aggiornando altresì il registro dei trattamenti.	Tempestivo

10. GESTIONE DEL DOCUMENTO

Il responsabile per il presente documento è il Referente privacy aziendale, il quale, con il supporto del DPO ed il coinvolgimento della Funzione Privacy, provvede ad aggiornarne i contenuti nel momenti in cui se ne ravvisi la necessità. Tale procedura operativa deve essere diffusa a tutti i soggetti interessati, i quali, in funzione delle relative aree e strutture organizzative di competenza, sono tenuti a fornire pieno supporto nell'esecuzione delle attività ivi descritte.

Allegati:

1): Accordo per il Trattamento dei Dati Personali ai sensi art. 28 GDPR:

2) : Modalità operative gestione informazioni privacy da rendere a operatori economici e fornitori

3): IOP – Informativa per operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere

4) IFC – Informativa per i Fornitori /contraenti

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

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

P.I./Cod.Fisc. 00634880033

All. 1)

SPETT.LE NOME FORNITORE
in personale del legale rappresentante p.t.
Via ….. – ……
P.iva ……

Oggetto: Accordo per il trattamento dei dati personali con il Responsabile del trattamento ai sensi dell'Art. 28 del Regolamento UE Generale sulla Protezione dei Dati n. 2016/679 (GDPR – General Data Protection Regulation) e della vigente normativa di settore.

In applicazione del contratto/affidamento/convenzione/sottoscritto in data……. avente ad oggetto (SPECIFICARE DISTINTAMENTE L'OGGETTO DELLA PRESTAZIONE/SERVIZIO CON IL RIFERIMENTO CONTRATTUALE)

L'Azienda Sanitaria di ……., C.F./P.IVA . ……, con sede legale in Via ….. – ……., – Titolare del trattamento dei dati personali - considerato che:

a) L'ASL – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;
b) La designazione a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 2016/679 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;

Il presente accordo integra e specifica gli obblighi derivanti dal Contratto, in oggetto indicato, sottoscritto in data…….. (di seguito indicato il "Contratto") tra l'ASL (di seguito indicata come "Titolare"), in persona del Legale Rappresentante (o Direttore Struttura……..) e **……** (di seguito il "Fornitore" o il "Responsabile") con particolare riferimento agli obblighi di protezione dei dati;

con il presente accordo designa
ai sensi dell'art. 28 del Reg. UE 2016/679
NOME FORNITORE (o altro soggetto esterno)
quale Responsabile del Trattamento

dei dati personali trattati per conto dell'ASL in virtù del contratto denominato …….., sottoscritto in data……., ed avente ad oggetto "……", qui da intendersi integralmente riportato e trascritto

Il presente Accordo sulla Protezione dei Dati (di seguito anche ATD) si applica a tutte le attività svolte dal Responsabile nell'ambito del trattamento dei dati personali ai sensi del Regolamento UE 2016/679 (di seguito "Regolamento" o "GDPR"), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito "Codice" – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore, nell'ambito del contratto, ivi comprese le attività svolte dai propri soggetti autorizzati al trattamento o terze parti (es.: sub-responsabili), designate dal Responsabile, che trattino dati per conto del Titolare (……).
Di seguito verranno intesi il Responsabile e l'ASL congiuntamente come le "**Parti**" e ciascuna singolarmente come la "**Parte**"; ogni comunicazione al Titolare dovrà essere trasmessa al seguente indirizzo PEC : protocollo@pec.aslvco.it e per conoscenza all'Ufficio Privacy al seguente indirizzo: privacy@aslvco.it .

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

1) Il presente ATD (Accordo Trattamento Dati) si applica al trattamento dei dati personali svolto dalla NOME FORNITORE/soggetto esterno**,** in qualità di Responsabile del Trattamento per conto dell'ASL, quale Titolare del Trattamento, ai sensi della Delibera e definisce gli obblighi delle Parti in materia di tutela dei dati personali;
2) La Natura, la finalità e l'ambito del trattamento sono definiti da tutti i trattamenti di dati personali effettuati nell'esecuzione dei servizi previsti del contratto e riportati all'art. 15 del presente ATD;
3) Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali;
4) Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.
5) La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata riportata nel Contratto;
6) Nell'Ambito di Trattamento definito, il Titolare chiede al Responsabile di trattare i dati nel rispetto dei seguenti principi:
    a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
    b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
    c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
    d) 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»);
    e) 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 («limitazione della conservazione»);
    f) 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»).

Articolo 2 – Categorie di interessati

1) I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente ATD possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Titolare, terzi incaricati, a qualunque titolo, controparti contrattuali del Titolare, pazienti, familiari e cargiver e, in generale, terze parti rispetto alle quali l'ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore.

Articolo 3 – Istruzioni

1) Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite è

indicato art. 15 indicato nel presente ATD. Il presente ATD ed il contratto con i suoi allegati costituiscono parte delle istruzioni fornite dal Titolare per il trattamento dei dati personali al Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

2) Qualsiasi istruzione aggiuntiva o modificata rispetto a quanto previsto nel Contratto e nel presente ATD dovrà essere trasmessa dal Titolare al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale ulteriore istruzione diverrà efficace entro 30 giorni dalla data di comunicazione (invio).

3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Disciplinari, ecc…

4) È fatto obbligo al Responsabile di:

   a) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 del presente ATD;

   b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32 del GDPR, come previsto dall'art. 5 del presente ATD;

   c) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'art. 6 del presente ATD;

   d) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 7 del presente ATD;

   e) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'art.8 del presente ATD;

   f) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'art.9 del presente ATD;

   g) nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 28.3.b) del Reg. UE 2016/679 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione come previsto dall'art. 10 del presente ATD;

   h) ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 2016/679, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall'art. 11 del presente ATD;

   i) ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall'art. 12 del presente ATD;

   j) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 del presente ATD;

   k) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 del presente ATD;

   l) redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e degli eventuali sub-Responsabili e verificare annualmente l'ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell'assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);

   m) controllare le operazioni di trattamento svolte dagli autorizzati ed eventualmente dai sub-Responsabili e la conformità all'ambito di trattamento consentito;

n) comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento (da parte propria o dei propri sub-Responsabili), ogni richiesta, ordine o attività di controllo da parte dell'interessato, del Garante o dell'Autorità Giudiziaria. Ciò in applicazione sia dell'art. 33, par. 1 Reg. UE 2016/679 e dell'art. 1, par. 2 della L.90/2024;

o)

p) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;

q) rispettare tutto quanto ulteriormente disciplinato dal presente ATD.

Articolo 4 – Riservatezza

1) Il Responsabile si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
2) Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto (Soggetti Autorizzati e Sub-Responsabili) si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

Articolo 5 – Sicurezza del trattamento

1) Il Responsabile si impegna ad adottare tutte le misure richieste dall'Art. 32 del GDPR e le procedure tecniche e organizzative in materia stabilite dal Titolare.

2) In particolare - in considerazione dello stato dell'arte, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative identificate dal Titolare e indicate nell'art. 19 al presente ATD.

3) In caso di non completa attuazione delle misure previste nell'Art. 19, il Responsabile, entro 30 giorni dalla sottoscrizione del presente ATD, predispone un piano di implementazione finalizzato a colmare le eventuali lacune e la cui scadenza verrà concordata con il Titolare, sentito il parere del DPO e/o con la collaborazione dell'Ufficio Privacy/Protezione Dati del Titolare.

4) Quanto dichiarato e riportato negli artt. 15,16,17,18 e 19 del presente ATD, sarà soggetto, ai sensi dell'art. 28.3 lett. h) del Regolamento, ad *attività di ispezione e verifica che verranno eseguite dal titolare del trattamento o da un altro soggetto da questi incaricato*.

5) Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative previste nell'Art. 2 del presente ATD, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva idonea comunicazione, via PEC al Titolare e, per conoscenza, all'Ufficio Privacy e Sicurezza delle Informazioni, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure di cui all'Art. 2 del presente accordo.

Articolo 6 – Assistenza

1) Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nel Contratto sottoscritto dalle Parti, esso si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 15 a 22 del GDPR.

2) Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti o di uno dei sub-responsabili (ved. Art. 11 del presente ATD) uno dei diritti di cui agli Artt. da 15 a 22 del GDPR.

3) Tenendo conto della natura del trattamento, come descritto nel Contratto allegato alla Delibera e nel presente ATD, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR.

