

Sistema Socio Sanitario



Regione  
Lombardia

ATS Brescia

*Agenzia di Tutela della Salute di Brescia*

*Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia*

Tel. 030.38381 Fax 030.3838233 - [www.ats-brescia.it](http://www.ats-brescia.it)

Posta certificata: [protocollo@pec.ats-brescia.it](mailto:protocollo@pec.ats-brescia.it)

Codice Fiscale e Partita IVA: 03775430980

DECRETO n. 239

del 30/04/2025

Cl.: 1.1.02

OGGETTO: Gestione adempimenti in materia di protezione dei dati personali. Approvazione del Regolamento sul "Modello organizzativo privacy" ("MOP"): aggiornamento delle policy, dei ruoli e dei sistemi di responsabilità ai sensi del Regolamento (UE) 27 aprile 2016, n. 2016/679.

**II DIRETTORE GENERALE – Dott. Claudio Vito Sileo  
nominato con D.G.R. XII/1645 del 21.12.2023**

Acquisiti i **pareri** del  
DIRETTORE SANITARIO F.F.  
del  
DIRETTORE SOCIOSANITARIO  
e del  
DIRETTORE AMMINISTRATIVO

Dott. Luca Maria Bassoli

Dott.ssa Franco Milani

Dott.ssa Sara Cagliani



---

IL DIRETTORE GENERALE

Richiamato il Decreto D.G. n. 511 del 12/10/2018 con il quale sono state assunte le determinazioni in ordine al "Modello Organizzativo privacy dell'Agenzia di Tutela della Salute di Brescia" in attuazione del Regolamento UE 2016/679;

Valutato che il Decreto D.G. n. 109 del 25/02/2021, in ragione delle disposizioni normative medio tempore introdotte (fra le altre, il D.Lgs. n. 101/2018) e delle modifiche intervenute all'interno di ATS Brescia (fra le altre, il "turn over" del Responsabile della Protezione dei Dati Personali, di seguito anche "DPO"), aveva apportato alcuni correttivi al modello originario al fine di meglio allineare le previsioni ed i compiti delle figure soggettive coinvolte nell'attuazione del Regolamento UE 2016/679 ai contenuti della stessa normativa comunitaria, nonché di quella nazionale;

Considerato che, in conseguenza della maturazione della nuova scadenza del servizio di Responsabile della Protezione dei Dati Personali, ATS Brescia ha indetto apposita procedura di gara, a conclusione della quale, con Determina n. 257 del 23/07/2024, è stato affidato il servizio di DPO, per un periodo di 36 mesi, dal 24/07/2024 al 23/07/2027, alla ditta LTA Srl;

Atteso che l'esperienza maturata nel corso degli anni, congiuntamente con l'acquisizione di maggiori competenze e conoscenze in materia di protezione dei dati personali, grazie anche al supporto fornito all'Agenzia da parte dei DPO che si sono susseguiti, rendono ATS Brescia consapevole che la materia della privacy meriti una sempre più puntuale e approfondita considerazione;

Rilevato che, a tale riguardo, il nuovo DPO ha suggerito l'aggiornamento del Modello Organizzativo Privacy al fine di renderlo ancora più *compliance* alla normativa, prima fra tutti, comunitaria;

Condivisa, l'opportunità di apportare le innovazioni suggerite al Modello Organizzativo Privacy (di seguito anche "MOP") a fronte, altresì, degli approfondimenti condotti dal Tavolo Tecnico Privacy di ATS Brescia (aggiornato nella sua composizione con Decreto D.G. n. 288 del 17/05/2022);

Rilevato che al fine di agevolare la circolazione e fruibilità dei contenuti del nuovo MOP, lo stesso assumerà la forma di un Regolamento aziendale;

Precisato che le disposizioni del nuovo decretando Regolamento dovranno intendersi come efficaci e vincolanti a decorrere dalla approvazione del presente Decreto e con efficacia *ex nunc*;

