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.

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;
a) 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,

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.

quale Titolare del Trattamento, ai sensi della Delibera e definisce gli obblighi delle Parti in materia di tutela dei dati personali;

1) 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;
2) Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali;
3) Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.
4) La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata riportata nel Contratto;
5) 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.

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.

1) 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).
2) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Disciplinari, ecc…
3) 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)

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.

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;
1) 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.

1) 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.

2) 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.

3) 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*.

4) 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.

1) 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.

2) 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.

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.

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.

1) 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 .

1) 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.

2) 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.

1) 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.

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.

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.

1) 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.

2) 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.

3) 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;
   1. adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).

4) 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.

5) 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.

6) 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

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.

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.

1) 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;
   1. 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;
   2. predisporre e conservare l’elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
   3. 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;
   4. 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;
   5. verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
   6. 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);
   7. 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.

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.

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.

1) 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.

2) 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.

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

4) 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;
   1. 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;
   2. 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;
   3. 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.

5) 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	**Affidamento del servizio di assistenza medica nella specialità di Radiologia presso i presidi ospedalieri di Domodossola e Verbania per un periodo di mesi nove**

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.

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

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.

		[ ] 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? Art. 24, 25, 32 GDPR	[ ] 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 [ ] 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

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.

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

Articolo 18 – Amministratori di sistemi

ID	Nome e Cognome (1)	Ragione Sociale (2)	Recapito E-mail/Telefono	Sistemi Amministrati
1				
2				

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.

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
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

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.

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)
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*

1) 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.
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

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.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		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.
	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.

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.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	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).
	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

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.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		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. 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	17.1	Gli utenti non devono essere in grado di disattivare o aggirare le

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.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
desktop/laptop/mobile		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 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.

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.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	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).
	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.

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.

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.

1) 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.

2) La mancata sottoscrizione del presente accordo non consentirà di dare attuazione di quanto previsto nel Contratto.

3) Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/12 di ogni anno.

4) 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.

5) 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

_____