R E G O L A M E N T O

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

"MOP"

	Responsabili - Firme			
	Nome e Cognome		**Funzione/i**	**Firma**
Redazione	Ilenia	Di Salvia	Collaboratore Amministrativo S.S.A ICT	
	Luca	Davico	Collaboratore Tecnico S.S.A ICT	
Verifica	Roberto	Pozzi	Dirigente Analista S.S.A ICT	
	Stefano	Garione	Collaboratore Tecnico S.S.A ICT	
	Ivan	Tosco	DPO RTI – Liguria Digitale S.p.A.	
Approvazione	Stefano	Bergagna	Direttore Amministrativo ASL AL	

Indice

1. Scopo e campo di applicazione

Il presente documento, nel descrivere i principi di riferimento, le regole, i ruoli e le responsabilità dei soggetti coinvolti nelle attività di gestione e Protezione dei Dati Personali in ottemperanza al principio di accountability (responsabilizzazione), ha lo scopo di illustrare il Modello Organizzativo per la Protezione dei Dati Personali (d'ora in Avanti MOP) definito in ASL AL per garantire l'osservanza di quanto disposto dal Regolamento Europeo 2016/679 e dal D.Lgs 196/2003 così come modificato dal D.Lgs 101/2018.

Il presente documento, che rappresenta un'evoluzione del MOP precedentemente in vigore (delibera 358/23), lo sostituisce e si applica con efficacia immediata ad ASL AL, ovvero alla rete ospedaliera (i Presidi Ospedalieri), alla rete territoriale (i Distretti Territoriali), al Dipartimento di Prevenzione, all'Area Amministrativa dell'Azienda e a tutti gli ulteriori Servizi, Strutture ed Uffici di cui all'organigramma aziendale, approvato con il relativo atto aziendale (Delibera 359/24 del 18/04/2024 e s.m.i.). Inoltre, si applica a tutto il personale dipendente e a tutti coloro che collaborano a qualsiasi titolo con ASL AL in tutte le attività che comportano un trattamento di dati personali.

2. Destinatari

Il documento è destinato a tutto il personale dirigente ed appartenente al comparto di ruolo sanitario, professionale, tecnico ed amministrativo, ovvero a a tutti coloro che trattano dati in nome e per conto del Titolare.

3. Riferimenti

3.1. Riferimenti interni

- Delibera 343/25 del 13/05/2025 ad oggetto "MODELLO ORGANIZZATIVO S.S.A. ICT."

- Delibera 170/25 del 27/03/2025 ad oggetto "ISTITUZIONE UFFICIO PRIVACY AZIENDALE."

- Delibera 1135/24 del 10/12/2024 ad oggetto "DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) AI SENSI DELL'ART. 37 DEL REGOLAMENTO UE 2016/679."

- Delibera n. 359/24 del 18/04/2024 ad oggetto "D.G.R. N. 11-8161 DEL 12.02.2024. CONCLUSIONE PROCEDIMENTO DI VERIFICA ATTO AZIENDALE ASL AL - RECEPIMENTO PRESCRIZIONI REGIONALI." e s.m.i.

- Delibera n. 358 del 09/05/2023 ad oggetto "APPROVAZIONE MODELLO ORGANIZZATIVO PRIVACY DELL'A.S.L. AL: AGGIORNAMENTO."

3.2. Riferimenti esterni

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

- Decreto legislativo 30 giugno 2003, n. 196 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI e successive modificazioni ed integrazioni, come novellato dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101;

- DECRETO LEGISLATIVO 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

- PROVVEDIMENTO 5 giugno 2019 del Garante per la Protezione dei Dati Personali. Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'articolo 21, comma 1 del decreto legislativo 10 agosto 2018, n. 101. (Provvedimento n. 146). (19A04879) (GU Serie Generale n.176 del 29-07-2019);

- PROVVEDIMENTO Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) e successive modificazioni (così modificato in base al provvedimento del 25 giugno 2009);

- Guida del Garante della Protezione dei Dati Personali italiano all'applicazione del Regolamento europeo in materia di Protezione dei Dati Personali.

4. Definizioni

- **RGPD / GDPR**: Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati / General Data Protection Regulation;

- **Codice Privacy**: Codice in materia di Protezione dei Dati Personali, D.Lgs 196/2003 e s.m.i.;

- **Titolare del Trattamento o Titolare**: 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 dei Dati Personali;

- **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;

- **RPD / DPO**: Responsabile della Protezione dei dati / Data Protection Officer;

- **Interessato**: la persona fisica a cui si riferiscono i dati personali;

- **Designato al Trattamento dei Dati Personali**: la persona fisica espressamente designata che opera sotto l'autorità dell'ente nell'ambito del proprio assetto organizzativo con specifici compiti e funzioni;

- **Amministratore di Sistema**: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza;

- **Autorità di controllo**: autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR;

- **Autorizzato al Trattamento dei Dati Personali**: la persona fisica che effettua materialmente le operazioni di trattamenti sui dati personali;

- **Violazione dei Dati Personali / Data Breach**: la violazione di sicurezza che comporta accidentalmente o in modo intenzionale la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali, conservati o comunque trattati, compromettendone la disponibilità, l'integrità o la riservatezza;

- **Garante per la Protezione dei Dati Personali**: Autorità di controllo pubblica indipendente prevista dalla normativa italiana ed europea inerente la Protezione dei Dati Personali, con lo scopo di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al Trattamento dei Dati Personali e di agevolarne la libera circolazione all'interno dell'Unione Europea.

4.1. Acronimi e abbreviazioni

Codice	Titolo
AdS	Amministratore di Sistema
ASL AL	Azienda Sanitaria Locale Alessandria
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
MOP	Modello Organizzativo Privacy
RPD/DPO	Responsabile per la Protezione dei Dati/Data Protection Officer
SC	Struttura Complessa
SSA	Struttura Semplice a valenza Aziendale
SSD	Struttura Semplice a valenza Dipartimentale
SS	Struttura Semplice

5. Modello organizzativo

ASL AL favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto sia qualora agisca in qualità di Titolare del Trattamento, che di Responsabile Esterno del Trattamento.

5.1 Titolare del Trattamento

L'organo di rappresentanza di ASL AL, nonché Titolare del Trattamento dei Dati Personali (d'ora in Avanti anche "Titolare") ai sensi del GDPR, è il Direttore Generale o il Commissario, in accordo con le nomine regionali. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR:

- liceità, correttezza e trasparenza;
- limitazione della finalità e minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza.

Il Titolare mette in atto le misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in conformità con il GDPR. Le misure sono definite fin dalla fase di progettazione (*privacy by design*) e messe in atto per applicare in modo efficace i principi di protezione dei dati, al fine di agevolare l'esercizio dei diritti dell'Interessato stabiliti dagli articoli 15-22 del GDPR e tutte le comunicazioni e informazioni occorrenti per il loro esercizio.

Il Titolare provvede a:

- nominare il Data Protection Officer (d'ora in poi anche solo "DPO") [*cfr. § 5.3*];
- nominare i Designati al Trattamento dei Dati [*cfr. § 5.4*];
- nominare i Responsabili del Trattamento dei Dati ex art. 28 GDPR [*cfr. § 5.5*];
- nominare gli Amministratori di Sistema [*cfr. § 5.6*];
- nominare gli Autorizzati al Trattamento dei Dati [*cfr. § 5.7*].
- assegnare distinti compiti a specifiche Strutture, al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento dell'Ente al GDPR;
- definire gli indirizzi per l'attribuzione di specifiche competenze all'Ufficio Privacy, anche con riguardo alla funzione di raccordo e di collaborazione con il Garante per la Protezione dei Dati Personali (d'ora in poi anche solo "Garante"), al fine di supportare l'attività del Titolare nel

rapporto con le Strutture Organizzative dell'Ente e fornire a queste ultime le necessarie indicazioni in materia di protezione dati sui trattamenti sviluppati dalle stesse;

- redarre, con il supporto del DPO, dei Soggetti Designati e dell'Ufficio Privacy, il Registro delle Attività di Trattamento [*cfr. § 6.1*].

Il Titolare è definito "Contitolare del Trattamento", ai sensi dell'art. 26 del GDPR, nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'ASL AL da enti ed organismi statali o regionali, allorché due o più Titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento. Il riferimento normativo per l'istituto della Contitolarità è l'art. 26 del GDPR.

5.2 Ufficio Privacy

L'Ufficio Privacy, istituito in ASL AL con delibera 170/25, è incardinato all'interno della Struttura ICT ed ha il compito di supportare il Titolare nel rapporto con tutte le Strutture Organizzative in materia di adeguamento al GDPR. L'Ufficio Privacy si relaziona con le Strutture Organizzative dell'Ente fornendo pareri laddove richiesti e indicazioni operative in relazione alle attività svolte dalle medesime, per la corretta e tempestiva applicazione del GDPR.

All'Ufficio Privacy compete l'individuazione di modalità e procedure operative volte alla:

- predisposizione della documentazione necessaria alla nomina da parte del Titolare dei Responsabili Esterni del Trattamento, su richiesta dei Designati o dei referenti della protezione dei dati;

- gestione e conservazione del Registro delle Attività di Trattamento ex art. 30 GDPR;

- valutazione di impatto (DPIA) su richiesta dei Designati o dei referenti protezione dei dati ed in collaborazione con il DPO;

- gestione degli episodi di violazione di dati personali (Data Breach), in collaborazione con il DPO;

- ricezione e riscontro alle richieste dei Soggetti Interessati inviate direttamente all'Ufficio Privacy;

- predisposizione ed aggiornamento, su richiesta, della modulistica in materia di trattamento dei dati;

- formulazione di pareri in materia di protezione dei dati, in collaborazione con il DPO e con l'Ufficio Legale, in riscontro alle istanze degli uffici richiedenti;

- assicurazione del necessario supporto ai Designati al Trattamento dei Dati nei processi di nomina dei Responsabili del Trattamento e degli Autorizzati;

- gestione dei rapporti con le altre aziende sanitarie del SSR, con la Regione Piemonte e con i Ministeri, per quanto concerne le tematiche in materia di Protezione dei Dati Personali.

L'Ufficio Privacy non ha competenza in ambito di contenzioso o pareri strettamente legali, che sono

demandati all'Ufficio Legale aziendale.

5.3 Gruppo Privacy Aziendale

Il Gruppo Privacy Aziendale rappresenta un organo di governo delle tematiche in ambito di Protezione dei Dati Personali. Del Gruppo Privacy Aziendale fanno parte:

- il Direttore Generale o Commissario;
- il Direttore Amministrativo;
- il Direttore Sanitario;
- i Responsabili o Direttori delle Strutture che stipulano contratti come:
  - Ufficio Tecnico
  - Ufficio Acquisti
  - Ufficio Personale;
- il Responsabile o Direttore dei Sistemi Informatici;
- il Responsabile o Direttore della Struttura Aziendale che ha in carico le attività di formazione;
- il Responsabile dell'Ufficio Legale di riferimento per le tematiche di protezione dei dati personali.

Il Gruppo Privacy Aziendale si riunisce con cadenza almeno annuale o in caso di specifica convocazione da parte del Titolare e, come accennato, ha in carico tematiche di governo aziendale nell'ambito della protezione dei dati personali. Sono suoi compiti:

- la definizione del piano di formazione dei dipendenti in ambito GDPR;
- la definizione dei ruoli e delle relative responsabilità per lo sviluppo ed il mantenimento delle procedure finalizzare alla Protezione dei Dati Personali;
- l'azione di verifica e controllo che le procedure finalizzare alla Protezione dei Dati Personali siano integrate in tutti i processi aziendali e che i conseguenti controlli siano sviluppati efficacemente;
- l'approvazione delle linee guida finalizzate all'innalzamento del livello di sicurezza nella gestione delle informazioni;
- l'attivazione di specifici programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni;
- la definizione degli obiettivi relativi alla sicurezza delle informazioni, assicurandone la coerenza con la realtà della struttura a cui si riferiscono;

- verifica dello stato di avanzamento degli obiettivi di cui al punto precedente.

5.4 Responsabile della protezione dei dati - Data protection Officer (DPO)

Il Data Protection Officer è individuato nella figura unica di un Professionista o di una Società nel rispetto delle prescrizioni recate dal Codice degli Appalti in materia di contratti di servizio. In entrambi i casi, il soggetto deve possedere i requisiti specificati dagli artt. 37 e 38 del GDPR.

Il DPO è incaricato dei seguenti compiti:

- informare e fornire consulenza all'Ente (in qualità di Titolare o di Responsabile Esterno del Trattamento) in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla Protezione dei Dati Personali;

- fungere da supporto alle Strutture competenti sulle richieste di accesso per tutti gli aspetti relativi alla Protezione dei Dati Personali ai sensi del GDPR;

- fornire, se richiesto, un parere in merito alla Valutazione di Impatto sulla Protezione dei Dati (DPIA) e supervisionarne lo svolgimento;

- rendere una consulenza idonea, scritta od orale, anche nell'individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati;

- cooperare con il Garante della Protezione dei Dati Personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione inerente al trattamento di dati personali;

- sorvegliare l'osservanza del GDPR e delle altre normative relative alla Protezione dei Dati Personali, ferme restando le responsabilità dell'Ente in qualità di Titolare o di Responsabile Esterno del Trattamento. Fanno parte di questi compiti: la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti dell'Ente;

- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere;

- altri compiti e funzioni a condizione che l'Ente (in qualità di Titolare o di Responsabile Esterno del Trattamento) si assicuri che non diano adito a un conflitto di interessi.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

La figura del DPO è incompatibile con chi determina le finalità o i mezzi del trattamento e con il ruolo di fornitore dell'Ente, tranne nel caso in cui l'attività di fornitura sia da considerarsi quale ausilio e supporto allo svolgimento delle attività in capo al DPO medesimo. In particolare, risultano incompatibili con la figura del DPO i seguenti ruoli:

- Responsabile per la Prevenzione della Corruzione e per la Trasparenza;

- Responsabile Esterno del Trattamento;

- Dirigente ed il personale afferente ai Sistemi Informatici Aziendali;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del Trattamento.