Atteso che, pertanto, le nomine delle figure privacy dell'Agenzia ad oggi formalizzate rimangono valide e non dovranno essere aggiornate, mentre le nuove procedure ed i nuovi modelli dovranno essere rispettati ed utilizzati in relazione alle nuove nomine da assegnare e formalizzare a decorrere dall'approvazione del presente Decreto;

Vista la proposta presentata dal Direttore f.f. della SC Pianificazione e Controllo, Ing. Ivan Campa, che anche in qualità di Responsabile del procedimento, attesta la regolarità tecnica del presente provvedimento;

Dato atto che dal presente provvedimento non discendono oneri per l'Agenzia;

Acquisiti i pareri del Direttore Sanitario f.f., Dott. Luca Maria Bassoli, del Direttore Sociosanitario, Dott. Franco Milani e del Direttore Amministrativo, Dott.ssa Sara Cagliani che attesta, altresì, la legittimità del presente atto;

D E C R E T A

- a) di approvare per le motivazioni di cui in premessa, il Regolamento sul Modello Organizzativo in materia di Protezione dei Dati Personali dell'ATS di Brescia che



- viene allegato, quale parte integrante e sostanziale, al presente provvedimento (Allegato "A" composto da n. 16 pagine);
- b) di approvare altresì i modelli di nomina, che si allegano al Regolamento e che parimenti ad esso costituiscono parte integrante e sostanziale, al presente provvedimento e precisamente:
- Allegato 1 "Nomina a Delegato al trattamento dei dati personali" (composto da n. 4 pagine);
  - Allegato 2 "Nomina Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE/679/2016 sulla protezione dei dati e la loro libera circolazione" (composto da n. 5 pagine);
  - Allegato 3 "Nomina Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE/679/2016 e nomina ad Amministratore di Sistema "esterno" ai sensi e per gli effetti del Provvedimento a carattere generale dell'Autorità Garante per la Protezione dei Dati Personali del 27 Novembre 2008 e ss.mm.ii." (composto da n. 9 pagine);
  - Allegato 4 "Nomina Autorizzato al trattamento dei dati personali" (composto da n. 2 pagine);
  - Allegato 5 "Nomina dell'Amministratore di Sistema "interno"" (composto da n. 4 pagine);
- c) di disporre che il presente Regolamento sostituisce, con decorrenza dalla data di adozione del presente atto, il precedente "Modello organizzativo privacy dell'Agenzia di Tutela della Salute di Brescia" assunto con Decreto D.G. n. 109 del 25/02/2021;
- d) di demandare alla Funzione di gestione adempimenti in materia di protezione dei dati personali la diffusione del presente provvedimento a tutte le Strutture dell'Agenzia e di ogni eventuale indicazione operativa ritenuta necessaria;
- e) di pubblicare a cura della Funzione di gestione delle relazioni interne ed esterne il presente provvedimento nella sezione Privacy del sito web istituzionale, nonché nella sezione dedicata della Intranet aziendale;
- f) di dare atto che dal presente provvedimento non discendono oneri per l'Agenzia;
- g) di dare atto che il presente provvedimento è sottoposto al controllo del Collegio Sindacale, in conformità ai contenuti dell'art. 3-ter del D.Lgs. n. 502/1992 e ss.mm.ii. e dell'art. 12, comma 14, della L.R. n. 33/2009;
- h) di disporre, a cura della SC Affari Generali e Legali, la pubblicazione all'Albo online - sezione Pubblicità legale - ai sensi dell'art. 17, comma 6, della L.R. n. 33/2009, e dell'art. 32 della L. n. 69/2009, ed in conformità alle disposizioni ed ai provvedimenti nazionali e comunitari in materia di protezione dei dati personali.