Articolo 7 – Conservazione, Riconsegna e Cancellazione

1) I dati personali trattati dal Titolare, che siano oggetto di trattamento da parte del Responsabile nell'ambito dell'esecuzione delle attività previste dal Contratto, alla cessazione del Contratto stesso, dovranno essere restituiti al Titolare entro un termine massimo di 30 giorni dalla cessazione dei servizi.

2) In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere alla cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile o del sub-responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile (o il sub-responsabile) alla conservazione dei dati personali trattati.

Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

1) Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati. Ciò in applicazione sia dell'art. 33, par. 1 Reg. UE 2016/679 e dell'art. 1, par. 2 della L.90/2024 .

2) Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

3) La comunicazione dovrà essere trasmessa all'att.ne del Titolare mediante comunicazione a mezzo PEC. Tale comunicazione dovrà essere inviata per conoscenza anche al DPO e/o all'Ufficio Privacy e Sicurezza delle Informazioni.

Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

1) Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, a fornire al Titolare ogni elemento utile all'effettuazione della valutazione di impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment), qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante ai sensi dell'art. 36 del Regolamento stesso.

Articolo 10 – Soggetti Autorizzati al Trattamento

1) Il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto e formalmente autorizzati (ex art. 2-*quaterdecies* del Codice), il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi previsti dal Contratto.

2) Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

Articolo 11 – Sub-responsabili del Trattamento

1) Per l'esecuzione di specifiche attività per conto del Titolare nell'ambito del Contratto, il Responsabile potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR (art. 28.2/28.4). I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente ATD tra il Titolare del trattamento e il Responsabile, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

2) Il Responsabile si impegna a informare anticipatamente il Titolare, a mezzo pec, laddove intenda designare o sostituire un Sub-responsabile del Trattamento. La comunicazione al Titolare dovrà contenere l'elencazione dettagliata delle attività, previste dal Contratto, affidate al sub-Responsabile e dovrà essere effettuata 15 giorni prima dell'operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 15 giorni dalla ricezione della comunicazione da parte del Responsabile.

3) Il Responsabile si impegna a informare anticipatamente, a mezzo pec, il Titolare, laddove intenda cessare il rapporto esistente con un sub-Responsabile del Trattamento senza procedere ad una sua sostituzione. Questa operazione prevede che le attività affidate al sub-Responsabile vengano riprese in carico da parte del Responsabile o riassegnate ad uno degli altri sub-Responsabili già designati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 15 giorni prima dell'operazione di cessazione.

4) Qualora il Titolare sollevi obiezioni su uno o più Sub-responsabili del Trattamento, darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, quest'ultimo potrà:
   1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni;
   2. adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).

5) L'elenco completo ed aggiornato dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto dovrà essere inviato all'indirizzo pec del Titolare entro e non oltre 30 giorni dalla sottoscrizione del presente ATD. Tale comunicazione dovrà essere inviata per conoscenza anche all'Ufficio Privacy dell'azienda.

6) Il Fornitore/soggetto esterno è responsabile nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi previsti dalla normativa vigente in materia di Protezione dei Dati Personali e dal presente ATD.

7) Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), dovrà darne preventiva comunicazione, a mezzo pec, al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

Articolo 12 – Amministratori di Sistema

1) Ove applicabile in relazione ai prodotti e servizi forniti, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

2) In riferimento ai sistemi informatici (interni o esterni alle strutture dell'Azienda Sanitaria) di trattamento dei dati del Titolare, per i quali il Responsabile (o un suo Sub-responsabile) nomini uno o più Amministratori di Sistema (di seguito anche "AdS"), il Responsabile si impegna a:
   1. designare quali Amministratori di Sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
   2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
   3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
   4. comunicare periodicamente (almeno una volta l'anno, entro e non oltre il 31/12) al Titolare l'elenco aggiornato degli Amministratori di Sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) ed i dati di contatto per l'attivazione di eventuali procedure di emergenza;
   5. comunicare tempestivamente (entro 3 giorni dall'ingresso, sostituzione o cessazione degli AdS) al Titolare eventuali variazioni che saranno riportate nell'elenco, specificando eventuali ingressi, sostituzioni o cessazioni, l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) e le eventuali credenziali di autenticazione introdotte o dismesse e, solo per i nuovi AdS, i dati di contatto per l'attivazione di eventuali procedure di emergenza;
   6. verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
   7. conservare, ove di competenza, i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili) o renderli disponibili per la conservazione da parte del Titolare (qualora i sistemi siano installati presso le strutture del Titolare);
   8. garantire una rigida separazione dei compiti tra chi autorizza e/o assegna i privilegi di accesso (credenziali di Amministratore) e chi effettua le attività tecnico-sistemistiche sui medesimi sistemi.

Articolo 13 – Rapporti con le Autorità

1) Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

Articolo 14 – Ulteriori Obblighi e Responsabilità

1) Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente ATD.

2) Il titolare effettuerà verifica delle dichiarazioni rese nel presente accordo dal responsabile per tutto il periodo di vigenza contrattuale, e se del caso anche prima dell'avvio del contratto stesso. L'inosservanza delle prescrizioni presenti nel presente accordo potrà comportare la risoluzione del contratto fra le parti ed ogni conseguenza per quanto previsto dalla normativa vigente.

3) Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

4) Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

5) Il Responsabile si impegna altresì a:
   1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e relativi adempimenti eseguiti) ed alle conseguenti risultanze;
   2. collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
   3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
   4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia o ritenga a suo parere che il trattamento dei Dati Personali violi la normativa vigente o presenti, comunque, rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato.

6) Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità (art. 28.10 del Regolamento).

Articolo 15 – Descrizione dettagliata dell'attività oggetto di trattamento

Al fine di valutare l'attività che si intende adeguare alla normativa vigente in materia di protezione dei dati personali, il Titolare descrive brevemente il contesto in cui in cui avviene il trattamento. Le informazioni fornite serviranno anche per la redazione dei documenti necessari a soddisfare i requisiti cogenti posti dalla legge, ovvero il registro dei trattamenti del titolare e l'informativa del trattamento. Il documento di riferimento è la Procedura per la Gestione delle nomine dei Responsabili del Trattamento. Per la consultazione dei riferimenti normativi citati si rimanda al seguente link https://www.garanteprivacy.it/garante/document?ID=6264597

Cod.	Voce	Descrizione
1	**AMBITO DI TRATTAMENTO**	
1.1	Descrivere l'attività che si intende effettuare, in ogni fase, nel suo completo ciclo di vita. Art. 30, par. 1, lett. a) GDPR	DESCRIVERE ATTIVITA' TRATTAMENTO
1.2	Descrivere quali attività di trattamento vengono complessivamente svolte da tutti i soggetti coinvolti Artt.4, par.2, 30, par. 1, lett. a) GDPR	[ ] Raccolta [ ] Registrazione [ ] Organizzazione [ ] Strutturazione [ ] Conservazione [ ] Adattamento o Modifica [ ] Estrazione [ ] Consultazione [ ] Uso [ ] Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione [ ] Raffronto o Interconnessione [ ] Limitazione [ ] Cancellazione o Distruzione [ ] Trasferimento verso un paese terzo o una organizzazione internazionale
1.3	Quali sono le finalità del trattamento? Art. 30, par. 1, lett. b) GDPR	[ ] a) Diagnosi e cura [ ] b) Ricerca scientifica [ ] c) Gestione del personale [ ] d) Obbligo legale (indicare la legge):_____ [ ] e) Altro:_fruizione di servizi di mobilità aziendale per flotte e privati
1.4	Quali sono le categorie delle persone interessate dal trattamento? (es. assistiti, clienti, fornitori, dipendenti) Art. 30, par. 1, lett. c) GDPR	[ ] a) Dipendenti/Collaboratori [ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali) [ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori [ ] d) Soggetti che ricoprono cariche sociali [ ] e) Beneficiari o assistiti [ ] f) Assistiti [ ] g) Minori [ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) [ ] i) Altro:_____
1.5	Quali sono le categorie di dati personali trattati? (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati) Art. 30, par. 1, lett. c) GDPR	[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) [ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) [ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…) [ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) [ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)