ASL AL (in qualità di Titolare o di Responsabile Esterno del Trattamento) fornisce al DPO le risorse necessarie per assolvere ai compiti attribuiti e per accedere ai dati personali ed ai trattamenti posti in essere.

Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti e non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione riguardante la normativa sulla Protezione dei Dati Personali. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente all'Ente (in qualità di Titolare o di Responsabile Esterno del Trattamento). Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, questo è tenuto a manifestare le proprie osservazioni e i propri rilievi comunicandoli all'Ente (in qualità di Titolare o di Responsabile Esterno del Trattamento).

5.5 Designati al Trattamento dei dati

Il Titolare nomina i Responsabili delle articolazioni organizzative delle strutture dell'Ente, quali Designati al Trattamento dei Dati Personali relativamente ai trattamenti effettuati dall'articolazione organizzativa di competenza.

Sulla base delle articolazioni definite all'interno dell'Atto Aziendale in vigore, sono nominati "Designato al Trattamento dei Dati" tutti i Direttori di Struttura Complessa, tutti i Responsabili di Struttura Semplice a valenza Aziendale, tutti i Responsabili di Struttura Semplice a valenza Dipartimentale e gli avvocati Responsabili degli Uffici Legali.

Ciascun Designato deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

E' facoltà di ciascun Designato quella di nominare uno o più Referenti del Trattamento dei Dati (a titolo esemplificativo, i Responsabili di Struttura Semplice) ai quali può delegare alcune o tutte le sue sue funzioni peculiari.

Ai Designati sono attribuiti i seguenti compiti:

- verificare la legittimità dei trattamenti di dati personali effettuati dalla Struttura di riferimento;

- collaborare con l'Ufficio Privacy e con il DPO, al fine di consentire agli stessi l'esecuzione dei compiti e delle funzioni assegnate;

- accertarsi che il personale afferente alla Struttura Organizzativa di competenza abbia sottoscritto la lettera di nomina ad Autorizzato al Trattamento;

- individuare il personale della propria articolazione organizzativa da sottoporre alle attività formative in materia di protezione dei dati;

- rapportarsi con l'Ufficio Privacy e con il DPO, al fine di adottare, nel caso di nuove attività che comportino il trattamento di dati, soluzioni di "*privacy by design*" e "*privacy by default*", ovvero di protezione dei dati fin dalla progettazione e per impostazione predefinita, prevedendo, già dall'origine e in considerazione del contesto complessivo ove il trattamento si colloca e dei rischi stimati, un paradigma di trattamento e misure di protezione prefissate;

- comunicare all'Ufficio Privacy le modifiche intervenute ai trattamenti di competenza e verificare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura Organizzativa;

- relazionarsi con L'Ufficio Privacy nell'idividuazione dei Responsabili del Trattamento ex art. 28 del GPDR e procedere in autonomia, o eventualmente con il supporto dell'Ufficio Privacy stesso, alla richiesta della loro nomina al Titolare, mediante utilizzo del modello allegato al presente regolamento. Qualora la richiesta di nomina avvenga in maniera autonoma, dovrà essere data opportuna comunicazione all'Ufficio Privacy ai fini dell'aggiornamento del relativo registro;

- qualora la propria Struttura riceva istanze da parte degli Interessati relative a questioni legate al trattamento dei dati, dovrà tempestivamente inoltrare le stesse all'Ufficio Privacy ed al DPO;

- rilevare e comunicare tempestivamente all'Ufficio Privacy e al DPO i casi di violazione, anche potenziale, dei dati personali (Data Breach), verificatisi nell'ambito organizzativo di riferimento;

- verificare, periodicamente, le abilitazioni rilasciate, per gli applicativi informatici, ai propri collaboratori e fornire evidenza di eventuali variazioni mediante gli strumenti messi a disposizione dell'Azienda;

- inoltrare all'Ufficio Privacy, segnalando la necessità di redigere una valutazione di impatto per un determinato trattamento, le informazioni previste all'art. 35 GDPR sul trattamento in oggetto (descrizione del trattamento, finalità, valutazione delle necessità e proporzionalità del trattamento in relazione alle finalità, valutazione dei rischi e misure previste per affrontare i rischi), al fine di permettere all'Ufficio Privacy di dare avvio alla valutazione per la parte di propria competenza;

- verificare, una volta esaurita la finalità del trattamento, la corretta ed effettiva eliminazione dei dati raccolti.

Per i trattamenti dei dati personali che coinvolgono più Strutture in modo trasversale, laddove applicabile, vige il criterio della prevalenza, secondo il quale la Struttura che ha competenza principale nel Trattamento dei Dati Personali coordina le attività delle altre Strutture coinvolte.

5.6 Responsabile del Trattamento ex art. 28 GDPR

Il Responsabile (esterno) ex art. 28 GDPR del Trattamento è il soggetto, pubblico o privato, che tratta dati personali, anche particolari e/o genetici, per conto del Titolare e che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei dati dell'Interessato. Tale soggetto assume il ruolo di Responsabile Esterno del Trattamento ai sensi dell'art. 28 del GDPR.

La formalizzazione di detto ruolo avviene mediante atto giuridico sottoscritto dal Titolare e dal Responsabile nominato, su indicazione dell'Ufficio Privacy o dei Designati al Trattamento dei dati per gli ambiti gestionali di loro competenza. I rapporti tra il Titolare ed i Responsabili esterni sono disciplinati dagli articoli del suddetto atto, i quali specificano la finalità perseguita, la tipologia dei dati, la categoria degli Interessati, la durata del trattamento, gli obblighi e i diritti del Responsabile Esterno del Trattamento e le modalità di trattamento. Il Responsabile Esterno del Trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa ed ai compiti affidatigli.

5.7 Amministratore di Sistema

Il Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 ad oggetto "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" e s.m.i. definisce l'Amministratore di Sistema come la "figura professionale dedicata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali".

Ai sensi del provvedimento del Garante per le Protezione dei Dati Personali dd. 27/11/2008 e s.m.i. vengono, tuttavia, considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza. Gli amministratori di sistema così più ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

La formalizzazione di detto ruolo avviene mediante atto giuridico sottoscritto dal Titolare e dall'Amministratore di Sistema. Gli Amministratori di Sistema devono essere individuati su indicazione del Responsabile della Struttura ICT. Gli obblighi del Titolare ed i doveri degli Amministratori di Sistema sono disciplinati dagli articoli del suddetto atto, i quali specificano la finalità perseguita, la tipologia dei dati, la categoria degli Interessati, la durata del trattamento, le modalità di tracciamento degli accessi e di controllo delle operazioni svolte.

In considerazione del ruolo primario ricoperto dal Responsabile della Struttura ICT nell'individuazione degli Amministratori di Sistema, il Titolare può delegare, con nota scritta, la

firma dell'atto di nomina ad Amministratore di Sistema al suddetto Responsabile.

5.8 Autorizzato al Trattamento

Il Titolare o il Designato al Trattamento, per gli ambiti di propria competenza, nominano gli Autorizzati al Trattamento quali persone ammesse a compiere operazioni sui dati personali, mediante mutua sottoscrizione dell'atto di nomina. All'interno di tale atto vengono indicati, per ciascun Autorizzato, gli ambiti di attività e/o l'elenco dei trattamenti di dati personali di competenza. L'autorizzato dovrà segnalare le eventuali modifiche inerenti alle proprie mansioni che si riflettano nelle attività di trattamento dei dati di propria competenza.

6. Registri

ASL AL, in relazione alla tematica di Protezione dei Dati Personali, adotta i Registri dettagliati ai paragrafi dal 6.1 al 6.6, manutenuti principalmente ad opera dell'Ufficio Privacy in collaborazione con i soggetti coinvolti (Designati, Responsabili, Autorizzati ed Amministratori di Sistema) e con il DPO.

ASL AL adotta software specializzati e sottoposti a adeguati criteri di sicurezza e backup tali da poter essere considerati, in ogni momento, la versione più aggiornata dei Registri di cui di seguito.

6.1 Registro delle Attività di Trattamento

Il Registro delle Attività di Trattamento contiene le informazioni relative alle operazioni di Trattamento dei Dati Personali svolte dal Titolare e, se nominati, dal Responsabile del Trattamento. Tale documento è finalizzato a dimostrare la conformità al GDPR e in ambito di gestione della Protezione dei Dati Personali.

Il Registro delle Attività di Trattamento deve contenere le informazioni aggiornate relative all'identità ed ai dati di contatto del Titolare del Trattamento, del Responsabile della Protezione dei Dati (DPO) e degli eventuali Contitolari dei Trattamenti. Per ogni trattamento deve definire:

- le finalità dello stesso con indicazione della base giuridica di riferimento (consenso, contratto, obbligo legale, ecc.);
- le categorie di Interessati (ad esempio, cittadini, dipendenti, fornitori);
- le categorie di dati personali trattati (ad esempio, dati anagrafici, dati di contatto, dati relativi alla salute);
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, inclusi i paesi terzi o le organizzazioni internazionali;
- gli eventuali trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, con indicazione delle garanzie adottate;

- la descrizione generale delle misure di sicurezza adottate.

Il Registro delle Attività di Trattamento è redatto dal Titolare che si avvale, per questa specifica attività, dell'Ufficio Privacy e dei Soggetti Designati, nonché del DPO.

Alla data di adozione del presente Modello Organizzativo, ASL AL implementa il Registro delle Attività di Trattamento all'interno del software DPM (fornitore: Studio Storti) e sono, pertanto, abrogati tutti i provvedimenti e gli atti pregressi che lo istituivano.

6.2 Registro delle violazioni dei dati personali

Questo Registro si suddivide in due sotto-registri: il Registro dei Data Breach ed il Registro degli Incidenti di Sicurezza e riportano gli eventi verificatisi in ambito di Violazione dei Dati Personali sulla base della loro categorizzazione di cui al paragrafo 8 del presente regolamento.

I registri di cui al presente paragrafo sono redatti a cura dell'Ufficio Privacy che, alla data di adozione del presente Modello Organizzativo, li manutiene all'interno del software DPM (fornitore: Studio Storti).

6.3 Registro delle nomine

Questo Registro si suddivide in quattro sotto-registri: il Registro delle nomine dei Soggetti Designati, il Registro delle nomine dei Responsabili al Trattamento, il Registro delle nomine degli Amministratori di Sistema ed il Registro delle nomine dei Soggetti Autorizzati.

Ognuno dei Registri elenca i soggetti nominati o Designati per lo specifico ruolo.

La redazione e manutenzione del Registro delle nomine dei Soggetti Designati è in carico all'Ufficio Privacy che deve ricevere opportuna comunicazione dalla S.C. Personale delle avvenute nomine dei Direttori di Struttura Complessa e dei Responsabili di Struttura Semplice a valenza Aziendale e di Struttura Semplice a valenza Dipartimentale e degli Uffici Legali. E' compito operativo dell'Ufficio Privacy quello di trasmettere ai Soggetti Designati l'atto di nomina a firma del Titolare e raccogliere il documento controfirmato, registrando l'avvenuta nomina sull'apposito registro. Il registro deve essere verificato ed, eventualmente, revisionato con cadenza almeno annuale.

La redazione e manutenzione del Registro delle nomine dei Responsabili al Trattamento è in carico all'Ufficio Privacy che deve ricevere opportuna informazione dal Soggetto Designato della necessità di nominare un Responsabile del Trattamento o atto di nomina già sottoscritto dal Titolare e dal Soggetto nominato, al fine di procedure con la registrazione dell'avvenuta nomina sull'apposito registro. Il registro deve essere verificato ed, eventualmente, revisionato con cadenza annuale.

La redazione e manutenzione del Registro delle nomine degli Amministratori di Sistema è in carico all'Ufficio Privacy che, in occasione della nomina di un nuovo Amministratore di Sistema sulla base di quanto riportato sull'applicativo CredNet (gestionale per la richiesta di accesso ai software; fornitore: System Technology), deve trasmettere all'Amministratore di Sistema l'atto di nomina a firma del Titolare (o, in caso di apposita delega, del Responsabile della Struttura ICT) e curare la ricezione del documento controfirmato procedendo con la registrazione dell'avvenuta nomina sull'apposito registro. Il registro deve essere verificato ed, eventualmente, revisionato con cadenza

almeno annuale.

La redazione e manutenzione del Registro delle nomine dei Soggetti Autorizzati è in carico ai Soggetti Designati che hanno l'onere di far sottoscrivere l'apposita nomina (Allegato 4 al presente regolamento) a tutti gli autorizzati afferenti alla propria Struttura, trasmettendo copia del documento sottoscritto all'Ufficio Privacy per la registrazione dell'avvenuta nomina sull'apposito registro. Il registro deve essere verificato ed, eventualmente, revisionato con cadenza biennale.