Firmato digitalmente dal Direttore Generale  
Dott. Claudio Vito Sileo



## **REGOLAMENTO**

---

REGOLAMENTO SUL MODELLO  
ORGANIZZATIVO IN MATERIA DI  
PROTEZIONE DEI DATI PERSONALI  
DELL'ATS BRESCIA

---



## Sommario

ART. 1 - OGGETTO.....	3
ART. 2 - DEFINIZIONI.....	3
ART. 3 - PRESUPPOSTI DI LICEITÀ DEL TRATTAMENTO.....	5
ART- 4 - TITOLARE DEL TRATTAMENTO DEI DATI.....	5
ART. 5 - DATA PROTECTION OFFICER (DPO) O RESPONSABILE DELLA PROTEZIONE DATI (RPD).....	6
ART. 6 - DELEGATI AL TRATTAMENTO DEI DATI PERSONALI .....	7
ART. 7 - TAVOLO TECNICO PRIVACY .....	9
ART. 8 - RESPONSABILE DEL TRATTAMENTO DEI DATI .....	10
ART. 9 - REFERENTE PER LA CYBERSICUREZZA .....	10
ART. 10 - AUTORIZZATI AL TRATTAMENTO DEI DATI .....	10
ART. 11 - AMMINISTRATORI DI SISTEMA .....	11
ART. 12 - SICUREZZA DEL TRATTAMENTO DEI DATI.....	11
ART. 13 - REGISTRO DEL TITOLARE DEL TRATTAMENTO DEI DATI .....	11
ART. 14 - REGISTRO DEL RESPONSABILE DEL TRATTAMENTO DEI DATI .....	12
ART. 15 - VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI .....	12
ART. 16 - RINVIO .....	13



## CAPO I – DISPOSIZIONI GENERALI

### ART. 1 - OGGETTO

Il presente Regolamento sul Modello Organizzativo in materia di Protezione dati personali (MOP o anche solo "Regolamento") disciplina l'assetto di *governance* e le disposizioni procedurali per l'adeguamento dell'Agenzia di Tutela della Salute di Brescia ("ATS Brescia") al Regolamento Generale Protezione Dati UE del 27 aprile 2016 n. 679 ("GDPR"<sup>1</sup>) ed al D. Lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali" o "Codice Privacy") e successive modifiche ed integrazioni.

### ART. 2 - DEFINIZIONI

Ai fini del presente Regolamento<sup>2</sup> si intende per:

**GDPR:** Regolamento Generale Protezione Dati Personali e la loro libera circolazione UE/679/2016 o General Data Protection Regulation (GDPR);

**Codice privacy:** "Codice in materia di protezione dei dati personali", D.Lgs. n. 196 del 30 giugno 2003 e successive modifiche ed integrazioni;

**Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. (Art. 4 Regolamento 679/2016/UE).

**Dati particolari:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici (i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione – Art. 4 Regolamento 679/2016/UE), dati biometrici (i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici – Art. 4 Regolamento 679/2016/UE) intesi a identificare in modo univoco una persona fisica, dati relativi alla salute (i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute – Art. 4 Regolamento 679/2016/UE) o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 Regolamento 679/2016/UE).

<sup>1</sup> Come presente sul sito del Garante Privacy.

<sup>2</sup> Si tengono in considerazione le definizioni di cui all'art. 4 del GDPR.



**Dati giudiziari:** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (Art. 10 Regolamento 679/2016/UE).

**Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. (Art. 4 Regolamento 679/2016/UE).

**Titolare del trattamento dei dati personali 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 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;

**Delegato al trattamento dei dati personali:** la persona fisica (Dirigenti titolari di Struttura Semplice, di Struttura Semplice Dipartimentale e di Struttura Complessa, Direttori di Dipartimento e Direttori della Direzione Strategica per i rispettivi ambiti di competenza) espressamente designata che opera sotto l'autorità di ATS (che agisce in qualità di Titolare o di Responsabile del trattamento) nell'ambito del proprio assetto organizzativo, con specifici compiti e funzioni atti a porre in essere misure tecniche e organizzative volte a garantire che i trattamenti siano effettuati in conformità al GDPR;