		[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza [ ] g) Dati di profilazione [ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) [ ] i) Dati relativi all'ubicazione [ ] l) Dati che rivelano l'origine razziale o etnica [ ] m) Dati che rivelano le opinioni politiche [ ] n) Dati che rivelano le convinzioni religiose o filosofiche [ ] o) Dati che rivelano l'appartenenza sindacale [ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale [ ] q) Dati relativi alla salute [ ] r) Dati genetici [ ] s) Dati biometrici [ ] t) Altro. Indicare:
1.6	Chi sono tutti i soggetti coinvolti in ogni fase, nel suo completo ciclo di vita, del trattamento? (es. fornitori, altri enti convenzionati) Art. 30, par. 1, lett. d) GDPR	[ ] a) Destinatari interni dipendenti e collaboratori _____ [ ] b) Fornitori (indicare la denominazione se nota) _____ [ ] c) Altri Enti (indicare la denominazione) Soggetti erogatori servizi finali, quali Comuni, Regioni, Altre Autorità Sanitarie [ ] d) Altro:_____
1.7	Qual è la durata prevista del trattamento? (es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione") Art. 30, par. 1, lett. f) GDPR	[ ] a) 10 anni dalla cessazione del trattamento principale [ ] b) Come da massimario di scarto aziendale [ ] b) Altro (indicare la durata) :_____
1.8	Dove vengono trattati i dati? Art. 30, par. 1, lett. e) GDPR	[ ] a) All'interno dell'Unione Europea [ ] b) Altro (indicare la località) :_____
1.9	Specificare la natura e le modalità del trattamento. (es. trattamento dati in formato cartaceo, trattamento informatizzato con archivio digitale) Art. 24, 25, 32 GDPR	[ ] a) Trattamento su supporti cartacei (riportare il dettaglio in descrizione al punto 1.1) [ ] b) Trattamento informatizzato (riportare il dettaglio in descrizione al punto 1.1)
1.10	Nel caso in cui i dati personali non siano raccolti presso l'Interessato, specificare la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico Art. 14, par. 2, lett. g) GDPR	[ ] a) I dati vengono forniti direttamente dalla persona interessata [ ] b) I dati della persona interessata vengono forniti da un altro soggetto (indicare la denominazione):_
1.11	Quali strumenti vengono utilizzati nel trattamento? Art. 24, 25, 32 GDPR	[ ] a) Dispositivo/Apparecchiatura (indicare la denominazione)__ [ ] b) Sistema (indicare la denominazione) _____ [ ] c) Software (indicare la denominazione) [ ] d) Altro (indicare la denominazione) _____
1.12	Quali misure di sicurezza sono presenti nel trattamento?	[ ] a) I dati sono trattati in misura minima [ ] b) La comunicazione dei dati avviene in modo protetto [ ] c) I fornitori hanno fornito una DPIA – Valutazione d'impatto

	Art. 24, 25, 32 GDPR	[ ] d) I fornitori hanno la certificazione ISO27001 [ ] e) I fornitori hanno designato il Responsabile della Protezione dei Dati [ ] f) Altro (indicare quali)_____

Articolo 16 – Recapiti della persona referente e del Responsabile della Protezione dei Dati (DPO) del Responsabile del trattamento

Nome e Recapito telefonico del referente	
Indirizzo E-mail del referente	
Indirizzo PEC del referente	
Recapito del DPO (1)	

(1) ove il responsabile della protezione dei dati non sia stato designato ai sensi dell'art. 37 del GDPR, il responsabile del trattamento allega al presente documento copia del documento attestante le valutazioni effettuate a tal proposito

Articolo 17 – Soggetti sub-responsabili

ID	Ragione sociale	Sede legale	E-mail/PEC	Recapito del DPO	Ambito di trattamento
1					
2					
3					
Ultimo aggiornamento dell'allegato			_____ /_____ /_____		
[ ] Il responsabile del trattamento NON affida a sub-fornitori attività che implichino trattamento di dati personali					

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

Articolo 18 – Amministratori di sistemi

ID	Nome e Cognome [1]	Ragione Sociale [2]	Recapito E-mail/Telefono	Sistemi Amministrati
1				
2				
3				
4				
Ultimo aggiornamento dell'elenco			____/____/____	

[1] se soggetti autorizzati ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03 e dell'art. 29 del Reg. UE 2016/679
[2] se soggetti individuati quali sub-responsabili ai sensi dell'art. 28, parr. 2 e 4, del Regolamento UE 2016/679

[ ] Il responsabile del trattamento NON svolge attività che implichino il ruolo di Amministratore Di Sistema

Articolo 19 – Principi, Diritti e Misure Tecniche e Organizzative – Requisiti/Schede di Audit

Si indicano, in base alla loro applicabilità in relazione al servizio erogato per conto del Titolare, i principi di trattamento, le misure di sicurezza e i diritti degli interessati, secondo le indicazioni del Regolamento UE 2016/679, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) unitamente alle misure di sicurezza previste, per i quali il responsabile si impegna con la sottoscrizione del presente atto.
Le indicazioni fornite nel presente allegato relative alle misure di sicurezza sono estrapolate dalle Linee Guida ENISA relative alla sicurezza dei trattamenti di dati personali: esse dovranno essere riportate all'interno del Registro dei Trattamenti del Responsabile.

1) Principi di Trattamento e Diritti degli Interessati

Req.	**Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)**
A.1	Art. 5.1.b – Misure per garantire la limitazione della finalità del trattamento (dati non utilizzati per altre finalità)
A.2	Art. 5.1.c – Misure per garantire la minimizzazione dei dati del trattamento
A.3	Art. 5.1.d – Misure per garantire la esattezza/qualità dei dati
A.4	Art. 5.1.e – Misure per garantire la limitazione della conservazione
A.5	Art. 15 – Misure per garantire il diritto di Accesso dell'interessato

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)
A.6	Art. 16 – Misure per garantire il diritto di Rettifica
A.7	Art. 17 – Misure per garantire il diritto alla Cancellazione (“Oblio”) – ove applicabile
A.8	Art. 18 – Misure per garantire il diritto alla Limitazione del Trattamento
A.9	Art. 19 – Misure per garantire l’obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento
A.10	Art. 20 – Misure per garantire il diritto alla portabilità dei dati – ove applicabile
A.11	Art. 21 – Misure per garantire il diritto di Opposizione
A.12	Art. 22 - Misure per garantire la sicurezza in caso di processo decisionale automatizzato relativo alle persone fisiche, compresa la *profilazione*