I registri di cui al presente paragrafo sono redatti e manutenuti, in conformità con quanto stabilito, all'interno del software DPM (fornitore: Studio Storti) e, pertanto, è abrogata la delibera 481/2021 ad oggetto "Istituzione del registro degli Amministratori di Sistema dell'ASL AL".

6.4 Registro dei consensi

Alla data di adozione del presente MOP, ASL AL ha in uso il software "Consent Manager" (fornitore Dedalus Italia S.p.A.) per la registrazione dei Consensi. Tale software, aggiornato dal personale di front office, rappresenta il raccoglitore informatico dei consensi rilasciati dai Soggetti Interessati.

E' in carico all'Ufficio Privacy il caricamento delle informative e dei modelli di consenso da sottoporre a firma da parte dei cittadini.

6.5 Registro delle istanze dei Soggetti Interessati

Il Registro, che raccoglie le istanze dei Soggetti Interessati pervenute ad ASL AL, il loro stato ed i riscontri ai cittadini, è memorizzato all'interno del software DPM (fornitore: Studio Storti) ed è redatto e manutenuto dal personale afferente all'Ufficio Privacy.

6.6 Registro delle Valutazioni di Impatto

Il Registro, che raccoglie le valutazioni di impatto eseguite sui trattamenti dell'Azienda [*cfr. § 9*], è memorizzato all'interno del software DPM (fornitore: Studio Storti), che mette a disposizione anche uno strumento per la redazione delle stesse. Il sistema permette il versionamento delle DPIA relative allo stesso trattamento ed è redatto e manutenuto dal personale afferente all'Ufficio Privacy.

7. Sicurezza dei dati personali

Il Titolare del Trattamento mette in atto misure tecniche ed organizzative finalizzate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche della probabilità e della magnitudo per i diritti e le libertà delle persone fisiche.

Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre: i sistemi di autenticazione, autorizzazione, rilevazione di intrusione, sorveglianza; di protezione (antivirus; firewall; antintrusione); sistemi di copiatura e conservazione di archivi elettronici; altre misure per

ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico, in via generale di competenza della Struttura ICT, fatta salva l'attività delegata agli incaricati o fornitori di servizi informatici.

La conformità del trattamento dei dati al GDPR è dimostrata attraverso l'adozione delle misure di sicurezza adeguate, oppure con l'adesione a codici di condotta approvati, ovvero a meccanismi di certificazione approvati.

ASL AL, attraverso i ruoli individuati nel presente MOP, si prende carico di impartire adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbiano accesso a dati personali.

8. Considerazioni conclusive

Il presente paragrafo riporta l'estratto del "Regolamento sui Data Breach" e del "Regolamento sulle Valutazioni di Impatto" in vigore in Azienda e, pur non essendo oggetto dell'organizzazione aziendale in ambito di gestione della Protezione dei Dati Personali, definisce alcuni concetti vitali per la comprensione del Modello Organizzativo stesso.

8.1 Violazione dei Dati Personali - DataBreach

Si definisce "Violazione dei Dati Personali" un qualsiasi evento che ne comprometta la disponibilità, l'integrità o la riservatezza. Si tratta di una violazione di sicurezza che può comportare, in maniera accidentale o intenzionale, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, conservati o comunque trattati dall'Ente.

Le violazioni dei dati personali possono avere un impatto più o meno esteso, tale da determinarne, in accordo con il DPO, la loro notifica o meno all'autorità Garante per la Protezione dei Dati Personali.

Qualora la Violazione dei Dati Personali possa essere derubricata ad "Incidente di Sicurezza" e non debba, conseguentemente, essere comunicata all'Autorità Garante, l'Ente deve comunque opportunamente documentare l'evento nell'apposito Registro, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura.

Viceversa, se la Violazione dei Dati Personali comporta un rischio per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante della Protezione dei Dati Personali. E' altresì necessario, utilizzando i canali più idonei, procedere con la comunicazione a tutti gli Interessati a meno che il Titolare non abbia già preso misure tali da ridurne considerevolmente l'impatto.

Il Titolare del Trattamento, a prescindere dalla notifica all'Autorità Garante, documenta tutte le violazioni dei dati personali secondo le modalità individuate dall'Ufficio Privacy. Tale

documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Il Responsabile Esterno del Trattamento che venga a conoscenza di un'eventuale violazione è tenuto ad informare tempestivamente il Titolare, in modo che quest'ultimo possa attivarsi secondo quanto disposto dalla normativa.

8.2 Valutazione di Impatto

Il Titolare, prima di effettuare un trattamento, deve procedere ad una Valutazione d'Impatto (DPIA) quando il trattamento medesimo, considerati la natura, l'oggetto, il contesto e le finalità dello stesso, nonché l'eventuale utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ai fini della decisione di effettuare o meno la DPIA, si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione, come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35 del GDPR.

La DPIA non è necessaria nei casi seguenti:

- se il trattamento non presenta un rischio elevato per i diritti e le libertà delle persone fisiche;

- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso, si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

- se il trattamento è stato sottoposto a verifica da parte del Garante della Protezione dei Dati Personali prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta;

- se i trattamenti sono già stati oggetto di verifica preliminare da parte del Garante Privacy o del DPO e che proseguono con le stesse modalità oggetto di tale verifica.

ASL AL, nella predisposizione delle Valutazioni di Impatto sulla Protezione dei Dati Personali, si adegua alle Linee Guida dell'Autorità Garante (Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati WP248 e s.m.i.).

9. Rinvio

Per quanto non espressamente disciplinato, si applicano le disposizioni del GDPR, del Codice Privacy, le Linee Guida del Garante per la Protezione dei Dati Personali e tutte le norme vigenti in materia.

Allegati

Sono parte integrante del presente MOP i seguenti allegati:

- Atto di nomina a Designato del Trattamento (*Allegato 1*)
- Atto di nomina a Responsabile del Trattamento ex art. 28 GDPR (*Allegato 2*)
- Atto di nomina ad Amministratore di Sistema (*Allegato 3*)
- Atto di nomina ad Autorizzato al Trattamento (*Allegato 4*)
- Modulo di segnalazione Data Breach (*Allegato 5*)
- Modello Unico per l'esercizio dei diritti dell'Interessato (*Allegato 6*)

I modelli allegati rappresentano una traccia indicativa dei modelli che l'Azienda deve adottare in ambito di Protezione dei Dati Personali. Per comprovate esigenze ed esclusivamente su disposizione del Titolare, i modelli allegati al presente MOP non necessitano di atto deliberativo per la loro modifica o aggiornamento, ma è sufficiente una semplice disposizione protocollata a sua firma, con opportuna pubblicazione della versione più aggiornata sul sito internet aziendale.

Allegato 1: Atto di nomina a Designato del Trattamento

Egr. Sig.

[*Titolo Cognome Nome del Designato*]

Direttore/Responsabile della Struttura

[*Descrizione Struttura*]

OGGETTO: Atto di nomina a Designato al Trattamento dei Dati Personali (art. 2-quaterdecies Codice privacy)

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati - RGPD)";

Visto in particolare il disposto dell'art. 29 del RGPD inerente al trattamento sotto l'autorità del Titolare del Trattamento o del Responsabile del Trattamento;

Visto il D.lgs. 30 giugno 2003, n.196 recante il "Codice in materia di Protezione dei Dati Personali", così come da ultimo novellato dal D.lgs. 10 agosto 2018, n. 101;

Visto in particolare il disposto dell'art. 2-quaterdecies del D.Lgs. 196/2003 e la libertà organizzativa interna prevista dal RGPD;

Visto il Modello Organizzativo in materia di Protezione dei Dati Personali ("MOP") dell'Azienda Sanitaria Locale di Alessandria;

Visto in particolare l'art. 5.4 del MOP che prevede la nomina quali Designati al Trattamento dei Dati Personali da parte del Titolare del Trattamento dei Direttori delle Strutture Complesse e dei Responsabili delle Strutture Semplici a valenza Aziendale e delle Strutture Semplici a valenza Dipartimentale in cui si articola l'Azienda;

Con la presente, l'Azienda Sanitaria Locale di Alessandria, in qualità di Titolare del Trattamento (in seguito "Titolare"), Le comunica la nomina a Designato al Trattamento dei Dati Personali (in seguito "Designato"), ai sensi dell'art. 29 del Reg. UE 2016/679 (Regolamento Generale sulla Protezione dei Dati - RGPD) e dell'art. 2-quaterdecies del d.lgs. 196/2003 e s.m.i. (Codice della privacy).

Con la presente nomina Lei è pertanto autorizzato a trattare i dati personali relativi ai procedimenti ed alle attività inerenti all'Ufficio di appartenenza, anche per il tramite dei sistemi informativi impiegati dal Titolare ed a coordinare le attività di trattamento svolte dai soggetti autorizzati al trattamento appartenenti a detto Ufficio.

Si precisa che tutti i trattamenti dei dati personali, anche eventualmente quelli di cui all'articolo 9 ("Trattamento di categorie particolari di dati personali") e quelli di cui all'articolo 10 relativi a

condanne penali e reati del Regolamento (UE) 2016/679, autorizzati al Designato dovranno essere svolti esclusivamente nel rispetto delle istruzioni ricevute e di ogni ulteriore indicazione fornita dal Titolare del Trattamento.

I trattamenti che il Designato è autorizzato a svolgere sono quelli relativi all'ufficio in cui il Designato svolge la propria attività lavorativa e specificatamente elencati nel registro dei trattamenti approvato dall'Azienda e che il Designato dichiara di conoscere.

In ogni caso, con la presente nomina il Designato è autorizzato a compiere tutte le operazioni di trattamento, sia in forma cartacea che informatica, di dati personali contenuti all'interno di archivi e/o banche dati, il cui accesso e trattamento si rendano strettamente necessari per lo svolgimento delle attività, mansioni e ruolo funzionale svolto presso le strutture e i locali dell'Azienda.

Con la sottoscrizione della presente lettera di autorizzazione, il Designato dichiara di avere preso visione dell'informativa ai sensi dell'Articolo 13 del RGPD (reperibile sul sito istituzionale di ASL AL), nonché puntuali indicazioni in merito all'ambito del Trattamento dei Dati Personali consentito, le istruzioni operative e le procedure recanti le modalità di Trattamento dei Dati Personali (ai sensi dell'articolo 29 del RGPD), nello specifico:

- Compiti del Designato
- Istruzioni generali per il Trattamento dei dati;
- Istruzioni sull'uso degli strumenti informatici;
- Regole per una corretta tenuta delle Postazioni di Lavoro;
- Istruzioni sull'utilizzo della Posta Elettronica Ordinaria;
- Istruzioni sul Trattamento dei Dati in ambito sanitario;
- Modello Organizzativo in materia di Protezione dei Dati Personali ("MOP") dell'Azienda Sanitaria Locale di Alessandria (allegato).

***

Compiti del Designato

I compiti del Designato sono:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla Struttura di riferimento;
b) collaborare con l'Ufficio Privacy e con il DPO, al fine di consentire agli stessi l'esecuzione dei compiti e delle funzioni assegnate;
c) accertarsi che il personale afferente alla Struttura Organizzativa di competenza, abbia sottoscritto la lettera di nomina ad Autorizzato al trattamento;
d) individuare ed incaricare i Referenti per la Protezione Dati per la propria Struttura Organizzativa. I nominativi dovranno essere comunicati all'Ufficio Privacy;
e) individuare il personale della propria articolazione organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
f) rapportarsi con l'Ufficio Privacy e con il DPO, al fine di adottare soluzioni di "privacy by design" e "privacy by default", ovvero di protezione dei dati fin dalla progettazione e per impostazione predefinita, prevedendo, già dall'origine e in considerazione del contesto

complessivo ove il trattamento si colloca e dei rischi stimati, un paradigma di trattamento e misure di protezione prefissate;

g) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e verificare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura Organizzativa;

h) individuare i Responsabili del trattamento ex art. 28 del GPDR e richiedere la loro nomina al Direttore Generale, mediante utilizzo del modello fornito dall'Ufficio Privacy e comunicare a quest'ultimo l'avvenuta nomina ai fini dell'aggiornamento del relativo registro;

i) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e verificare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura Organizzativa;

j) inoltrare tempestivamente all'Ufficio Privacy e al DPO le richieste pervenute, alla propria Struttura, da parte degli Interessati a questioni legate al trattamento dei dati;

k) rilevare e comunicare tempestivamente all'Ufficio Privacy e al DPO i casi di violazione, anche potenziale, dei dati personali (Data Breach), verificatisi nell'ambito organizzativo di riferimento;

l) verificare, con cadenza almeno semestrale, le abilitazioni rilasciate, per gli applicativi informatici, ai propri collaboratori e segnalare alla Struttura ICT eventuali cessazioni o modifiche nel rapporto di lavoro;

m) inoltrare all'Ufficio Privacy, segnalando la necessità di redigere una valutazione di impatto per un determinato trattamento, le informazioni previste all'art. 35 GDPR sul trattamento in oggetto (descrizione del trattamento, finalità, valutazione delle necessità e proporzionalità del trattamento in relazione alle finalità, valutazione dei rischi e misure previste per affrontare i rischi), al fine di permettere all'Ufficio Privacy di dare avvio alla valutazione per la parte di propria competenza;

n) verificare, una volta esaurita la finalità del trattamento, la corretta ed effettiva eliminazione dei dati raccolti.