**Autorizzato al trattamento dei dati personali:** la persona fisica (dipendenti, personale somministrato, tirocinanti, borsisti, volontari, titolari di incarico gratuito, titolari di incarichi libero professionali, studenti dei Corsi di Laurea, Collegio Sindacale, Nucleo di Valutazione delle Prestazioni, Ufficio di Pubblica Tutela e Consigliere di Fiducia, che agiscono senza mezzi propri – personal computer e altre applicazioni di ATS - nello svolgimento dell'attività presso le sedi di ATS) che tratta dati personali, effettuando materialmente le operazioni di trattamento sui dati personali sotto la diretta autorità dei Delegati e previa nomina da parte di questi;

**Referente per la Cybersicurezza:** il soggetto di comprovate professionalità e competenze in materia di Cybersicurezza individuato dal Titolare del trattamento cui competono le funzioni di cui all'art. 8 della Legge n. 90 del 28/06/2024 e che opera presso la Struttura che provvede agli adempimenti di cui allo stesso art. 8, comma 1 della Legge 90/2024 parimenti individuata dal Titolare del trattamento;

**Responsabile del trattamento dei dati personali:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

**Amministratori di Sistema:** le figure previste dal Provvedimento del Garante del 27/11/2008, autorizzate al trattamento di dati personali per la gestione dei sistemi informativi/informatici o responsabili nominate all'uopo dal Titolare;



**RPD/DPO:** Responsabile Protezione Dati personali o Data Protection Officer;

**Tavolo Tecnico Privacy:** gruppo di lavoro tecnico composto da più membri identificati all'interno di ATS, nominati dal Titolare del trattamento, con funzioni di gestione degli adempimenti in materia di protezione dei dati personali;

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

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

**Garante Privacy:** l'autorità di controllo pubblica istituita dallo Stato Italiano; nello specifico, l'Autorità Garante per la Protezione dei Dati Personali;

---

### ART. 3 - PRESUPPOSTI DI LICEITÀ DEL TRATTAMENTO

---

1. Ai sensi di quanto previsto dal GDPR ogni trattamento deve trovare fondamento in un'ideale base giuridica.
2. I trattamenti di dati personali sono effettuati da ATS sulla base dei presupposti di liceità indicati nel GDPR all'art. 6 (rubricato "Liceità del trattamento") e all'art. 9 (rubricato "Trattamento di categorie particolari di dati personali") e, di volta in volta, devono essere individuati al fine di rendere tali trattamenti legittimi.

## CAPO II – MODELLO ORGANIZZATIVO

---

### ART- 4 - TITOLARE DEL TRATTAMENTO DEI DATI

---

1. ATS, rappresentata, ai fini previsti dal GDPR, dal Direttore Generale, è il Titolare del trattamento dei dati personali (d'ora in poi anche solo "Titolare") raccolti anche in banche dati, digitali o cartacee.
2. 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.
3. 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 modo conforme al GDPR. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati, per 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.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio, mediante analisi della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'applicazione, del contesto e delle finalità del



trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

5. Il Titolare provvede a:

- a) nominare il Data Protection Officer o Responsabile Protezione Dati (d'ora in poi anche solo "DPO" o "RPD");
- b) nominare i Delegati al trattamento dei dati personali (nelle persone dei Dirigenti titolari di Struttura Semplice, di Struttura Semplice Dipartimentale e di Struttura Complessa, Direttori di Dipartimento e Direttori della Direzione Strategica per i rispettivi ambiti di competenza), ai sensi del successivo art. 6 del presente Regolamento, quali soggetti preposti al trattamento dei dati personali contenuti nelle banche dati di competenza delle articolazioni organizzative cui sono preposti, nonché quali soggetti responsabili della predisposizione di interventi programmatici, di coordinamento, di supervisione nonché operativi relativi alle attività di trattamento dei dati personali svolti nell'ambito della Struttura/Direzione di competenza;
- c) assegnare distinti compiti a specifiche Strutture, in ragione delle peculiari competenze alle medesime attribuite, al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento della ATS al GDPR;
- d) nominare i membri del Tavolo Tecnico Privacy e definire gli indirizzi per l'attribuzione di specifiche competenze al Tavolo Tecnico Privacy, come meglio precisato al successivo art. 7, a supporto del DPO, anche con riguardo alla funzione di raccordo e di collaborazione con il Garante Privacy, al fine di supportare l'attività del DPO nel rapporto con le Strutture di ATS e fornire a queste ultime le necessarie indicazioni in materia di protezione dati personali sui trattamenti sviluppati dalle stesse;
- e) individuare la Struttura ed il referente ai sensi e per gli effetti di cui all'art. 8 della Legge n. 90 del 28/06/2024 (legge cybersicurezza).

6. Il Titolare è 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 a ATS da enti ed organismi statali o regionali, allorché due o più Titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.

7. ATS 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 sia di Responsabile del trattamento.

---

## **ART. 5 - DATA PROTECTION OFFICER (DPO) O RESPONSABILE DELLA PROTEZIONE DATI (RPD)**

---

1. Il Data Protection Officer o Responsabile della Protezione Dati è individuato nella figura di una persona fisica o giuridica selezionata nel rispetto delle prescrizioni recate dal Codice degli appalti in materia di contratti di servizio. Il soggetto deve possedere i requisiti specificati dagli artt. 37 e 38 del GDPR. I dati di contatto del DPO/RPD sono reperibili sul sito istituzionale della ATS nella sezione Privacy, nonché nelle informative messe a disposizione degli interessati.

2. Il DPO è incaricato dei seguenti compiti:



- a) informare e fornire consulenza ad ATS, nonché ai dipendenti che eseguono il trattamento per il tramite del Tavolo tecnico privacy, in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati personali;
- b) fungere da supporto alle Strutture competenti sulle richieste di accesso per tutti gli aspetti relativi alla protezione dei dati personali ai sensi del GDPR;
- c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- d) rendere una consulenza idonea, scritta od orale, anche nell'individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati;
- e) cooperare con il Garante Privacy 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;
- f) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati personali, ferme restando le responsabilità di ATS. 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 di ATS;
- g) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere da ATS;

il tutto a condizione che ATS 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.

3. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio di ATS. ATS fornisce al DPO le risorse necessarie per assolvere ai compiti attribuiti e per accedere ai dati personali ed ai trattamenti posti in essere.

In particolare, al DPO sono assicurati:

- il supporto attivo per lo svolgimento dei compiti da parte dei Delegati al trattamento dei dati personali, del Tavolo Tecnico Privacy;
- le risorse infrastrutturali e di funzionamento (sede, attrezzature, strumentazione), nonché di personale, attraverso la collaborazione del Tavolo Tecnico Privacy;
- l'accesso alle articolazioni funzionali di ATS per fornire il supporto, le informazioni e gli *input* essenziali.

4. 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 ad ATS. 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 ad ATS.

---

## **ART. 6 - DELEGATI AL TRATTAMENTO DEI DATI PERSONALI**

---

1. Il Titolare individua e nomina i Dirigenti titolari di Struttura Semplice, di Struttura Semplice Dipartimentale e di Struttura Complessa, Direttori di Dipartimento e Direttori della Direzione Strategica per i rispettivi ambiti di competenza, quali Delegati al trattamento dei dati personali