2) Misure di Sicurezza

Il perimetro di sicurezza definito come ambito di applicazione delle misure di sicurezza di seguito elencate è costituito dal servizio effettuato dal Responsabile per conto dell’ASL; di conseguenza le seguenti misure sono applicabili all’organizzazione, alle informazioni/dati, agli strumenti HW, SW e di rete ed al personale coinvolti nell’erogazione del servizio contrattualizzato.
Le presenti misure di sicurezza verranno utilizzate quale riferimento per l’esecuzione degli audit previamente concordati.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Politiche di sicurezza e procedure per la protezione dei dati personali	1.1	Il Responsabile deve disporre di una propria regolamentazione (o politica di sicurezza) in materia di protezione dei dati personali conforme alla normativa vigente e che disciplini i servizi erogati per conto del Titolare.
	1.2	La regolamentazione di cui al punto precedente deve essere riesaminata e aggiornata almeno su base annuale.
	1.3	La regolamentazione deve essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.
	1.4	La regolamentazione deve disciplinare almeno i seguenti punti: ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili e sub-responsabili del trattamento dei dati e per le altre terze parti coinvolte nel trattamento dei dati personali.
Ruoli e responsabilità	2.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.
	2.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
	2.3	Deve essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Riservatezza del personale	3.1	Il Responsabile deve garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di attivazione del Servizio/Contratto.
	3.2	Prima di assumere i propri compiti, il personale del Responsabile deve essere invitato a riesaminare e concordare la Regolamentazione di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
Formazione	4.1	Il Responsabile deve garantire che tutto il personale sia adeguatamente formato sui controlli di sicurezza previsti per il servizio e per gli eventuali sistemi informatici ad esso correlati. Il personale coinvolto nel trattamento dei dati personali deve inoltre essere adeguatamente informato e periodicamente aggiornato in merito ai requisiti in materia di protezione dei dati e agli obblighi previsti dalla normativa vigente attraverso regolari campagne di sensibilizzazione.
	4.2	Il Responsabile deve disporre programmi di formazione (relativi alla protezione dei dati personali e alla sicurezza delle informazioni) strutturati e regolari per il proprio personale, compresi programmi specifici per l'inserimento di eventuali nuovi arrivati (es.: job rotation, nuove assunzioni, ecc...).
Politica controllo accessi	5.1	Specifici diritti di accesso devono essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
	5.2	Deve essere definita una politica di controllo degli accessi. Nel documento l'organizzazione deve determinare le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.
	5.3	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata.
Controllo accessi e autenticazione	6.1	Ove fornita dall'Organizzazione, deve essere attuata la politica di controllo accessi applicabile a tutti gli utenti che accedono ai sistemi IT, con particolare riguardo agli aspetti relativi alla creazione, approvazione, riesame ed eliminazione degli account.
	6.2	L'uso di account generici (non personali) deve essere evitato. Nei casi in cui ciò sia necessario, l'utilizzo deve essere autorizzato dal referente dell'Organizzazione. Qualora tale autorizzazione fosse fornita, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
	6.3	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, deve essere presente un meccanismo di autenticazione che consenta l'accesso che sia in linea con la politica di controllo degli accessi ove fornita dall'Organizzazione. Come minimo deve essere utilizzata una combinazione di user-id e password.
	6.4	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, il sistema di controllo degli accessi deve essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano i criteri definiti al punto precedente.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	6.5	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio deve essere possibile configurare i seguenti parametri relativi alle password: complessità, maximum age, password history, lunghezza e il numero di tentativi di accesso non riusciti accettabili. I criteri dovranno essere concordati con il referente dell'Organizzazione (in base alla politica di controllo accessi).
Gestione risorse e degli asset	7.1	Deve essere predisposto un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete), in funzione di quanto applicabile al servizio esternalizzato. Il compito di mantenere e aggiornare il registro deve essere esplicitamente assegnato.
	7.2	Le risorse IT all'interno del registro essere riesaminate e aggiornate regolarmente.
	7.3	I ruoli che hanno accesso alle risorse devono essere definiti e documentati. In particolare devono essere definite le responsabilità in relazione alle risorse.
Sicurezza fisica	8.1	Il perimetro fisico dei locali in cui è ospitata l'infrastruttura IT utilizzata a fini di erogazione del servizio o vengono effettuati trattamenti di dati personali del Titolare deve essere accessibile esclusivamente a personale esplicitamente autorizzato da parte del Responsabile.
	8.2	Il personale autorizzato all'accesso ai locali di trattamento o ai locali in cui è ospitata l'infrastruttura IT per l'erogazione del servizio deve essere dotato di strumenti di identificazione personali (es. badge identificativi, PIN personali).
	8.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Deve essere mantenuto e monitorato in modo sicuro un registro fisico o una traccia elettronica del controllo di tutti gli accessi.
	8.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.
	8.5	Dovrebbero essere predisposte barriere fisiche per impedire l'accesso fisico non autorizzato.
	8.6	Le aree dei locali non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate.
	8.7	Nella sala server devono essere predisposti opportuni sistemi antincendio automatici, sistemi dedicati di climatizzazione e gruppi di continuità (UPS) che garantiscano l'erogazione sicura del servizio secondo quanto stabilito contrattualmente.
	8.8	Il personale di supporto esterno deve avere accesso limitato alle aree protette.
Change management	9.1	L'organizzazione deve adottare un processo di cambiamento che consenta di assicurarsi che tutte le modifiche al sistema/servizio siano opportunamente registrate (anche con eventuali aggiornamenti dell'inventario delle risorse) e monitorate.
	9.2	Ogni Cambiamento al sistema/servizio deve essere previamente segnalato al referente interno dell'organizzazione (committente) e da questi autorizzato. Nella segnalazione devono essere documentati: gli estremi del cambiamento (es.: cambiamento di versione), le tempistiche, eventuali prescrizioni aggiuntive che prevedano azioni da adottare prima che il cambiamento sia operativo (es.: formazione utenti).

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	9.3	Lo sviluppo del software deve essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali in produzione. Quando è necessario eseguire i test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, il fornitore deve predisporre specifiche procedure per la protezione dei dati personali utilizzati nei test.
Logging e monitoraggio	10.1	I log devono essere attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	10.2	I log devono essere registrati e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica fonte temporale di riferimento (server NTP).
	10.3	È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.
	10.4	Non deve essere possibile la cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio effettuato per la rilevazione di attività insolite.
	10.5	Deve essere configurato un sistema di monitoraggio per l'elaborazione dei log e la produzione di rapporti sullo stato del sistema e notifica di potenziali allarmi.
Protezione dal malware	12.1	Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
Backup	14.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità; devono essere definite e documentate le strategie di backup da applicare ai dati in maniera coerente con il livello di criticità (RPO) dei servizi a cui afferiscono
	14.2	Ai backup deve essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	14.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	14.4	Le strategie di backup definite devono essere completate regolarmente.
	14.5	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati.
	14.7	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.
	14.8	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare dei dati.
Sicurezza Server e Database	15.1	I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	15.2	I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione.
	15.3	Nei sistemi utilizzati per l'erogazione del servizio, devono essere considerate soluzioni di crittografia per i dati at rest, in transit e in use.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		Qualora non ritenute applicabili, deve essere data adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati
	15.4	Nei sistemi utilizzati per l'erogazione del servizio, ove possibile, devono essere applicate tecniche di pseudonimizzazione attraverso la separazione dei dati dagli identificatori al fine di evitare il collegamento diretto con l'interessato. In caso non fosse possibile, deve essere fornita adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati.
Network/ Communication security	16.1	Deve essere predisposta e monitorato il rispetto di una policy per la Sicurezza di Rete (Network Security Policy) e per la gestione delle Comunicazioni Sicure (Network Communication Security) che preveda l'adozione di misure di cifratura delle comunicazioni nell'ambito dei processi di trattamento effettuati (TLS/Https, VPN, SSH, ecc…).
Sicurezza desktop/laptop/mobile	17.1	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza.
	17.2	Le applicazioni anti-virus e le relative signatures devono essere configurate regolarmente in maniera continuativa.
	17.3	Gli utenti non devono avere i privilegi per installare applicazioni software non autorizzate o disattivare applicazioni autorizzate
	17.4	I sistemi utilizzati per l'erogazione del servizio, devono disporre di un timeout di sessione nel caso in cui l'utente non sia stato attivo per un determinato periodo di tempo (max 10 min).
	17.5	Gli aggiornamenti critici di sicurezza rilasciati dalle case produttrici di software di sistema devono essere installati regolarmente.
	17.6	Non è consentito il trasferimento di dati personali dai Database dei sistemi aziendali alle workstation utilizzate a fini di assistenza tecnica, se non previa esplicita autorizzazione del Responsabile dei Sistemi Informativi. I dati temporaneamente memorizzati devono essere cancellati alla fine della sessione di lavoro.
	17.7	Non deve essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	17.8	Deve essere abilitata la crittografia dei dischi delle postazioni di lavoro/laptop/device mobili utilizzate nell'ambito dell'erogazione del servizio
Dispositivi portatili	18.1	Le procedure di gestione dei dispositivi mobili e portatili devono essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	18.2	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati: non è consentito l'utilizzo di dispositivi personali, salvo eventuali specifiche autorizzazioni.
	18.3	I dispositivi mobili devono essere soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali (client).
	18.4	Il Responsabile deve individuare e comunicare al Titolare un proprio referente a cui attribuire la responsabilità della gestione dei dispositivi mobili e portatili utilizzati nell'ambito dell'erogazione del servizio.
	18.5	Il Responsabile deve essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso, nel caso in cui questo