Inoltre, il Designato ha il compito di coordinare i trattamenti dei dati personali nella Struttura/Ufficio di competenza, fornendo agli Autorizzati le istruzioni del caso, vigilando sull'osservanza delle disposizioni in materia.

Il Designato deve sempre attenersi alle norme del RGPD, al Codice della privacy (D.lgs. 196/2003 e s.m.i.), ai provvedimenti del Garante e alle istruzioni e misure di sicurezza comunicate dal Titolare, anche mediante Regolamenti interni.

Il Designato si impegna a frequentare i corsi di formazione e aggiornamento, organizzati dal Titolare, in materia di privacy e Protezione dei Dati Personali. Il Designato si impegna, altresì, affinché gli Autorizzati appartenenti alla sua Struttura partecipino ai corsi di formazione ed aggiornamento in materia.

***

Istruzioni generali sul trattamento dei dati

1) Il Designato è tenuto al rispetto ed all'applicazione dei principi generali in ambito di data protection indicati dall'art. 5 del Regolamento Europeo n. 2016/679 "principi applicabili al trattamento di dati personali", quali:

- i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (<<liceità, correttezza e trasparenza>>);
- i dati devono essere raccolti per finalità determinate, esplicite e legittime e, successivamente, trattati in un modo che non sia incompatibile con tali finalità (<<limitazione delle finalità>>);
- i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (<<minimizzazione dei dati>>);
- i dati devono essere esatti e, se necessario, aggiornati (<< esattezza>>);
- i dati devono essere 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>>);
- i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (<<integrità e riservatezza>>).

2) Il Designato deve rispettare le misure tecniche ed organizzative messe in atto dal Titolare.

3) Il Designato deve rispettare il Regolamento Aziendale per l'utilizzo delle postazioni di lavoro e le indicazioni della Struttura ICT relative all'utilizzo di posta elettronica e internet.

4) Il Designato deve rispettare il segreto d'ufficio e/o il segreto professionale. Il DESIGNATO sarà tenuto alla riservatezza anche dopo la cessazione del rapporto di lavoro o il trasferimento o eventuale revoca della nomina.

5) Il Designato deve curare che sia garantita, nella Struttura di competenza, la massima riservatezza, con specifico riferimento alle categorie particolari di dati (dati che rivelano l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).

6) Il Designato deve accertarsi che, all'interno della propria organizzazione, i soggetti Autorizzati al trattamento dei dati abbiano ricevuto apposita nomina.

7) Il Designato deve fornire agli Autorizzati le istruzioni per il corretto Trattamento dei Dati Personali ed eseguire successivamente gli opportuni controlli, vigilando sull'osservanza delle disposizioni impartite.

8) Il Designato deve informare prontamente il Titolare e il Referente Protezione Dati nominato dall'Azienda di ogni questione rilevante in materia.

9) Il Designato deve verificare annualmente con gli Amministratori di Sistema i livelli di abilitazione ai diversi gestionali/applicativi relativi ai singoli Autorizzati al trattamento e aggiornare periodicamente (almeno una volta l'anno) le relative autorizzazioni.

10) Il Designato deve procedere, se necessario, con l'individuazione di ulteriori misure di sicurezza da adottare, sia organizzative, sia fisiche, sia logiche e procedurali.

11) Il Designato vigila affinché siano evitate cessioni, consegne, copiature, riproduzioni, comunicazioni e divulgazioni non autorizzate di dati personali da parte degli Autorizzati della propria Struttura.

12) Il Designato deve rispettare il divieto di fotografare utenti o colleghi nell'esercizio delle loro attività all'interno dell'Azienda.

13) Il Designato deve adottare le istruzioni sopra descritte in tutte le sedi, anche territorialmente dislocate, di competenza.

***

Istruzioni sull'uso degli strumenti informatici

L'accesso agli strumenti informatici (server, applicativi, posta elettronica) deve avvenire attraverso l'utilizzo del proprio profilo di autorizzazione, composto da username (codice identificativo personale) e password (chiave riservata) o altri strumenti di autenticazione messi a disposizione dal Titolare del Trattamento.

1) È necessario che le credenziali di accesso:
- non siano condivise con altri soggetti;
- siano custodite con accuratezza e non rese facilmente visibili/accessibili (es. retrostante tastiera del pc, post-it posto sulla scrivania/monitor, etc.);
- non vengano memorizzate automaticamente dal sistema per un accesso più rapido;
- non siano riportate in elenchi su file elettronici memorizzati sul desktop oppure conservati in agende poste sulla scrivania;
- abbiano una password che rispetti i requisiti di sicurezza e complessità, così come definiti dal Gruppo Sicurezza di cui al Modello Oranizzativo ICT.

2) I supporti removibili (pen drive, hard disk esterni, cd, dvd, etc.) che permettono di copiare/archiviare files e documenti esternamente al PC, sono da considerarsi strumenti di lavoro e come tali essere utilizzati dagli operatori cui la struttura abbia assegnato gli stessi.

3) Alcune regole per la gestione ed utilizzo dei supporti removibili:
- cautela per evitare che il contenuto sia trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
- divieto di uso in luoghi diversi da quelli della sede di lavoro e conservazione in luoghi sicuri (cassettiere o armadi chiusi a chiave);
- l'operatore, se ritiene necessario portare con sé lo strumento, dovrà ritenersi responsabile in caso di furto o perdita dello stesso e farne tempestiva comunicazione al Titolare.

4) Se la struttura ha messo a disposizione degli operatori telefoni cellulari, questi ultimi dovranno rispettare le seguenti regole:
- non memorizzare immagini/video personali;
- non riportare numeri di telefono di propri familiari o conoscenti;
- usare smartphone criptati;
- attivare blocco schermo temporizzato con PIN o altro sistema per sblocco;

- non scaricare App per uso personale (social network, home banking, posta elettronica personale, acquisti);
- non effettuare backup automatici su Google, Whatsapp o sistemi similari;
- riversare su server dell'organizzazione video/immagini raccolti per fini lavorativi evitando di utilizzare Whatsapp, Dropbox o sistemi similari.

L'abuso o l'uso scorretto degli strumenti assegnati (computer, dispositivi portatili, posta elettronica, banche dati, collegamento ad Internet, credenziali di accesso, social network) costituiscono comportamenti contrari ai doveri di diligenza e fedeltà, punibili con sanzioni disciplinari e penali.

***

Regole per una corretta tenuta della postazione di lavoro

1) La postazione di lavoro è uno strumento da utilizzare secondo le regole della diligenza e della buona condotta e ciò rende ciascun operatore responsabile della sua corretta tenuta;

2) Ogni utilizzo non conforme può causare disservizi, costi di manutenzione, minacce di sicurezza, danni a persone o al patrimonio informativo del Titolare del Trattamento, da ciò ne deriva che ciascun utente è tenuto a rispettare la configurazione e gli strumenti applicativi messi a disposizione dall'organizzazione per lo svolgimento della propria mansione;

3) I documenti in lavorazione e le cartelle devono essere memorizzati in apposite aree di rete dedicate presenti sul server per evitare dispersioni o perdita di informazioni o accesso illecito agli stessi;

4) Non è permesso il salvataggio di file dell'organizzazione sulla memoria locale del PC, né in apposite cartelle locali, né sul desktop, per i quali non sono garantite operazioni di manutenzione, backup e ripristino dei dati, in casi di perdita;

5) Trattandosi di strumento di lavoro, non è consentito memorizzare sulla propria postazione documentazione personale (file, fotografie, video), installare dispositivi di comunicazione o memorizzazione (modem, masterizzatori) e scaricare software senza l'autorizzazione preventiva del Titolare del Trattamento o della Struttura ICT;

6) Al fine di evitare accessi illeciti a dati personali, l'utente è tenuto a:
- adottare politiche dello "schermo pulito";
- non lasciare incustodita la postazione con documentazione riservata visibile;
- eseguire la procedura di logout dall'applicativo e/o dal sistema operativo tramite la funzione del blocca/disconnetti;
- attivare screensaver il cui sblocco è reso possibile attraverso l'inserimento di password.

***

Istruzioni sull'utilizzo della posta elettronica ordinaria

1) La posta elettronica ordinaria, sia intestata all'Ufficio/Struttura, sia nominativa, è da considerarsi uno strumento di lavoro messo a disposizione dal Titolare del Trattamento.

2) Deve essere utilizzata solo per motivi strettamente connessi allo svolgimento dell'attività lavorativa.

3) Non deve essere considerata "privata" anche se recante il proprio nome e cognome.

4) Soggetti assegnatari di account di posta elettronica ordinaria sono responsabili del corretto utilizzo dello stesso e sono obbligati a rispettare anche i criteri definiti per l'accesso agli strumenti informatici.

5) È fatto divieto di utilizzare l'account messo a disposizione dal Titolare del Trattamento per:
- trasmettere e ricevere documenti di natura personale;
- fare re-inoltri dei messaggi su caselle di posta elettronica personale con dominio diverso da quello dell'organizzazione;
- trasmettere documenti ufficiali dell'organizzazione recanti rilevanza giuridica verso terzi per cui è richiesto l'utilizzo della posta elettronica certificata istituzionale. Si rispettino, pertanto, le regole definite per una corretta gestione documentale informatica nelle more dei principi dettati dal Codice dell'Amministrazione Digitale (D.lgs. 82/2005 smi).

6) Per la trasmissione di documenti/dati/informazioni (es. bozze, documenti informali) contenenti categorie particolari di dati (es. dati idonei a rivelare lo stato di salute) è necessario utilizzare delle maggiori cautele, ovvero:
- trasmettere i dati come allegato e non come testo nel corpo del messaggio;
- cifrare i dati rendendo nota al destinatario la chiave crittografica tramite canali differenti da quelli utilizzati per la trasmissione stessa;
- proteggere l'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi (es. password per l'apertura del file resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati).

7) In ambito sanitario, la trasmissione di referti tramite posta elettronica è una pratica non corretta.

8) I messaggi di posta elettronica sono uno dei principali vettori di attacco ai sistemi informatici che rendono necessari accorgimenti particolari quali:
- non aprire mail che risultano sospette;
- diffidare da mail che, sebbene arrivate da indirizzi conosciuti, richiedono l'apertura di un allegato tramite l'inserimento di password o codici;
- non procedure con l'avvio di codici eseguibili qualora la mail lo richieda.

***

Istruzioni sul trattamento di dati in ambito sanitario

Nel trattamento dei dati relativi alla salute delle persone, il Designato deve assicurare il rispetto, anche da parte degli Autorizzati al trattamento della propria Struttura, delle regole seguenti.

1) Dignità della persona
La prestazione medica e ogni operazione di Trattamento dei Dati Personali deve avvenire nel pieno rispetto della dignità dell'Interessato.

La tutela della dignità personale deve essere garantita nei confronti di tutti gli utenti dei servizi sanitari, con particolare riguardo ai soggetti più vulnerabili quali:

- disabili, fisici e psichici
- minori
- anziani
- pazienti sottoposti a trattamenti medici invasivi
- persone sieropositive
- donne che abbiano richiesto o effettuato l'interruzione volontaria della gravidanza
- persone offese da atti di violenza sessuale
- pazienti ricoverati nei reparti di rianimazione/terapia intensiva
- tossicodipendenti o persone affette da altre dipendenze (ad es. etilismo o ludopatia)

2) Trasparenza e informazione

In base alle norme vigenti (Reg. UE 2016/679, art. 9 par. 2 lett. h), non occorre il consenso dell'Interessato per finalità di diagnosi, terapia, cura ed assistenza sanitaria o sociale.
L'Autorizzato verifica che l'Interessato abbia ricevuto l'informativa sul trattamento dei dati relativi alla salute e che abbia firmato per presa visione il documento predisposto dal Titolare.
Ove previsto, in luogo della firma per presa visione, l'Autorizzato può annotare di aver fornito l'informativa nel documento (cartaceo o digitale) predisposto dal Titolare.
E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.
Laddove l'Interessato intenda esercitare un proprio diritto relativo al trattamento dei dati (es. richiesta di accesso o cancellazione di dati personali), l'Autorizzato trasmette la richiesta all'Ufficio Privacy (email: privacy@aslal.it) o al Responsabile della Protezione dei Dati Personali (email: dpo@aslal.it).