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		sia utilizzato nell'ambito dell'erogazione del servizio.
	18.6	In caso di utilizzo promiscuo dei dispositivi mobili (fini di erogazione del servizio al titolare e fini privati) deve essere prevista, mediante opportuni software containers sicuri, la separazione dell'uso privato dall'uso aziendale del dispositivo.
	18.7	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
Sicurezza del ciclo di vita delle applicazioni	19.1	Lo sviluppo degli applicativi deve essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID.
Sub-responsabile del trattamento	20.1	Il Responsabile ed i suoi sub-responsabili adottano le linee guida e le procedure relative al trattamento dei dati personali contenute nell'atto di designazione e nei suoi allegati (tra cui il presente documento).
	20.2	Il Responsabile del Trattamento deve osservare le indicazioni fornite nell'atto di designazione in caso di violazione di dati personali e nelle presenti misure di sicurezza.
	20.3	Il Responsabile deve sottoscrivere l'atto di designazione in cui sono contenuti requisiti formali e obblighi. Il Responsabile del trattamento deve, in risposta, fornire prove documentate sufficienti di conformità (es.: certificazioni di sicurezza, schede tecniche relative alle misure di sicurezza adottate per il servizio/sistema): in caso alternativo, verrà adottata una specifica politica di auditing.
	20.4	Il Responsabile dovrebbe verificare regolarmente la conformità del sub-responsabile al livello concordato di requisiti e obblighi.
	20.5	Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione.
Gestione degli incidenti / Violazione dei dati personali	21.1	Il Responsabile deve predisporre un proprio piano di risposta agli incidenti con procedure dettagliate che preveda la comunicazione al titolare (committente), secondo le indicazioni fornite nell'atto di designazione, al fine di garantire una risposta efficace e ordinata agli incidenti e violazioni relativi ai dati personali.
	21.2	Le violazioni dei dati personali, di competenza del Titolare, devono essere segnalate immediatamente alla Direzione. In qualità di Responsabile devono essere adottate specifiche procedure di supporto al Titolare per la notifica e la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
	21.3	La procedura di gestione delle violazioni di cui al punto precedente, deve essere documentata: essa deve includere un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.
	21.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.
Business Continuity	22.1	Il Responsabile deve predisporre un proprio Piano di Continuità Operativa (BCP - Business Continuity Plan) in relazione all'erogazione dei servizio, in linea con quanto previsto dall'Organizzazione (Committente). Tale Piano deve stabilire procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del servizio (ad es.: in caso di incidente / violazione dei dati personali o interruzione del servizio).

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	22.2	Il Piano di Continuità Operativa indicato al punto precedente deve includere azioni chiare e assegnazione di ruoli.
	22.3	Il Piano di Continuità Operativa deve essere in linea con il livello di qualità del servizio da garantire all'Organizzazione (Committente), con particolare riguardo alla sicurezza dei dati personali dei processi fondamentali di erogazione.
Cancellazione/ eliminazione dei dati	23.1	I supporti di memorizzazione da dismettere devono essere distrutti fisicamente; in caso in cui ciò non sia possibile (es.: per indicazioni contrattuali relative all'assistenza dei dispositivi), prima della loro eliminazione (o riconsegna al fornitore) devono essere sottoposti a tecniche di distruzione dei dati (es.: ripetute operazioni di sovrascrittura con tecniche di clearing/purging).
	23.2	La distruzione di documenti deve avvenire mediante opportuni dispositivi di triturazione.
	23.3	Se sono utilizzati servizi di terzi per eliminare in modo sicuro i supporti di memorizzazione o documenti cartacei, è necessario stipulare uno specifico contratto di servizio e produrre un formale attestato di distruzione.

Articolo 20 – Disposizioni Finali

1) La presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto.
2) Gli allegati al presente ATD fanno parte integrante dello stesso: essi costituiscono parte integrante del Registro dei Trattamenti del Responsabile e dovranno essere mantenuti aggiornati da parte del Responsabile.
3) La mancata sottoscrizione del presente accordo non consentirà di dare attuazione di quanto previsto nel Contratto.
4) Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/12 di ogni anno.
5) Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente ATD, costituisce una violazione del Contratto, di cui il presente ATD è parte integrante, del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018) oltre che di quanto disposto dalla normativa vigente.
6) Il presente Accordo sulla Protezione dei Dati Personali, deve essere restituito, opportunamente sottoscritto digitalmente entro 7 giorni dal ricevimento a mezzo PEC. La restituzione dovrà anch'essa essere effettuata a mezzo PEC all'indirizzo fornito dal Titolare ed indicato in premessa.
   Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Luogo, _____data_____

Il titolare del trattamento

_____

Per ricezione ed integrale accettazione del Responsabile

_____

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)

MODALITÀ OPERATIVE GESTIONE INFORMAZIONI PRIVACY DA RENDERE A OPERATORI ECONOMICI E FORNITORI

PREMESSA: La seguente istruzione operativa è rivolta alle Strutture aziendali che gestiscono procedure di affidamento di beni e servizi ed ha lo scopo di fornire indicazioni per la corretta gestione delle informazioni privacy.
Il soggetto fornitore all'interno dell'organizzazione privacy dell'ASL può assumere il duplice ruolo di:

a) soggetto passivo, quale **interessato** del titolare del trattamento. Tale situazione si verifica nella totalità dei casi, dal momento che, ogni qualvolta il titolare del trattamento per l'acquisizione di beni e servizi decide di affidarsi a fornitori/soggetti esterni, tratta necessariamente dati personali dei soggetti selezionati con riferimento alle persone fisiche di cui raccoglie i dati;

b) soggetto attivo, quale **responsabile del trattamento**. Tale situazione si verifica esclusivamente nei casi in cui il fornitore aggiudicatario dell'affidamento tratta dati personali per conto del titolare del trattamento.
In tale ipotesi il fornitore/responsabile del trattamento rientra nell'organizzazione privacy dell'ente e come tale deve essere designato formalmente Responsabile del trattamento. Per le indicazioni di dettaglio sui criteri e le modalità di gestione della designazione a Responsabile del trattamento si rinvia alla specifica procedura *(Procedura per la gestione dei Responsabili del Trattamento di dati personali).*

In relazione alla situazione di soggetto passivo, il Titolare del trattamento è tenuto a rendere edotti i potenziali fornitori e/o fornitori contraenti, in qualità di interessati, dei trattamenti messi in atto con riguardo ai loro dati personali, nonché in merito alle finalità del trattamento stesso; pertanto gli operatori economici (fornitori potenziali) che partecipano alle procedure per l'affidamento di servizi, lavori, forniture e opere, siano esse ad evidenza pubblica o di altra tipologia, dovranno ricevere l'informativa **"IOP – Informativa per Operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere"** *(cfr. Allegato 3).*
Le indicazioni privacy e il riferimento all'informativa saranno gestite nella documentazione di gara al paragrafo dedicato al trattamento dei dati personali con i seguenti testi tipo:

"Testo 1" – procedura per affidamento che non implica la nomina a Responsabile del Trattamento
"L'Azienda ASL VCO con sede legale in Via Mazzini n. 117, CAP 28887 Omegna (VB), PEC: protocollo@pec.aslvco.it in qualità di Titolare del trattamento fornisce informazioni agli operatori economici, con riguardo al trattamento dei dati personali conferiti nell'ambito della partecipazione a procedure di affidamento di servizi, forniture, lavori e opere. Ai sensi degli artt. 13 e 14 del Regolamento UE n.679 del 2016 in materia di protezione dei dati personali e in attuazione del D.lgs. 101 del 2018, i dati conferiti [dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità, dati di contatto, informazioni inerenti il nucleo familiare) e giudiziari (eventuali condanne penali, iscrizione nel casellario giudiziale) del Titolare dell'impresa partecipante o del/i soggetto/i munito/i dei poteri di rappresentanza, ivi compresi institori e procuratori generali; ove previsto dalla Legge, i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità) e giudiziari dei soci e del direttore tecnico dell'impresa partecipante (eventuali condanne penali, iscrizione nel casellario giudiziale); ove applicabile, i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità) e giudiziari dei soggetti cessati dalla carica nell'anno antecedente la pubblicazione del bando (eventuali condanne penali, iscrizione nel casellario giudiziale), saranno trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ed esclusivamente per le finalità della presente procedura come meglio dettagliato nell'informativa ***"IOP – Informativa per Operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere".***
Il Responsabile per la protezione dei dati personali (RPD) o Data Protection Officer dell'ASL VCO è contattabile all'indirizzo di posta elettronica dpo@aslvco.it ".

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

"Testo 2" – procedura per affidamento che implica la nomina a Responsabile del Trattamento
"L'Azienda ASL VCO con sede legale in Via Mazzini n. 117, CAP 28887 Omegna (VB), PEC: protocollo@pec.aslvco.it , in qualità di Titolare del trattamento fornisce informazioni agli operatori economici, con riguardo al trattamento dei dati personali conferiti nell'ambito della partecipazione a procedure di affidamento di servizi, forniture, lavori e opere. Ai sensi degli artt. 13 e 14 del Regolamento UE n.679 del 2016 in materia di protezione dei dati personali e in attuazione del D.lgs. 101 del 2018, i dati conferiti [dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità, dati di contatto, informazioni inerenti il nucleo familiare) e giudiziari (eventuali condanne penali, iscrizione nel casellario giudiziale) del Titolare dell'impresa partecipante o del/i soggetto/i munito/i dei poteri di rappresentanza, ivi compresi institori e procuratori generali; ove previsto dalla Legge, i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità) e giudiziari dei soci e del direttore tecnico dell'impresa partecipante (eventuali condanne penali, iscrizione nel casellario giudiziale); ove applicabile, i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità) e giudiziari dei soggetti cessati dalla carica nell'anno antecedente la pubblicazione del bando (eventuali condanne penali, iscrizione nel casellario giudiziale), saranno trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ed esclusivamente per le finalità della presente procedura come meglio dettagliato nell'informativa ***"IOP – Informativa per Operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere".***
In ragione dell'oggetto della presente procedura, il Fornitore è chiamato ad eseguire attività di trattamento di dati personali, per conto dell'Amministrazione contraente e, pertanto, lo stesso sarà nominato ***"Responsabile del trattamento",*** *ai sensi dell'art. 28 del Regolamento UE; a tal fine, esso si impegnerà ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto disposto dall'art. 5 del Regolamento UE, limitandosi ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti.*
In particolare gli aspetti connessi alla protezione dei dati personali, derivanti dal rapporto contrattuale, saranno indicati nell'"Accordo per il Trattamento dei Dati Personali ai sensi art. 28 GDPR" (Allegato 1), che dovrà essere sottoscritto successivamente all'affidamento.

L'operatore economico/soggetto esterno, in riferimento alla partecipazione alla presente procedura, attesta di essere in possesso dei requisiti di sicurezza previsti dall'art. 19 del modello di Accordo per il Trattamento dei Dati personali (incluso nei documenti di gara) o, in alternativa, di impegnarsi formalmente, sin da ora, ed in caso di aggiudicazione, ad adeguare la propria struttura in tal senso.

Il Responsabile per la protezione dei dati personali (RPD) o Data Protection Officer dell'ASL VCO è contattabile all'indirizzo di posta elettronica dpo@aslvco.it.".

Solo nel caso intervenga un'aggiudicazione e/o un affidamento a loro favore, i fornitori dovranno essere edotti altresì, delle informazioni riguardanti gli ulteriori trattamenti che saranno messi in atto e inerenti più specificatamente gli aspetti contrattuali e dovranno ricevere l'informativa "IFC – Informativa per i Fornitori/Contraenti" (cfr. Allegato 4).

Le indicazioni privacy e il riferimento all'informativa saranno gestite nel contratto in corrispondenza del paragrafo dedicato al trattamento dei dati personali con i seguenti testi tipo:

"Testo 3" – contratto per affidamento che non implica la nomina a Responsabile del Trattamento
"In riferimento al Regolamento UE 679/2016 (GDPR) e al D.lgs.196/2003, come novellato dal D.lgs. 10 agosto 2018, n. 101, le parti si impegnano ad improntare il trattamento dei dati personali ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente e con particolare attenzione a quanto prescritto circa le misure di sicurezza da adottare.
L'ASL VCO, in qualità di Titolare del trattamento, fornisce al contraente le informazioni relative al trattamento dei dati personali che lo riguardano, ai sensi degli artt. 13 e 14 del Regolamento Europeo 679/2016, come da Informativa resa al medesimo soggetto ("IFC - Informativa per i Fornitori/Contraenti")".

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

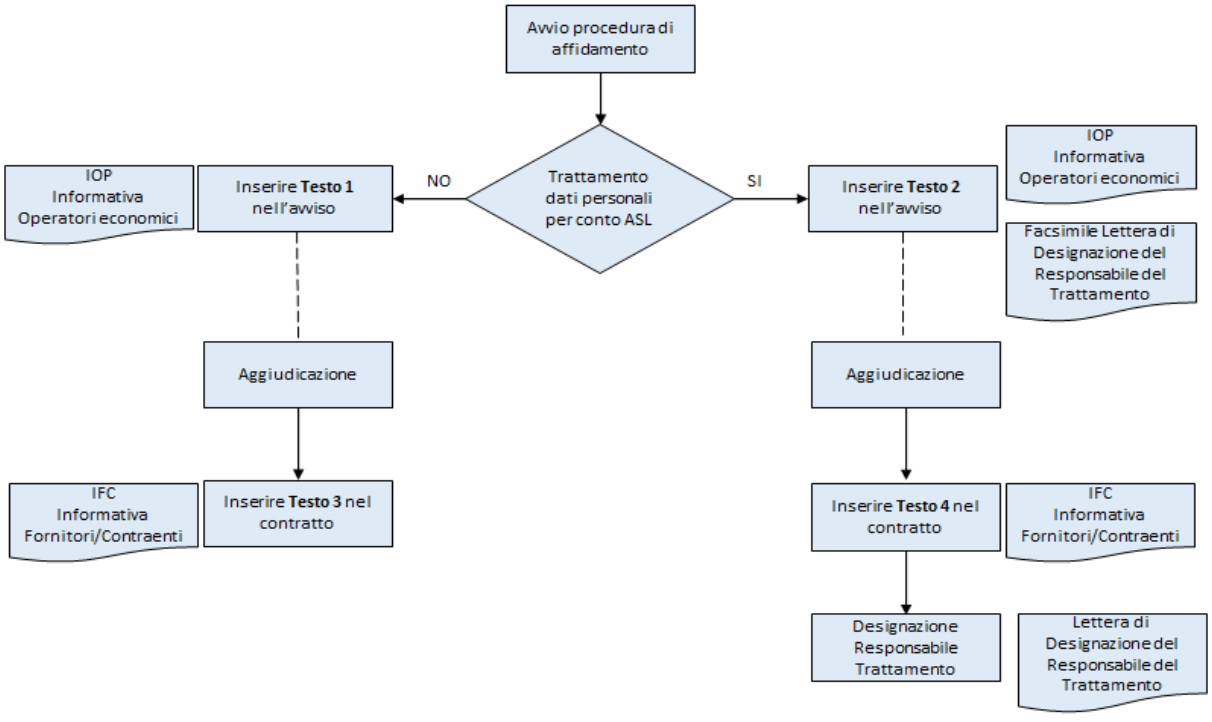
"Testo 4" – contratto per affidamento che implica la nomina a Responsabile del Trattamento

"In riferimento al Regolamento UE2016/679 (di seguito GDPR) e al D.lgs. n. 196/2003, come novellato dal D.lgs. n. 101/2018, le Parti si impegnano ad improntare il trattamento dei dati personali ai principi di correttezza, liceità e trasparenza, con particolare attenzione all'adozione di misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento dei dati personali svolto.

Ai sensi degli art. 13 e 14 del sopracitato Regolamento, la medesima controparte negoziale è informata, come meglio specificato nell'informativa "IFC - Informativa per i Fornitori/Contraenti", che i dati personali, raccolti direttamente presso l'interessato oppure ottenuti presso altre fonti, saranno utilizzati dall'ASL VCO, Titolare del Trattamento ai soli fini contrattuali. Il trattamento dei suddetti dati è funzionale, necessario, pertinente e, in ogni modo, non incompatibile con le finalità per le quali gli stessi sono raccolti come descritto nell'informativa resa all'interessato/contraente.
L'ASL VCO, in qualità di Titolare del trattamento, in relazione al trattamento dei dati di cui al presente contratto, incarica il Contraente quale Responsabile del Trattamento con atto di designazione. Lo scopo di tale atto è quello di vincolare il responsabile del trattamento al Titolare e di disciplinare le condizioni del trattamento dei dati personali, eseguito per conto del Titolare, nel rispetto dei relativi obblighi di legge. In particolare, gli aspetti connessi alla protezione dei dati personali, derivanti dal rapporto contrattuale, saranno indicati nell'"Accordo per il Trattamento dei Dati Personali ai sensi art. 28 GDPR" . (allegato 1)

Si precisa che, laddove le procedure di affidamento fossero espletate e gestite da Centrali di Committenza o tramite il Mercato Elettronico della Pubblica Amministrazione, sarà cura di tali Enti fornire le proprie informative e l'ASL VCO interverrà nel processo rendendo l'informativa appropriata solo in caso di aggiudicazione.