3) Riservatezza nei colloqui e nelle prestazioni sanitarie

L'Autorizzato deve tutelare la riservatezza dei dati personali e della documentazione in suo possesso riguardante le persone, anche se affidata a codici o sistemi informatici.
L'Autorizzato non deve diffondere, attraverso la stampa o altri mezzi di informazione, notizie che possano consentire l'identificazione del paziente.
L'Autorizzato presta particolare attenzione alle modalità di svolgimento dei colloqui con gli utenti dei servizi sanitari ed assistenziali (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che le informazioni sulla salute dell'Interessato possano essere accidentalmente conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.
È vietata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico.
L'Autorizzato cura che i documenti contenenti informazioni cliniche dell'Interessato non siano resi visibili a terzi non legittimati (es. cartelle infermieristiche poste in prossimità del letto di degenza).
E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

4) Informazioni sullo stato di ricovero o sulla salute di un paziente

L'Autorizzato si attiene alle eventuali indicazioni del paziente (se cosciente e capace) circa i soggetti che possono essere informati del ricovero, del reparto di degenza o dello stato di salute.
L'Autorizzato rispetta l'eventuale richiesta dell'Interessato di non comunicare tali informazioni

neanche ai terzi legittimati.
Le informazioni da fornire ai terzi legittimati riguardano la sola presenza nel reparto; l'Autorizzato si assicura dell'identità della persona prima di fornire ogni informazione.
L'Autorizzato non comunica informazioni sullo stato di salute, salvo che l'Interessato abbia manifestato il proprio consenso. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere del paziente, il consenso può essere manifestato da parte di un altro soggetto legittimato.
E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

5) Notizie su prestazioni di Pronto Soccorso

L'Autorizzato in servizio nel Pronto Soccorso, se ciò rientra nelle proprie mansioni, può dare notizia (o conferma), anche telefonica, dell'accesso di un paziente alla struttura ai soli soggetti legittimati: familiari, parenti o conviventi del paziente. L'Autorizzato si assicura dell'identità della persona prima di fornire ogni informazione.
L'Autorizzato di Pronto Soccorso si limita, in tal caso, a comunicare che è in atto o si è svolta una prestazione e non fornisce informazioni sullo stato di salute.
L'Interessato - se cosciente e capace - deve essere preventivamente informato (ad es. in fase di accettazione), e posto in condizione di indicare i soggetti che possono essere informati della prestazione di pronto soccorso. L'Autorizzato rispetta eventuali indicazioni specifiche o contrarie del paziente.
E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

6) Distanza di cortesia

L'Autorizzato verifica che siano rispettate le distanze di cortesia nelle operazioni di sportello, nell'acquisizione di informazioni sullo stato di salute e, in generale, nelle operazioni di trattamento di dati sanitari.
E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

7) Ordine di precedenza e di chiamata nelle sale di attesa (escluso Pronto Soccorso)

Al di fuori del reparto di Pronto Soccorso, nell'erogare prestazioni sanitarie, assistenziali o amministrative, che richiedono un periodo di attesa (ad es., analisi cliniche, visite ambulatoriali), l'Autorizzato rispetta le misure tecnico organizzative adottate dal Titolare per evitare la chiamata nominativa dei pazienti (ad es., uso di codici forniti all'utente in fase di prenotazione o accettazione).
Se la chiamata nominativa risulta necessaria (ad es. in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), l'Autorizzato, ove possibile, cerca di instaurare un contatto diretto con il paziente per chiamarlo.
E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

8) Consegna di documentazione sanitaria

Per la consegna di documentazione sanitaria (es. certificati, referti, copie di cartelle cliniche) o di altra documentazione da cui si desuma lo stato di salute della persona (es. fatture, ricevute di prenotazione di prestazioni, etc.), l'Autorizzato si attiene alle istruzioni fornite dal Titolare e dal Direttore o Responsabile della Struttura (Designato).
In mancanza di diverse istruzioni, i documenti vengono consegnati solo in formato cartaceo ed in busta chiusa.Tali documenti vengono consegnati al diretto Interessato o a terzi soggetti legittimati (es. genitori del minore) o muniti di delega scritta accompagnata dal documento d'identità.

E' compito del Designato vigilare sulla corretta applicazione di quanto sopra.

9) Violazione dei Dati Personali

Il Designato informa immediatamente (e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza) l'Ufficio Privacy (email: privacy@aslal.it) e il Responsabile della Protezione dei Dati Personali (email: dpo@aslal.it) 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.

***

La presente nomina è da intendersi a tempo indeterminato e copre l'intera durata dell'incarico di Direttore/Responsabile della Struttura. Può essere revocata dal Titolare del Trattamento dei Dati Personali o può terminare in caso di interruzione del rapporto di lavoro, salvo eventuali e/o diversi accordi tra le Parti.
L'attività di trattamento individuata nel presente atto sarà soggetta a revisione almeno annuale; da ciò discende la possibilità che nel periodo intercorrente tra due revisioni le attività di trattamento possano differire da quelle ivi indicate. In tali casi il soggetto destinatario della presente si riterrà comunque autorizzato allo svolgimento dei trattamenti derivanti dalle attività conferite sulla base di specifica disposizione organizzativa sviluppata nelle forme individuate dal Titolare del Trattamento. Le casistiche nelle quali i trattamenti dovranno considerarsi autorizzati pur in assenza di specifica indicazione nel presente atto sono le seguenti:

- impiego temporaneo di personale in attività generalmente non di competenza del medesimo per la gestione di urgenze;
- impiego temporaneo di personale in attività generalmente non di competenza del medesimo per esigenze organizzative non superiori ad un mese;
- impiego di personale in attività caratterizzata da "turnazione" degli addetti la quale comporti lo svolgimento di attività non di competenza dell'unità organizzativa a cui è assegnato il soggetto.

***

Il Designato dichiara di aver ricevuto le istruzioni, di averne presa visione e di impegnarsi ad adottare tutte le misure necessarie alla loro attuazione.

***

Presa visione della nomina a Soggetto Designato in data [*gg/mm/aaaa*] da parte del dott. [*Nome Cognome Designato*]

Firma: _____

Allegato 2: Atto di nomina a Responsabile del Trattamento ex art. 28 GDPR

ADDENDUM AL [rapporto] [oggetto del servizio] [ANNO] [DELIBERA/DETERMINA]

Il presente Addendum disciplina le responsabilità dell'**Azienda Sanitaria Locale Alessandria**, (di seguito anche "ASL AL") con sede legale in Via Venezia n.6, 15121 Alessandria, Titolare del Trattamento[1] (l'Azienda o il "Titolare[2]") e del Contraente Fornitore **[AZIENDA]** ciascuno dei quali deve intendersi come "Parte" e congiuntamente come "Parti", per gli aspetti relativi alla Protezione dei Dati Personali ed integra il contratto in oggetto relativo a: "**[OGGETTO]**", **[CIG]**.

Le disposizioni indicate nel presente atto si riferiscono a qualsiasi dato personale[3] trattato dal Contraente per conto dell'ASL AL, in relazione ai servizi oggetto del Contratto, laddove tale trattamento rientri nel campo di applicazione del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("GDPR").

Questo Addendum, stipulato in forma scritta in coerenza con l'art. 28, par. 9 del GDPR, è soggetto ai medesimi termini e condizioni dell'accordo (contratto, convenzione, ecc.), salvo diversamente disposto e sarà considerato parte integrante dello stesso.

CONSIDERAZIONI

- È in vigore il Regolamento (UE) 2016/679 che garantisce la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto di Protezione dei Dati Personali.
- È in essere un Contratto tra l'Azienda e il Fornitore, approvato con **[DELIBERA/DETERMINA]** ASL AL n. **[NUMERO]** del **[DATA],** che ha per oggetto: "**[OGGETTO]**".
- Ai sensi dell'art. 28, paragrafo 1, del GDPR, qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del Trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate nell'ambito della Protezione dei Dati Personali.
- L'articolo 28, par. 3, del GDPR prevede che i trattamenti dei dati personali siano disciplinati da un contratto o da altro atto giuridico, che indichi alcune informazioni riguardanti il trattamento e che contenga alcune condizioni (così descritte nel seguito).

---

1 Per "*trattamento*" si intende, 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 (art. 4 par. 2 del GDPR).

2 Per *Titolare",* come definito ai sensi del Regolamento UE 2016/679 ("GDPR"), si intende 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 (art 4 par. 7 del GDPR).

3 Per "*dato personale*" si intende 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 (art. 4 par. 1 del GDPR).

Sulla base di questo Addendum:

l'**ASL AL**, Titolare del Trattamento dei Dati Personali **NOMINA** il Contraente **[AZIENDA]**, *che accetta l'incarico,* **Responsabile del Trattamento**[4], ai sensi e per gli effetti degli articoli 4, par. 8 e 28 del Regolamento (UE) 2016/679 ("GDPR").

Le Parti concordano l'osservanza delle seguenti DISPOSIZIONI

L'ASL AL è il Titolare dei dati personali e **[AZIENDA]** deve intendersi il Responsabile del Trattamento di tali dati, e ciascuna delle Parti deve uniformarsi alla vigente normativa sulla Protezione dei Dati Personali, in quanto applicabile alle Parti nei loro rispettivi ruoli.

1. Il presente Addendum stabilisce:
   a) oggetto del trattamento: è limitato ai Dati Personali del Titolare così come identificati in questo Addendum;
   b) natura e finalità del trattamento: la prestazione dei servizi come definiti con **[DELIBERA/DETERMINA]** ASL AL n. **[NUMERO]** del **[DATA]** - CIG n. **[CIG]**. I dati sono trattati per finalità **[FINALITA']**;
   c) tipologia di dati personali trattati:

Tipo di dato	Descrizione	Sì	No
Dati identificativi	Nome e cognome, data e luogo di nascita, indirizzo di residenza, numeri di telefono, indirizzi email, numeri identificativi dei documenti e carte di pagamento, identità digitale, ecc.		
Dati particolari	Dati relativi all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati giudiziari, ecc.		
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca.		

   d) categorie di Interessati: **[CATEGORIE INTERESSATI]**;
   e) durata del trattamento: durata affidamento fino alla cancellazione dei dati oggetto del trattamento.
2. Nell'espletamento dell'incarico, il Fornitore, nella qualità di Responsabile del Trattamento, tratterà i dati personali del Titolare conformemente alle istruzioni di trattamento di seguito enunciate dal Titolare di cui al Contratto e a questo Addendum, se non diversamente previsto dalla legge. I trattamenti eseguiti dal Fornitore dovranno essere svolti nel pieno rispetto delle previsioni legislative vigenti in materia di Protezione dei Dati Personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali.

[4] Per "*responsabile del trattamento*" si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare (art. 4 par. 8 del GDPR).

3. Il Fornitore garantirà che le persone autorizzate al trattamento (inclusi i subfornitori) siano vincolate da un obbligo, legalmente assunto, di riservatezza. Le persone autorizzate al trattamento operano sotto la diretta responsabilità del Fornitore.

4. Il Fornitore dovrà eseguire i trattamenti in modo non incompatibile con le finalità per cui i dati sono stati raccolti e trattati. Qualora sorgesse la necessità di effettuare trattamenti sui dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, Il Fornitore dovrà preventivamente informare il Titolare.

5. Il Fornitore adotterà misure di sicurezza tecniche e organizzative adeguate per proteggere i dati personali del Titolare in coerenza ed ai sensi dell'articolo 32 del GDPR e delle vigenti pertinenti disposizioni. In particolare, tenuto conto dello stato dell'arte delle misure di sicurezza applicabili, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze derivate dall'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Fornitore attiverà le misure adeguate per proteggere i dati personali, in particolare e ad esempio dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi dal Titolare, conservati o comunque trattati.
   Tali misure comprendono, tra le altre:
   a) la cifratura dei dati personali;
   b) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
   d) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

6. Il Fornitore dovrà attivare le necessarie procedure aziendali per identificare ed istruire tutto il personale Autorizzato al Trattamento dei Dati Personali ed organizzarli nei loro compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente Addendum, facendo anche in modo che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati.
   Pertanto il Fornitore si impegna a far svolgere attività di formazione in materia di Protezione dei Dati Personali ai propri dipendenti e ai collaboratori autorizzati al trattamento.

7. Il Fornitore, se richiesto per iscritto dell'ASL AL, dovrà cancellare e/o restituire tutti i dati personali al termine della prestazione dei servizi relativi al trattamento e cancellare tutte le copie esistenti in qualsiasi formato e/o supporto. Il Fornitore fornirà attestazione scritta dell'avvenuta distruzione dei dati personali del Titolare.

8. Il Fornitore assisterà l'ASL AL nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36

del GDPR[5], tenuto conto della natura del trattamento e delle informazioni di cui dispone in qualità di Responsabile del Trattamento.

9. Il Fornitore, ai sensi dell'art. 33 paragrafo 2, nel caso venga a conoscenza di una Violazione dei Dati Personali (Data Breach), è tenuto ad informare tempestivamente e senza ingiustificato ritardo l'ASL AL. Nell'ipotesi di un Data Breach, il Fornitore dovrà collaborare (obbligando i suoi sub-responsabili o sub-fornitori a cooperare) con il Titolare nell'indagine sul data Breach e su quanto correlato alla gestione dello stesso, nell'ambito di apposite procedure adottate dal Titolare e/o attivate dal Fornitore, nel rispetto dei tempi concordati tra le Parti e dei termini di legge.

10. Il Fornitore assisterà il Titolare, per quanto ragionevolmente e tecnicamente possibile, con misure tecniche ed organizzative adeguate qualora sia necessario dare seguito a specifiche richieste di esercizio dei diritti dell'Interessato, così come enunciati dal Capo III del GDPR, inclusi il diritto di accesso, rettifica, cancellazione, portabilità e il diritto di limitazione o opposizione a taluni trattamenti.

11. L'ASL AL, ai sensi dell'art 28 par. 2 del GDPR, **AUTORIZZA** il Fornitore ad avvalersi di soggetti terzi, Responsabili del trattamento (responsabili o sub-responsabili), per l'esecuzione di specifiche attività rientranti nell'oggetto del contratto in essere tra le parti.
    Il Fornitore renderà noto al Titolare la lista dei responsabili/sub-responsabili autorizzati al Trattamento dei Dati Personali del Titolare e le attività di trattamento delegate.
    Il Fornitore informerà tempestivamente, attraverso comunicazione scritta, il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di uno o più responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche.
    Le Parti concordano nel disciplinare, mediante apposita procedura, la gestione del processo di modifica della nomina a responsabile.
    Il Fornitore informerà tempestivamente l'ASL AL del ricorso a un altro Responsabile del Trattamento e procederà alla nomina di tale altro responsabile, imponendo, mediante contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati contenuti nel presente Addendum, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR.
    Qualora l'altro Responsabile del Trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Fornitore conserverà nei confronti dell'ASL AL l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile, così come disposto dall'art. 28, paragrafo 4 del GDPR.