Flow chart che sintetizza le indicazioni fornite:



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)

IOP – Informativa per operatori economici che partecipano a procedure di affidamento di servizi, forniture, lavori e opere (art. 13 e 14 regolamento UE 2016/679)

La presente informativa, resa ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 – General Data Protection Regulation, è destinata agli operatori economici (persone fisiche o soggetti che operano in nome e per conto di persone giuridiche) che partecipano alle procedure per l'affidamento di servizi, forniture, lavori e opere dell'Azienda Sanitaria Locale VCO (in seguito "ASL VCO").

1.Titolare del trattamento

Titolare del trattamento è l'ASL VCO, con sede in Via Mazzini n. 117 – 28887 Omegna (VB), PEC: protocollo@pec.aslvco.it sito internet: www.aslvco.it , P.I./Cod. Fisc. 00634880033.

2. Responsabile della protezione dati (RPD o DPO)

Il Responsabile per la Protezione dei Dati (RPD/DPO) designato dal Titolare del trattamento è contattabile all'indirizzo e-mail: dpo@aslvco.it

3. Tipologia dei dati raccolti

Nell'ambito della procedura di gara per la conclusione di contratti di fornitura di lavori, beni e servizi, l'ASL VCO tratta i dati personali presenti nella domanda di partecipazione o contenuti nei documenti acquisiti da altre pubbliche amministrazioni in ottemperanza agli adempimenti di Legge e, in particolare:
- i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità, dati di contatto, informazioni inerenti il nucleo familiare) e giudiziari (eventuali condanne penali, iscrizione nel casellario giudiziale) del Titolare dell'impresa partecipante o del/i soggetto/i munito/i dei poteri di rappresentanza, ivi compresi institori e procuratori generali;
- ove previsto dalla Legge, i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità) e giudiziari dei soci e del direttore tecnico dell'impresa partecipante (eventuali condanne penali, iscrizione nel casellario giudiziale);
- i dati personali comuni (nome, cognome, luogo e data di nascita, residenza, codice fiscale, documento d'identità) e giudiziari dei soggetti cessati dalla carica nell'anno antecedente la pubblicazione del bando (eventuali condanne penali, iscrizione nel casellario giudiziale).

4. Finalità del trattamento

Il trattamento dei dati personali forniti è finalizzato alla gestione della procedura (ivi compresa la pubblicazione della graduatoria e dei verbali di gara) e, pertanto, a:
- valutare i requisiti di ammissibilità alla procedura con riferimento alla situazione giuridica, alla capacità economica, finanziaria e tecnica dell'impresa e agli ulteriori adempimenti richiesti dalla normativa applicabile in materia di settore;
- verificare l'assenza di cause ostative alla partecipazione;
- consentire all'impresa di prendere parte alle varie fasi dell'iter di selezione.

5. Base giuridica del trattamento

Le basi giuridiche che giustificano il trattamento sono:
- art. 6, par. 1, lett. c) GDPR, adempimento di un obbligo legale al quale è soggetto il Titolare del trattamento;
- art. 6, par. 1 lett. e) GDPR, esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

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

-art. 9, par. 1, lett. g) GDPR, sussistenza di motivi di interesse pubblico rilevante […];

6. Modalità di trattamento

I dati personali sono trattati per le finalità esposte, secondo i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione ed esattezza dei dati di cui all'art 5 del GDPR in forma cartacea ed automatizzata. La disponibilità, la gestione, l'accesso, la conservazione e la fruibilità dei dati è garantita dall'adozione di misure tecniche ed organizzative per assicurare adeguati livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR.

7. Natura del conferimento dei dati

Il conferimento dei dati personali per le finalità di cui al punto 2 risulta necessario. La mancata comunicazione degli stessi pregiudica, pertanto, la partecipazione dell'operatore economico alla procedura di selezione e l'ammissione dello stesso alle successive fasi.

8. Destinatari o categorie di destinatari dei dati personali

I dati personali sono utilizzati e comunicati in modo adeguato e corretto a soggetti destinatari interni e/o esterni all'organizzazione del Titolare. A tal fine, nello svolgimento della propria attività e per il perseguimento delle finalità previste, il Titolare potrebbe comunicare i dati personali a:
- personale debitamente istruito ed autorizzato dal Titolare che agisce sotto l'autorità del medesimo e nel rispetto del segreto d'ufficio;
- persone fisiche e/o giuridiche, quali Responsabili al trattamento di dati personali ex artt. 28 e 29 GDPR che trattano dati per conto del Titolare, in rapporto contrattuale o convenzionale con il medesimo idoneamente designati e selezionati, altresì, per le garanzie prestate in materia di protezione dei dati personali, ciascuno nei limiti della propria professione e delle funzioni assegnate;
- organismi di controllo, organi della pubblica amministrazione ed enti o autorità che agiscono nella loro qualità di Titolari autonomi del trattamento, a cui sia obbligatorio comunicare i dati personali in forza di disposizioni di Legge o di ordini delle autorità (componenti della commissione esaminatrice);
- altre autorità pubbliche nel rispetto del Diritto dell'unione e/o dello Stato membro;
- autorità di pubblica sicurezza e autorità giudiziaria, nei limiti necessari per svolgere il loro compito istituzionale e/o di interesse pubblico (le suddette autorità nell'ambito di specifica indagine, conformemente al diritto dell'Unione o degli stati membri non sono considerate destinatarie).

I dati personali non sono soggetti a diffusione (intendendosi come tale il darne conoscenza in qualunque modo ad una pluralità di soggetti indeterminati), fatta salva la pubblicazione on-line nella sezione "Amministrazione Trasparente, prevista dalla normativa in materia di trasparenza amministrativa.

9.Trasferimento dei dati personali

I dati personali non sono trasferiti in paesi extra–UE. Tuttavia, in caso di un eventuale futuro trasferimento, il trattamento avverrà nel rispetto della normativa, ovvero, secondo una delle modalità consentite dalla Legge vigente, quali:
- trasferimento verso Paesi che offrono garanzie di protezione adeguate;
- adozione di Clausole contrattuali Standard approvate dalla Commissione Europea;
- adozione di Norme vincolanti d'impresa autorizzate dall'Autorità Garante;
- selezione di soggetti aderenti a programmi internazionali per la libera circolazione dei dati

10.Periodo di conservazione dei dati

I dati personali sono conservati per il tempo necessario al conseguimento delle finalità perseguite o per qualsiasi altra legittima finalità collegata, nel rispetto del principio di limitazione della conservazione di cui all'art. 5 del GDPR, comma 1, lett. e), nonché degli obblighi di Legge cui è tenuto il Titolare.

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

11.Diritti dell'interessato

I partecipanti alla procedura di gara hanno il diritto di ottenere, nei casi previsti:

- l'accesso ai dati personali ex art. 15 GDPR, diritto di accesso;
- la rettifica dei dati personali inesatti o l'integrazione di quelli incompleti ex art. 16 GDPR, diritto di rettifica;
- la cancellazione dei dati personali ex art. 17 GDPR, diritto alla cancellazione o diritto all'oblio;
- la limitazione del trattamento dei dati ex art. 18 GDPR, diritto di limitazione di trattamento;
- la comunicazione dei dati personali in formato strutturato, di uso comune e leggibile da dispositivo automatico ex art. 20 GDPR, diritto alla portabilità dei dati;
- la possibilità di opporsi, in qualsiasi momento, al trattamento dei dati personali ex art. 21 GDPR, diritto di opposizione.

Per l'esercizio dei diritti, è possibile rivolgersi al Titolare del trattamento con le seguenti modalità:
-raccomandata A/R all'indirizzo: Via Mazzini n. 117 – 28887 Omegna (VB);
-PEC: protocollo@pec.aslvco.it.
In particolare, i diritti sono esercitabili specificando nell'oggetto della richiesta, il diritto che si intende esercitare ed allegando la fotocopia di un documento di identità che attesti la legittimità della richiesta.

12.Proposizione di reclamo e segnalazione al Garante

L'interessato, ricorrendone i presupposti ha, altresì, il diritto di:

-proporre reclamo all'Autorità di controllo dello stato di residenza (ex art. 77 Reg. n. 679/2016), secondo le procedure previste dall'art. 142 del D.lgs. n. 196/2003, emendato dal D.lgs. n. 101/2018;
-rivolgere una segnalazione all'Autorità di controllo ex art. 144 D.lgs. n. 101/2018.

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. 4)

IFC – Informativa per i Fornitori /contraenti
(art. 13 e 14 regolamento UE 2016/679)

La presente informativa, resa ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 – General Data Protection Regulation, è resa ai fornitori persone fisiche e ai soggetti che operano in nome e per conto dei fornitori persone giuridiche dell'Azienda Sanitaria Locale VCO (in seguito "ASL VCO").