12. In caso di trasferimento di dati personali del Titolare verso un paese terzo, extra UE, o un'organizzazione internazionale, ad esempio perché il Fornitore o l'eventuale sub-responsabile è stabilito in un paese extra UE, il Fornitore garantisce per conto del titolare un livello di Protezione dei Dati Personali adeguato, nel rispetto delle norme di cui al Capo V del GDPR (art. 44 e seguenti). Le parti prendono atto dell'applicazione delle pertinenti disposizioni di cui all'art. 28 par. 3, lett. a), del GDPR e cooperano per l'esecuzione degli obblighi.

[5] Art. 32 "Sicurezza del trattamento"; art. 33 "Notifica di una violazione dei dati personali all'autorità di controllo"; art. 34 "Comunicazione di una violazione dei dati personali all'interessato"; art. 35 "Valutazione d'impatto sulla protezione dei dati"; art. 36 "Consultazione preventiva".

13. Il Fornitore renderà disponibili al Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dall'art.28 del GDPR e degli impegni stabiliti in questo Addendum, consentendo al Titolare di effettuare periodicamente un'attività di verifica, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato, in base ad una procedura stabilita di comune accordo delle Parti. Il Fornitore, qualora secondo la sua opinione, una prescritta disposizione di questo Addendum violi il GDPR o la normativa (europea o nazionale) vigente applicabile, informerà immediatamente l'ASL AL.

14. Il Fornitore si impegna a compilare e restituire, debitamente firmato, unitamente al presente Addendum, l'allegato tecnico "C2" Checklist di Verifica del Responsabile.

Amministratori di Sistema

Il Fornitore si impegna ad adottare, per conto del Titolare, ogni misura idonea a garantire l'osservanza del provvedimento del Garante per la Protezione dei Dati Personali emanato in data 27 novembre 2008 e successive modifiche e integrazioni: "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" (di seguito "Provvedimento AdS").

In particolare, il Fornitore dovrà valutare la sussistenza dei requisiti previsti dal suddetto Provvedimento per la selezione del personale da designare come Amministratore di Sistema (di seguito "AdS"), e dovrà provvedere, una volta individuato tale personale, ad effettuare le designazioni individuali previste dal Provvedimento AdS di coloro i quali svolgano funzioni dedicate alla gestione e alla manutenzione delle apparecchiature di elaborazione del Titolare con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza.

Il Fornitore, al momento della sottoscrizione del presente atto e comunque con cadenza almeno annuale, dovrà comunicare al Titolare (scrivendo al Responsabile della Struttura ICT dell'ASL AL), gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati e/o di Rete. Il Fornitore dovrà consentire all'ASL AL l'esercizio, con cadenza almeno annuale, delle attività di verifica dell'operato degli Amministratori prescritte dal Provvedimento AdS.

In coordinamento con il Fornitore, il Titolare si riserva di adottare misure tecniche ed organizzative idonee ai fini di assolvere ai compiti per esso assegnati dal provvedimento sopra citato in materia di tenuta degli elenchi nominativi degli "AdS" e di gestione dei log di accesso ai sistemi del Titolare.

Modifiche normative e interpretative.

Per quanto concerne le tutele da adottare dalle Parti in caso di modifiche, integrazioni normative e interpretative di norme, incluse quelle in materia di Protezione dei Dati Personali, si rimanda a quanto disciplinato dalla normativa vigente.

****

Con la sottoscrizione del presente Addendum, **[AZIENDA]** accetta l'incarico di **RESPONSABILE DEL TRATTAMENTO**, ai sensi e per gli effetti delle disposizioni contenute negli articoli 4. par. 8 e 28 del GDPR, con riguardo alle operazioni di trattamento connesse all'esecuzione del suddetto contratto e, in ottemperanza di quanto disposto dall'art. 28 del GDPR, dichiara che le operazioni di Trattamento dei Dati Personali del Titolare avverrà in conformità a quanto previsto dal GDPR, attenendosi al presente Addendum e alle istruzioni impartite dal Titolare.

La validità del presente Addendum si intende altresì estesa ad ulteriori, eventuali proroghe contrattuali; ogni altra pattuizione resta pienamente confermata ed impregiudicata.
In relazione a quanto sopra esposto, La preghiamo di voler restituire all'ASL AL il presente atto sottoscritto per approvazione ed accettazione.

Per accettazione:

Azienda Sanitaria Locale Alessandria

[AZIENDA]

_____

<firma per esteso nome e cognome>

Per il Titolare , Firma del Legale Rappresentante

Data _____

_____

<firma per esteso nome e cognome>

Per il Responsabile, Firma del Legale Rappresentante

Data _____

Allegato 3: Atto di designazione ad Amministratore di Sistema

[NOME] [COGNOME]

Oggetto: **Atto di Designazione ad Amministratore di Sistema (ai sensi del provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 27 novembre 2008 ss.mm.ii).**

L'Azienda Sanitaria Locale Alessandria (di seguito, "ASL AL"), con sede legale in via Venezia n.6, 15121 Alessandria, rappresentata dal [Direttore Generale/Commissario] [Nome e Cognome del Titolare], munito dei necessari poteri per il compimento del presente atto (di seguito, "il Titolare"),

Il Titolare, dr. [Nome e Cognome del Titolare],

PREMESSO CHE:

1. È in vigore e pienamente applicabile il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito, il "GDPR") che garantisce la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto di Protezione dei Dati Personali;
2. Il GDPR, integrato da leggi e provvedimenti nazionali, costituisce la disciplina applicabile al Trattamento dei Dati Personali (di seguito, la "Normativa Privacy Applicabile");

VISTO CHE:

a) È vigente, in quanto non in contrasto con la Normativa Privacy Applicabile, il Provvedimento del Garante per la Protezione dei Dati Personali "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di "Amministratore di Sistema", emanato in data 27/11/2008 e pubblicato sulla Gazzetta Ufficiale del 24/12/2008 e successive modifiche ed integrazioni;
b) Il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Sistemi Software Complessi (Complex Software System Administrators) o degli Amministratori di Rete (Network Administrator) che, nell'esercizio delle proprie funzioni, hanno accesso, anche limitato e/o occasionale, ai dati personali;
c) Gli Amministratori di Sistema esercitano le funzioni in un contesto che rende ad essi tecnicamente possibile l'accesso, anche fortuito, a particolari categorie di dati personali previste dall'art. 9 del GDPR, tra cui i dati relativi alla salute, e ai dati relativi a condanne penali e reati previsti dall'art. 10 del GDPR;

CONSIDERATO CHE:

1. [NOME] [COGNOME], con Codice Fiscale [CODICE FISCALE] e [DIPENDENTE/COLLABORATORE ESTERNO] dell'ASL AL, nella sua qualità di [RUOLO], utilizza per lo svolgimento delle sue funzioni tecniche i seguenti profili utente di tipo Amministratore*:

   Applicativo: [APPLICATIVO] Account: [ACCOUNT]

2. tenuto conto della sua esperienza professionale, in particolare con riferimento alle capacità e affidabilità dimostrate nello svolgimento delle proprie funzioni, è in possesso dei requisiti richiesti dal Provvedimento per assolvere la funzione di AdS;
3. [NOME] [COGNOME] ha confermato di possedere tutti i requisiti riconosciutigli dal Titolare, e indicati alla precedente lett. a), fornendo idonea garanzia al pieno rispetto delle vigenti disposizioni in materia di trattamento (ivi compreso il profilo relativo alla sicurezza) e, pertanto, ha manifestato la propria disponibilità ad assolvere l'incarico di AdS, ai sensi delle disposizioni dettate nel Provvedimento;

VALUTATA:

La necessità di assicurare che i trattamenti di dati personali di titolarità dall'ASL AL siano svolti nel pieno rispetto di qualsiasi disposizione prevista dalla Normativa sulla Protezione dei Dati Personali Applicabile.

TUTTO CIO' PREMESSO
DESIGNA

[NOME] [COGNOME]
AMMINISTRATORE DI SISTEMA ("AdS")
Per i sistemi dettagliati in premessa

autorizzandolo a compiere le attività e le mansioni svolte per conto dell'ASL AL e consentite in base al suo profilo di autorizzazione, così come descritte nel presente atto.
A tal proposito, è di seguito precisato l'elenco degli ambiti di operatività che Le sono consentiti quale Amministratore di Sistema in base al profilo di autorizzazione assegnato, con espresso riferimento al Registro delle Attività di Trattamento:

1. [*Elencare qui le operazioni autorizzate per l'AdS sul Sistema Informativo*]
2.
3.
4.
5.
6.
7.
8.
9.
10.

L'Amministratore di Sistema

ACCETTA LA DESIGNAZIONE

e, nel confermare la conoscenza degli obblighi che si assume in relazione alle prescrizioni dettate dal Provvedimento,

SI IMPEGNA A

1. osservare, nell'adempimento dell'esercizio delle proprie funzioni, le istruzioni, attuali e future, impartite dal Titolare e/o dal responsabile interno** del trattamento. In tal senso, l'Amministratore di Sistema opera quale persona autorizzata al trattamento di dati personali, ai sensi dell'art.29 del GDPR.
2. comunicare prontamente al Titolare e/o al responsabile interno del trattamento, seguendo le procedure adottate dal Titolare in materia di Incident Management, Data Breach e altre applicabili allo specifico caso, qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto e lecito Trattamento dei Dati Personali;
3. collaborare con il Titolare e/o il responsabile interno del trattamento per l'attuazione delle prescrizioni impartite dall'Autorità Garante per la Protezione dei Dati Personali;

La informiamo, inoltre, che, ai sensi del punto 4.5 del Provvedimento Amministratori di Sistema, le sue attività compiute in qualità di AdS devono essere registrate dal Titolare, in ottemperanza alla normativa vigente, anche con particolare riferimento alle tutele di cui all'art. 4 della L. n. 300/70 (Statuto dei Lavoratori). Si rammenta, ad esempio, che, ai sensi del citato Provvedimento:

1. l'operato dell'Amministratore di Sistema dovrà essere oggetto con cadenza almeno annuale, nei limiti consentiti dalle norme legali e contrattuali, di un'attività di verifica da parte del Titolare del Trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati personali previste dalle norme vigenti;
2. è prevista, mediante l'adozione di idonei sistemi, la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell'Amministratore di Sistema e la conservazione degli stessi per un congruo periodo, non inferiore a 6 mesi. I dati registrati a tale scopo dai sistemi non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.

La presente designazione ha validità per tutta la durata del rapporto contrattuale intercorrente tra il Titolare e l'ADS, salva la facoltà di revoca, in qualsiasi momento, del Titolare. La perdita accertata da parte dell'AdS dei requisiti di cui al paragrafo a. del Provvedimento sopracitato al numero 1. del CONSIDERATO di cui al presente atto, consentirà al Titolare di esercitare la facoltà di revoca mediante invio di una comunicazione scritta contenente la manifestazione di tale volontà.

In caso di cessazione, per qualunque causa, dell'efficacia del presente atto di designazione, l'AdS dovrà interrompere ogni operazione di trattamento dei dati, agevolando, per quanto di sua competenza, l'eventuale "passaggio di consegne" con il nuovo AdS designato dal Titolare.

In relazione a quanto sopra esposto, la preghiamo di voler trasmettere all'Ufficio Privacy di ASL AL il presente atto di incarico sottoscritto per accettazione e presa visione entro e non oltre 15 giorni

solari dal suo ricevimento.

Alessandria, li [DATA]

_____

Il Titolare del Trattamento <firma per nome e cognome>

Per ricevuta e accettazione:

_____

L'Amministratore di Sistema <firma per nome e cognome>

[*] La valutazione delle caratteristiche soggettive dell'Amministratore di Sistema dovrà essere eseguita dal Responsabile della Struttura ICT.

[**] I responsabili (interni) del trattamento, identificati dall'ASL AL, pur conservando la denominazione avuta finora, diventano soggetti che operano sotto l'autorità diretta del titolare ai sensi dell'art.29 del GDPR, ai quali l'Azienda – in forza di una propria scelta organizzativa ritenuta opportuna e compatibile con il quadro disegnato dal GDPR – attribuisce particolari deleghe nella gestione dell'organigramma privacy interno, conferendo, di fatto, la delega ad identificare i soggetti autorizzati al trattamento ai sensi dell'Art. 29 del GDPR (persone incaricate del trattamento ai sensi dell'art. 30 del Codice Privacy - articolo abrogato).

Allegato 4: Atto di nomina ad Autorizzato al Trattamento

Egr. Sig.

[Cognome Nome dell'AUTORIZZATO]

[DESCRIZIONE STRUTTURA]

OGGETTO: Atto di nomina ad Autorizzato al Trattamento dei Dati Personali (art. 2-quaterdecies Codice privacy)

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati - RGPD)";

Visto in particolare il disposto dell'art. 29 del RGPD inerente al trattamento sotto l'autorità del Titolare del Trattamento o del Responsabile del Trattamento;

Visto il D.lgs. 30 giugno 2003, n.196 recante il "Codice in materia di Protezione dei Dati Personali", così come da ultimo novellato dal D.lgs. 10 agosto 2018, n. 101;

Visto in particolare il disposto dell'art. 2-quaterdecies del D.Lgs. 196/2003 e la libertà organizzativa interna prevista dal RGPD;

Visto il Modello Organizzativo in materia di Protezione dei Dati Personali ("MOP") dell'Azienda Sanitaria Locale di Alessandria;

Visto in particolare l'art. 5.7 del MOP che prevede l'individuazione da parte del Titolare del Trattamento delle persone ammesse a compiere operazioni sui dati personali quali Autorizzati al Trattamento dei Dati Personali;

Con la presente, l'Azienda Sanitaria Locale di Alessandria, in qualità di Titolare del Trattamento (in seguito "Titolare"), Le comunica la nomina ad Autorizzato al Trattamento dei Dati Personali (di seguito "Autorizzato"), ai sensi dell'art. 29 del Reg. UE 2016/679 (Regolamento Generale sulla Protezione dei Dati - RGPD) e dell'art. 2-quaterdecies del d.lgs. 196/2003 e s.m.i. (Codice della privacy).

Con la presente nomina Lei è pertanto autorizzato a trattare i dati personali relativi ai procedimenti ed alle attività inerenti all'Ufficio di appartenenza, anche per il tramite dei sistemi informativi impiegati dal Titolare.

Si precisa che tutti i trattamenti dei dati personali, anche eventualmente quelli di cui all'articolo 9 ("Trattamento di categorie particolari di dati personali") e quelli di cui all'articolo 10 relativi a condanne penali e reati del Regolamento (UE) 2016/679, autorizzati dal Designato dovranno essere svolti esclusivamente nel rispetto delle istruzioni ricevute e di ogni ulteriore indicazione fornita dal Titolare del Trattamento per il perseguimento delle finalità istituzionali.

I trattamenti consentiti all'Autorizzato sono quelli relativi all'Ufficio in cui svolge la propria attività lavorativa e specificatamente elencati nel registro dei trattamenti approvato dall'Azienda e che l'Autorizzato dichiara di conoscere.

In ogni caso, con la presente nomina, all'Autorizzato è consentito compiere tutte le operazioni di

trattamento, sia in forma cartacea che informatica, di dati personali contenuti all'interno di archivi e/o di banche dati, il cui accesso e trattamento si rendano strettamente necessari per lo svolgimento delle attività, mansioni e ruolo funzionale svolto presso le strutture ed i locali dell'Azienda.

L'Autorizzato può effettuare le operazioni di elaborazione dei dati personali, contenuti in atti e documenti presenti negli archivi di tipo cartaceo o trattati con strumenti automatizzati e/o contenuti nelle eventuali banche dati elettroniche automatizzate, necessarie per lo svolgimento delle proprie attività. Non è consentito l'accesso e/o il trattamento di dati la cui conoscenza non sia necessaria per l'adempimento dei compiti assegnati. Gli archivi e le banche dati cui l'Autorizzato può accedere sono, esclusivamente, quelle utilizzate nella Struttura di appartenenza.

Con la sottoscrizione della presente lettera di autorizzazione, l'Autorizzato dichiara di aver preso visione dell'informativa ai sensi dell'Articolo 13 del RGPD (reperibile sul sito istituzionale di ASL AL), nonché puntuali indicazioni in merito all'ambito del Trattamento dei Dati Personali consentito, le istruzioni operative e le procedure recanti le modalità di Trattamento dei Dati Personali (ai sensi dell'articolo 29 del RGPD), nello specifico:

- Istruzioni generali per il Trattamento dei Dati;
- Istruzioni per l'uso degli strumenti informatici;
- Regole per una corretta tenuta delle postazioni di lavoro;
- Istruzioni sull'utilizzo della Posta Elettronica Ordinaria;
- Istruzioni su trattamento dei dati in ambito sanitario;
- Modello Organizzativo in materia di Protezione dei Dati Personali ("MOP") dell'Azienda Sanitaria Locale di Alessandria (reperibile sul sito istituzionale di ASL AL).

L'Autorizzato deve sempre attenersi alle norme del Reg. UE 2016/679 (Regolamento Generale sulla Protezione dei Dati), al Codice della privacy (D.lgs. 196/2003 e s.m.i.), ai provvedimenti del Garante, e alle istruzioni e misure di sicurezza comunicate dal Titolare e dal Direttore o dal Responsabile della Struttura presso la quale presta servizio (Designato), anche mediante Regolamenti interni.

L'Autorizzato si impegna a frequentare i corsi obbligatori di formazione e aggiornamento, organizzati dal Titolare, in materia di privacy e Protezione dei Dati Personali.

***

Istruzioni generali sul trattamento dei dati

1) L'Autorizzato è tenuto al rispetto e all'applicazione dei principi generali in ambito di data protection indicati dall'art. 5 del Regolamento Europeo n. 2016/679 "principi applicabili al trattamento di dati personali", quali:
   - ► i dati devono essere trattare i dati in modo lecito, corretto e trasparente nei confronti dell'Interessato (<<liceità, correttezza e trasparenza>>);
   - ► i dati devono essere raccolti per finalità determinate, esplicite e legittime e, successivamente, trattati in un modo che non sia incompatibile con tali finalità (<<limitazione delle finalità>>);

- i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (<<minimizzazione dei dati>>);
- i dati devono essere esatti e, se necessario, aggiornati (<< esattezza>>);
- i dati devono essere 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>>);
- i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (<< integrità e riservatezza>>).

2) L'Autorizzato dovrà rispettare le misure di sicurezza predisposte dal Titolare e/o dal Responsabile di Struttura.
3) L'Autorizzato dovrà garantire, in ogni operazione di trattamento, la massima riservatezza ed in particolare:
   - il divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare e/o del Responsabile di Struttura;
   - il divieto di effettuare colloqui con utenti o colleghi che contengono informazioni o dati personali, in presenza di persone non specificatamente autorizzate a conoscere tali informazioni;
   - la verifica, in caso di allontanamento dal posto di lavoro, che i dati trattati non siano accessibili a terzi non autorizzati (ad es. non lasciare incustoditi sopra la postazione di lavoro documenti contenenti dati personali, ricordarsi di bloccare la sessione di lavoro sul PC);
   - nel caso di fotocopie di documenti assicurarsi di non lasciare incustodite le copie nella macchina e ricordarsi di distruggere eventuali copie o stampe che non servono più prima di gettarle nel cestino;
   - al termine della giornata lavorativa è buona norma chiudere a chiave il proprio ufficio o, qualora ciò non sia possibile, è necessario riporre i documenti in cassetti o armadi che vanno chiusi a chiave;
   - il divieto di estrarre copie di documenti contenenti dati personali per uso personale, non collegato alle proprie mansioni lavorative.
4) L'Autorizzato deve conservare in luogo sicuro le proprie credenziali di autenticazione e non dovrà divulgarle a nessuno.
5) La raccolta dei dati, da parte dell'Autorizzato, deve essere preceduta dall'informativa e, se necessario, dal consenso dell'Interessato; se è necessario il consenso, deve essere raccolta la firma dell'Interessato.
6) L'Autorizzato deve rispettare il Regolamento Aziendale per l'utilizzo delle postazioni di lavoro e le indicazioni della Struttura ICT relative all'utilizzo di posta elettronica e internet.
7) L'Autorizzato dovrà rispettare il segreto d'ufficio e/o il segreto professionale. L'Autorizzato è tenuto alla riservatezza anche dopo la cessazione del rapporto di lavoro, o il trasferimento o l'assegnazione ad altre mansioni.

8) L'Autorizzato dovrà rispettare il divieto di fotografare utenti o colleghi nell'esercizio delle loro attività all'interno dell'Azienda.

***

Istruzioni sull'uso degli strumenti informatici

La gestione degli accessi agli strumenti informatici (server, applicativi, posta elettronica) deve avvenire attraverso l'utilizzo del proprio profilo di autorizzazione, composto da username (codice identificativo) e password (chiave riservata) o altri strumenti di autenticazione messi a disposizione dal Titolare del Trattamento.

1) È necessario che le credenziali di accesso:
   - non siano condivise con altri soggetti;
   - siano custodite con accuratezza e non rese facilmente visibili/accessibili (es. retrostante tastiera del pc, post-it posto sulla scrivania/monitor, etc.);
   - non vengano memorizzate automaticamente dal sistema per un accesso più rapido;
   - non siano riportate in elenchi su file elettronici memorizzati sul desktop oppure conservati in agende poste sulla scrivania;
   - abbiano una password che rispetti i requisiti di sicurezza e complessità, così come definiti dal Gruppo Sicurezza di cui al Modello Organizzativo ICT.
2) I supporti removibili (pen drive, hard disk esterni, cd, dvd, etc.) che permettono di copiare/archiviare files e documenti esternamente al PC, sono da considerarsi strumenti di lavoro e come tali essere utilizzati dagli operatori cui la struttura abbia assegnato gli stessi.
3) Alcune regole per la gestione ed utilizzo dei supporti removibili:
   - cautela per evitare che il contenuto sia trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
   - divieto di uso in luoghi diversi da quelli della sede di lavoro e conservazione in luoghi sicuri (cassettiere o armadi chiusi a chiave);
   - l'operatore, se ritiene necessario portare con sé lo strumento, dovrà ritenersi responsabile in caso di furto o perdita dello stesso e farne tempestiva comunicazione al Titolare.
4) Se la struttura ha messo a disposizione degli operatori telefoni cellulari, questi ultimi dovranno rispettare le seguenti regole:
   - non memorizzare immagini/video personali;
   - non riportare numeri di telefono di propri familiari o conoscenti;
   - usare smartphone criptati;
   - attivare blocco schermo temporizzato con PIN o altro sistema per sblocco;
   - non scaricare App per uso personale (social network, home banking, posta elettronica personale, acquisti);

- non effettuare backup automatici su Google, Whatsapp o sistemi similari;
- riversare su server dell'organizzazione video/immagini raccolti per fini lavorativi evitando di utilizzare Whatsapp, Dropbox o sistemi similari.

L'abuso o l'uso scorretto degli strumenti assegnati (computer, dispositivi portatili, posta elettronica, banche dati, collegamento ad Internet, credenziali di accesso, social network) costituiscono comportamenti contrari ai doveri di diligenza e fedeltà, punibili con sanzioni disciplinari e penali.

***

Regole per una corretta tenuta della postazione di lavoro

1) La postazione di lavoro è uno strumento da utilizzare secondo le regole della diligenza e della buona condotta e ciò rende ciascun operatore responsabile della sua corretta tenuta.
2) Ogni utilizzo non conforme può causare disservizi, costi di manutenzione, minacce di sicurezza, danni a persone o al patrimonio informativo del Titolare del Trattamento, da ciò ne deriva che ciascun utente è tenuto a rispettare la configurazione e gli strumenti applicativi messi a disposizione dall'organizzazione per lo svolgimento della propria mansione.
3) I documenti in lavorazione e le cartelle devono essere memorizzati in apposite aree di rete dedicate presenti sul server per evitare dispersioni o perdita di informazioni o accesso illecito agli stessi.
4) Non è permesso il salvataggio di file dell'organizzazione sulla memoria locale del PC, né in apposite cartelle locali, né sul desktop, per i quali non sono garantite operazioni di manutenzione, backup e ripristino dei dati, in caso di perdita.
5) Trattandosi di strumento di lavoro, non è consentito memorizzare sulla propria postazione documentazione personale (file, fotografie, video), installare dispositivi di comunicazione o memorizzazione (modem, masterizzatori) e scaricare software senza l'autorizzazione preventiva del Titolare del Trattamento o della Struttura ICT.
6) Al fine di evitare accessi illeciti a dati personali, l'utente è tenuto a:
   - adottare politiche dello "schermo pulito";
   - non lasciare incustodita la postazione con documentazione riservata visibile;
   - eseguire la procedura di logout dall'applicativo e/o dal sistema operativo tramite la funzione del blocca/disconnetti;
   - attivare screensaver il cui sblocco è reso possibile attraverso l'inserimento di password.

***

Istruzioni sull'utilizzo della posta elettronica ordinaria

1) La posta elettronica ordinaria, sia intestata all'Ufficio/Struttura, sia nominativa, è da considerarsi uno strumento di lavoro del Titolare del Trattamento.

2) Deve essere utilizzata solo per motivi strettamente connessi allo svolgimento dell'attività lavorativa.
3) Non deve essere considerata "privata" anche se recante il proprio nome e cognome.
4) Soggetti assegnatari di account di posta elettronica ordinaria sono responsabili del corretto utilizzo dello stesso e sono obbligati a rispettare anche i criteri definiti per l'accesso agli strumenti informatici.
5) È fatto divieto di utilizzare l'account messo a disposizione dal Titolare del Trattamento per:
   - trasmettere e ricevere documenti di natura personale;
   - fare re-inoltri dei messaggi su caselle di posta elettronica personale con dominio diverso da quello dell'organizzazione;
   - trasmettere documenti ufficiali dell'organizzazione recanti rilevanza giuridica verso terzi per cui è richiesto l'utilizzo della posta elettronica certificata istituzionale. Si rispettino, pertanto, le regole definite per una corretta gestione documentale informatica nelle more dei principi dettati dal Codice dell'Amministrazione Digitale (D.lgs. 82/2005 s.m.i.).
6) Per la trasmissione di documenti/dati/informazioni (es. bozze, documenti informali) contenenti categorie particolari di dati (es. dati idonei a rivelare lo stato di salute) è necessario utilizzare delle maggiori cautele, ovvero:
   - trasmettere i dati come allegato e non come testo nel corpo del messaggio;
   - cifrare i dati rendendo nota al destinatario la chiave crittografica tramite canali differenti da quelli utilizzati per la trasmissione stessa;
   - proteggere l'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi (es. password per l'apertura del file resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati);
7) In ambito sanitario la trasmissione di referti tramite posta elettronica è una pratica non corretta;
8) I messaggi di posta elettronica sono uno dei principali vettori di attacco ai sistemi informatici che rendono necessari accorgimenti particolari quali:
   - non aprire mail che risultano sospette;
   - diffidare da mail che, sebbene arrivate da indirizzi conosciuti, richiedono l'apertura di un allegato tramite l'inserimento di password o codici;
   - non procedure con l'avvio di codici eseguibili qualora la mail lo richieda.