1.Titolare del trattamento

Titolare del trattamento è l'ASL VCO, con sede in Via Mazzini n. 117 – 28887 Omegna (VB), PEC: protocollo@pec.aslvco.it sito internet: www.aslvco.it , P.I./Cod. Fisc. 00634880033.

2. Responsabile della protezione dati (RPD o DPO)

Il Responsabile per la Protezione dei Dati (RPD/DPO) designato dal Titolare del trattamento è contattabile all'indirizzo e-mail: dpo@aslvco.it

3. Tipologia dei dati raccolti

I dati personali trattati, a titolo esemplificativo e non esaustivo, sono:
- dati identificativi e dati di contatto (dati anagrafici, indirizzo, recapiti telefonici, e-mail, dati bancari, composizione del nucleo familiare, dati fiscali, etc.);
- dati giudiziari.

4. Finalità del trattamento

I dati personali sono trattati dal Titolare del trattamento per:
a) acquisire dati e informazioni pre-contrattuali;
b) effettuare le operazioni necessarie per l'evasione degli ordini e delle altre richieste;
c) gestire gli adempimenti di natura amministrativa, contabile, civilistica, fiscale;
d) predisporre e presentare dichiarazioni e documenti di natura civilistica, fiscale, previsti da Leggi, Regolamenti, norme e direttive comunitarie ed extra comunitarie;
e) gestire e controllare i rischi, prevenire possibili frodi, insolvenze o inadempienze, prevenire e gestire possibili contenziosi, adire le vie legali in caso di necessità;
f) avviare e gestire transazioni e pratiche risarcitorie in caso di danno subito dai fornitori.

5. Base giuridica del trattamento

I dati personali saranno trattati, nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione ed esattezza dei dati ai sensi dell'art. 5 del GDPR, senza il suo specifico consenso essendo il trattamento legittimato dalle seguenti basi giuridiche:

- per le finalità di cui ai punti a) e b): art. 6, par. 1, lett. 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 e art. 6, par. 1, lett. 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;
-per le finalità di cui a ai punti c) e d): art. 6, par. 1, lett. c), il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
-per le finalità di cui ai punti e) e f): art.9, par. 2, lett. f), il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali.

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

6. Modalità di trattamento

Il trattamento dei dati per le finalità esposte ha luogo con modalità sia automatizzate, su supporto elettronico o magnetico, sia non automatizzate, su supporto cartaceo, nel rispetto delle regole di riservatezza e di sicurezza previste dalla Legge, dai Regolamenti e da disposizioni interne.

7. Natura del conferimento dei dati

Il conferimento dei dati personali è necessario per tutto quanto è richiesto dagli obblighi legali e contrattuali che regolamentano le transazioni commerciali e la fiscalità. Pertanto, il rifiuto al conferimento può dar luogo all'impossibilità di dare esecuzione al contratto o di svolgere correttamente tutti gli adempimenti, connessi al rapporto quali: l'evasione degli ordini, l'evasione di altre richieste, erogazione/fornitura del servizio/prodotto, etc. Il conferimento dei dati personali è, inoltre, necessario per una corretta ed efficiente gestione del rapporto contrattuale.

8. Destinatari o categorie di destinatari dei dati personali

I dati personali sono utilizzati e comunicati in modo adeguato e corretto a soggetti destinatari interni e/o esterni all'organizzazione del Titolare. A tal fine, nello svolgimento della propria attività e per il perseguimento delle finalità di cui al precedente paragrafo 2, il Titolare potrebbe comunicare i Suoi Dati Personali a:
- personale debitamente istruito ed autorizzato dal Titolare che agisce sotto l'autorità del medesimo e nel rispetto del segreto professionale e d'ufficio;
- persone fisiche e/o giuridiche, quali Responsabili al trattamento di dati personali ex artt. 28 e 29 del GDPR che trattano dati per conto del Titolare, in rapporto contrattuale o convenzionale con il medesimo, idoneamente designati e selezionati, altresì, per le garanzie prestate in materia di protezione dei dati personali, ciascuno nei limiti della propria professione e delle funzioni assegnate, ovvero:

- fornitori di servizi (come consulenti, istituti di credito, enti certificatori, società di gestione dell'archivio, etc.);
- consulenti tecnici e legali per la gestione di eventuali controversie per responsabilità civile di terzi;
- enti che operano in ambito clinico/scientifico (Fondazione/Onlus/associazioni di ricerca);

- organismi sanitari di controllo, organi della pubblica amministrazione ed enti assicurativi e altri soggetti, enti o autorità che agiscono nella loro qualità di Titolari autonomi del trattamento, a cui sia obbligatorio comunicare i dati personali in forza di disposizioni di Legge o di ordini delle autorità;
- organismi del SSN, enti previdenziali o assistenziali, assicurazioni;
- autorità di pubblica sicurezza e autorità giudiziaria, nei limiti necessari per svolgere il loro compito istituzionale e/o di interesse pubblico (le suddette autorità nell'ambito di specifica indagine, conformemente al diritto dell'Unione o degli stati membri non sono considerate destinatarie).

I dati personali non sono soggetti a diffusione (intendendosi come tale il darne conoscenza in qualunque modo ad una pluralità di soggetti indeterminati), fatta salva la pubblicazione on-line nella sezione "Amministrazione Trasparente", prevista dalla normativa in materia di trasparenza amministrativa.

9.Trasferimento dei dati personali

I dati personali non sono trasferiti in paesi extra–UE. Tuttavia, in caso di un eventuale futuro trasferimento, il trattamento avverrà nel rispetto della normativa, ovvero, secondo una delle modalità consentite dalla Legge vigente, quali:
- trasferimento verso Paesi che offrono garanzie di protezione adeguate;
- adozione di Clausole contrattuali Standard approvate dalla Commissione Europea;
- adozione di Norme vincolanti d'impresa autorizzate dall'Autorità Garante;

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

- selezione di soggetti aderenti a programmi internazionali per la libera circolazione dei dati.

10.Periodo di conservazione dei dati

Il Titolare del trattamento conserva e tratta i dati personali per il tempo necessario ad adempiere alle finalità indicate. Successivamente, i dati personali saranno conservati, e non ulteriormente trattati, per il tempo stabilito dalle vigenti disposizioni in materia civilistica e fiscale. Eventuali altri dati saranno conservati per il tempo strettamente necessario all'erogazione del servizio, salvo l'espressa richiesta di cancellazione da parte Sua.

11.Diritti dell'interessato

Relativamente ai Suoi dati personali, il GDPR Le conferisce, come Interessato del trattamento, l'esercizio di specifici diritti, ove applicabile, e in particolare:
-l'accesso ai dati personali ex art. 15 GDPR, diritto di accesso;
-la rettifica dei dati personali inesatti o l'integrazione di quelli incompleti ex art. 16 GDPR, diritto di rettifica;
-la cancellazione dei dati personali ex art. 17 GDPR, diritto alla cancellazione o diritto all'oblio;
-la limitazione del trattamento dei dati ex art. 18 GDPR, diritto di limitazione di trattamento;
-la comunicazione dei dati personali in formato strutturato, di uso comune e leggibile da dispositivo automatico ex art. 20 GDPR, diritto alla portabilità dei dati;
-la possibilità di opporsi, in qualsiasi momento, al trattamento dei dati personali ex art. 21 GDPR, diritto di opposizione.

Per l'esercizio dei diritti, è possibile rivolgersi al Titolare del trattamento con le seguenti modalità:
-raccomandata A/R all'indirizzo: Via Mazzini n. 117 – 28887 Omegna (VB);
-PEC: protocollo@pec.aslvco.it.
In particolare, i diritti sono esercitabili specificando nell'oggetto della richiesta, il diritto che si intende esercitare ed allegando la fotocopia di un documento di identità che attesti la legittimità della richiesta.

12. Proposizione di reclamo e segnalazione al Garante

L'interessato, ricorrendone i presupposti ha, altresì, il diritto di:

-proporre reclamo all'Autorità di controllo dello stato di residenza (ex art. 77 Reg. n. 679/2016), secondo le procedure previste dall'art. 142 del D.lgs. n. 196/2003, emendato dal D.lgs. n. 101/2018;
-rivolgere una segnalazione all'Autorità di controllo ex art. 144 D.lgs. n. 101/2018.