***

Istruzioni sul trattamento di dati in ambito sanitario

Nel trattamento dei dati relativi alla salute delle persone, l'Autorizzato si attiene alle seguenti regole:

1) Dignità della persona

La prestazione medica e ogni operazione di Trattamento dei Dati Personali deve avvenire nel pieno rispetto della dignità dell'Interessato.

La tutela della dignità personale deve essere garantita nei confronti di tutti gli utenti dei servizi sanitari, con particolare riguardo ai soggetti più vulnerabili quali:

- disabili, fisici e psichici
- minori
- anziani
- pazienti sottoposti a trattamenti medici invasivi
- persone sieropositive
- donne che abbiano richiesto o effettuato l'interruzione volontaria della gravidanza
- persone offese da atti di violenza sessuale
- pazienti ricoverati nei reparti di rianimazione/terapia intensiva
- tossicodipendenti o persone affette da altre dipendenze (ad es. etilismo o ludopatia).

2) Trasparenza e informazione

In base alle norme vigenti (Reg. UE 2016/679, art. 9 par. 2 lett. h), non occorre il consenso dell'Interessato per finalità di diagnosi, terapia, cura ed assistenza sanitaria o sociale.

L'Autorizzato verifica che l'Interessato abbia ricevuto l'informativa sul trattamento dei dati relativi alla salute e che abbia firmato per presa visione il documento predisposto dal Titolare. Ove previsto, in luogo della firma per presa visione, l 'Autorizzato può annotare di aver fornito l'informativa nel documento (cartaceo o digitale) predisposto dal Titolare.

Laddove l'Interessato intenda esercitare un proprio diritto relativo al trattamento dei dati (es. richiesta di accesso o cancellazione di dati personali), l 'Autorizzato trasmette la richiesta al Referente Protezione Dati nominato dall'Azienda (email: privacy@aslal.it) o al Responsabile della Protezione dei Dati Personali (email: dpo@aslal.it).

3) Riservatezza nei colloqui e nelle prestazioni sanitarie

L'Autorizzato deve tutelare la riservatezza dei dati personali e della documentazione in suo possesso riguardante le persone, anche se affidata a codici o sistemi informatici.

L'Autorizzato non deve diffondere, attraverso la stampa o altri mezzi di informazione, notizie che possano consentire l'identificazione del paziente.

L'Autorizzato presta particolare attenzione alle modalità di svolgimento dei colloqui con gli utenti dei servizi sanitari ed assistenziali (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che le informazioni sulla salute dell'Interessato possano essere accidentalmente conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

È vietata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico.

L'Autorizzato cura che i documenti contenenti informazioni cliniche dell'Interessato non

siano resi visibili a terzi non legittimati (es. cartelle infermieristiche poste in prossimità del letto di degenza).

4) Informazioni sullo stato di ricovero o sulla salute di un paziente

L'Autorizzato si attiene alle eventuali indicazioni del paziente (se cosciente e capace) circa i soggetti che possono essere informati del ricovero, del reparto di degenza o dello stato di salute.

L'Autorizzato rispetta l'eventuale richiesta dell'Interessato di non comunicare tali informazioni neanche ai terzi legittimati.

Le informazioni da fornire ai terzi legittimati riguardano la sola presenza nel reparto; l'Autorizzato si assicura dell'identità della persona prima di fornire ogni informazione.

L'Autorizzato non comunica informazioni sullo stato di salute, salvo che l'Interessato abbia manifestato il proprio consenso. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere del paziente, il consenso può essere manifestato da parte di un altro soggetto legittimato.

5) Notizie su prestazioni di Pronto Soccorso

L'Autorizzato in servizio nel Pronto Soccorso, se ciò rientra nelle proprie mansioni, può dare notizia (o conferma), anche telefonica, dell'accesso di un paziente alla struttura ai soli soggetti legittimati: familiari, parenti o conviventi del paziente. L'Autorizzato si assicura dell'identità della persona prima di fornire ogni informazione.

L'Autorizzato di Pronto Soccorso, si limita, in tal caso, a comunicare che è in atto o si è svolta una prestazione e non fornisce informazioni sullo stato di salute.

L'Interessato - se cosciente e capace - deve essere preventivamente informato (ad es. in fase di accettazione) e posto in condizione di indicare i soggetti che possono essere informati della prestazione di Pronto Soccorso. L'Autorizzato rispetta eventuali indicazioni specifiche o contrarie del paziente.

6) Distanza di cortesia

L'Autorizzato verifica che siano rispettate le distanze di cortesia nelle operazioni di sportello, nell'acquisizione di informazioni sullo stato di salute e, in generale nelle operazioni di trattamento di dati sanitari.

7) Ordine di precedenza e di chiamata nelle sale di attesa (escluso Pronto Soccorso)

Al di fuori del reparto di Pronto Soccorso, nell'erogare prestazioni sanitarie, assistenziali o amministrative, che richiedono un periodo di attesa (ad es., analisi cliniche, visite ambulatoriali), l'Autorizzato rispetta le misure tecnico organizzative adottate dal Titolare per evitare la chiamata nominativa dei pazienti (ad es., uso di codici forniti all 'utente in fase di prenotazione o accettazione).

Se la chiamata nominativa risulta necessaria (ad es. in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), l'Autorizzato, ove possibile, cerca di instaurare un contatto diretto con il paziente per chiamarlo.

8) Consegna di documentazione sanitaria

Per la consegna di documentazione sanitaria (es. certificati, referti, copie di cartelle

cliniche) o di altra documentazione da cui si desuma lo stato di salute della persona (es. fatture, ricevute di prenotazione di prestazioni, etc.), l'Autorizzato si attiene alle istruzioni fornite dal Titolare e dal Direttore o Responsabile della Struttura (Designato).

In mancanza di diverse istruzioni, i documenti vengono consegnati solo in formato cartaceo ed in busta chiusa.

Tali documenti vengono consegnati al diretto Interessato o a terzi soggetti legittimati (es. genitori del minore) o muniti di delega scritta accompagnata dal documento d'identità.

9) Violazione dei Dati Personali

L'Autorizzato informa immediatamente il Direttore o Responsabile della Struttura (Designato) 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.

Senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, l'Autorizzato, ove non abbia provveduto il Direttore o Responsabile della Struttura (Designato), comunica la Violazione dei Dati Personali all'Ufficio Privacy (email: privacy@aslal.it) e al Responsabile della Protezione dei Dati Personali (email: dpo@aslal.it).

***

La presente nomina è da intendersi a tempo indeterminato sino alla revoca del Titolare del Trattamento dei Dati Personali o all'interruzione del rapporto di lavoro, salvo eventuali e/o diversi accordi tra le Parti.

L'attività di trattamento individuata nel presente atto sarà soggetta a revisione almeno annuale; da ciò discende la possibilità che, nel periodo intercorrente tra due revisioni, le attività di trattamento possano differire da quelle ivi indicate. In tali casi il soggetto destinatario della presente si riterrà comunque autorizzato allo svolgimento dei trattamenti derivanti dalle attività conferite sulla base di specifica disposizione organizzativa sviluppata nelle forme individuate dal Titolare del Trattamento. Le casistiche nelle quali i trattamenti dovranno considerarsi autorizzati pur in assenza di specifica indicazione nel presente atto sono le seguenti:

- impiego temporaneo di personale in attività generalmente non di competenza del medesimo per la gestione di urgenze;
- impiego temporaneo di personale in attività generalmente non di competenza del medesimo per esigenze organizzative non superiori ad un mese;
- impiego di personale in attività caratterizzata da "turnazione" degli addetti la quale comporti lo svolgimento di attività non di competenza dell'unità organizzativa a cui è assegnato il soggetto.

***

L'Autorizzato al Trattamento dichiara di aver ricevuto le istruzioni, di averne presa visione e di impegnarsi ad adottare tutte le misure necessarie alla loro attuazione.

Data Firma

(Cognome Nome dell'Autorizzato)

Allegato 5: Modulo di segnalazione Data Breach

MODULO PER LA SEGNALAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI

DATA BREACH

All'UFFICIO PRIVACY ASL AL

privacy@aslal.it

aslal@pec.aslal.it

Il/La sottoscritto/a ……,

□ Direttore S.C. / Responsabile S.S.A/S.S.D. ……..,

□ Altro (specificare) ……..,

segnala quanto segue.

1. **Tipologia di violazione**

   A. VIOLAZIONE DELLA RISERVATEZZA

   (diffusione di dati, accesso non autorizzato)

   B. VIOLAZIONE DELL'INTEGRITA'

   (modifica di dati non autorizzata)

   C. VIOLAZIONE DELLA DISPONIBILITA'

   (impossibilità di accesso ai dati, perdita, distruzione non autorizzata)

2. **Struttura/e coinvolta/e**

   ……

3. **Quando si è verificato l'evento (data ed ora)**

   ……

4. **Quando si è venuti a conoscenza della violazione (data ed ora)**

   ……

5. **Descrizione dettagliata dell'evento (Natura e descrizione)**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. **Categoria di dati personali oggetto di violazione (precisare se i dati determinano l'immediata identificabilità dell'Interessato, se trattasi di dati in grado di rivelare patologie e/o aspetti della personalità che possono comportare discriminazioni o danneggiare gravemente la dignità o la reputazione dell'Interessato).**

.....

.....

.....

.....

.....

.....

7. **Volume / numero di dati personali oggetto di violazione**

.....

.....

.....

.....

.....

.....

8. **Numero e tipologia di soggetti che hanno ricevuto e visionato i dati oggetto di violazione**

   .....

   .....

   .....

9. **Possibili conseguenze dannose per l'Interessato (danni fisici, materiali, immateriali)**

   .....

   .....

   .....

   .....

   .....

   .....

10. **Sistemi di elaborazione e/o memorizzazione e loro ubicazione (se nota)**

    .....

    .....

    .....

11. **Eventuale Responsabile/i Esterno/i del Trattamento coinvolto/i**

    .....

    .....

    .....

12. **Misure tecniche ed organizzative adottate nell'immediato per porre rimedio alla violazione e ridurre gli effetti negativi sugli Interessati**

    .....

    .....

    .....

    .....

    .....

    .....

13. **Eventuali proposte per la mitigazione della presunta violazione**

.....

.....

.....

14. **Elementi / circostanze che si ritiene utili indicare**

.....

.....

.....

.....

.....

.....

15. **Esito della autovalutazione mediante il tool messo a disposizione da parte del Garante:**

.....

.....

.....

Firma leggibile

_____

Allegato 6: Modello Unico per l'esercizio dei diritti dell'Interessato

MODELLO UNICO PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO
(ai sensi del Regolamento UE 2016/679 – GDPR)

Spett.le [Nome del Titolare del Trattamento]
ASL AL
aslal@pec.aslal.it

Dati dell'Interessato

- Nome e Cognome: _____
- Data di nascita: _____
- Luogo di nascita: _____
- Indirizzo di residenza: _____
- Telefono: _____
- Email: _____

Con riferimento al trattamento dei miei dati personali, chiedo di esercitare i seguenti diritti, previsti dal Regolamento (UE) 2016/679:

☐ Diritto di accesso (art. 15 GDPR):
Esistenza di un trattamento che riguarda il soggetto istante.

☐ Diritto di rettifica (art. 16 GDPR):
Rettifica dei miei dati personali inesatti/incomplete di cui al riquadro A.

☐ Diritto alla cancellazione (oblio) (art. 17 GDPR):
Cancellazione/Oscuramento dei miei dati personali di cui al riquadro A.

☐ Diritto alla limitazione del trattamento (art. 18 GDPR):
Richiedo che il trattamento dei miei dati sia limitato nei termini di cui al riquadro A.

☐ Diritto alla portabilità dei dati (art. 20 GDPR):
Richiesta dei miei dati personali in formato strutturato come dettagliato al riquadro A.

☐ Diritto di opposizione (art. 21 GDPR):
Opposizione al trattamento dei miei dati personali come dettagliato al riquadro A.

☐ Diritto a non essere sottoposto a processi decisionali automatizzati (art. 22 GDPR): Opposizione a decisioni basate unicamente su trattamenti automatizzati.

Dettaglio dell'istanza:

.....

.....

.....

.....

.....

.....

.....

.....

Riquadro A

Documenti allegati:

☐ Copia documento di identità (*non necessaria se l'istanza è firmata digitalmente dall'istante e/o trasmessa da casella di posta elettronica certificata di cui è il titolare*)

☐ Altro (*dettagliare*): _____

Luogo e data: _____

Firma: _____