relativamente ai trattamenti effettuati dalla Struttura/Direzione di competenza, utilizzando l'atto di nomina allegato al presente Regolamento (Allegato 1). Ciascun Delegato 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 volte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. L'atto di nomina, indica gli specifici ambiti di attività cui i singoli Delegati al trattamento sono preposti.
3. L'atto di nomina a Delegato al trattamento dei dati personali, con riguardo al personale dipendente, viene predisposto dalla SC Gestione e Sviluppo delle Risorse Umane, inserito nel fascicolo personale e condiviso con la Struttura di afferenza (ad eccezione delle nomine dei Direttori della Direzione Strategica predisposte a cura della SC Affari Generali e Legali).  
In caso di modifica dell'incarico deve essere eventualmente rinnovato l'atto di nomina con le predette modalità. Sul punto si rimanda allo Schema in calce al presente Regolamento.
4. Ai Delegati al trattamento dei dati personali sono attribuiti i seguenti compiti:
  - a) collaborare con il Titolare nell'identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività di ATS;
  - b) collaborare con il Titolare nel predisporre ed aggiornare il registro delle attività di trattamento, procedendo alla comunicazione delle modifiche intervenute ai trattamenti di competenza al Tavolo Tecnico Privacy, al fine di aggiornare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura, nonché il registro dei trattamenti;
  - c) collaborare con il Titolare nel definire, per ciascun trattamento di dati personali, la durata del trattamento, l'archiviazione e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
  - d) collaborare con il Titolare nel condurre ogni valutazione atta a verificare la necessità dell'effettuazione della valutazione d'impatto sui trattamenti di competenza;
  - e) collaborare con il Titolare nella predisposizione delle informative relative alle competenze della Struttura e provvedere a che siano rese disponibili ai soggetti interessati;
  - f) disporre l'attuazione dei provvedimenti emessi dal Garante Privacy sulla scorta delle indicazioni del Titolare;
  - g) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
  - h) individuare, tra gli operatori assegnati alla Struttura o ai collaboratori/professionisti alla stessa afferenti, designandoli per iscritto, gli Autorizzati al trattamento e adoperarsi al fine di rendere effettive le istruzioni cui devono attenersi gli stessi, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati - anche presenti nelle banche dati e sulle piattaforme informatiche disponibili - nonché l'osservanza da parte degli stessi, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
  - i) gestire ogni adempimento istruttorio finalizzato alla formalizzazione della nomina di un Responsabile del trattamento dei dati personali o della nomina di ATS a Responsabile del trattamento dei dati personali;
  - j) per l'istruttoria che precede, lett. i), coordinarsi con la S.C. Sistemi Informativi con riferimento alle necessarie valutazioni ed identificazioni (che confluiranno nel relativo atto di nomina) rispetto all'eventuale ruolo di Amministratore di sistema assunto dal Responsabile del trattamento dei dati personali o assunto da ATS quale Responsabile del trattamento dei dati personali;



- k) far osservare gli adempimenti previsti in caso di nuovi trattamenti e archiviazione di trattamenti;
  - l) individuare il personale della propria Struttura organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
  - m) adottare, con il supporto del Tavolo Tecnico Privacy e della S.C. Sistemi Informativi aziendali soluzioni di privacy "by design e by default", ovvero di protezione dei dati personali 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, riducendo al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
  - n) collaborare con il Titolare nel definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti al trattamento dei dati e assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
  - o) attenersi alle previsioni previste dal Titolare in ordine alle procedure di "data breach" ed a quelle relative all'esercizio dei diritti da parte degli interessati.
5. 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.
6. Gli atti di nomina dei Delegati al trattamento dei dati personali si intendono pienamente validi ed efficaci anche relativamente ai trattamenti di dati che ATS effettuerà nelle qualità e ruolo di Responsabile del trattamento dei dati ex art. 28 GDPR.

## ART. 7 - TAVOLO TECNICO PRIVACY

1. Il Tavolo Tecnico Privacy è istituito dal Titolare, che ne nomina i componenti e ne individua il Coordinatore, ed è incaricato della generale gestione degli adempimenti in materia di protezione dei dati personali.
2. I compiti di supporto affidati al Tavolo Tecnico Privacy riguardano:
  - a) assolvimento di ogni adempimento imposto dalla normativa in materia di protezione dei dati personali (compresa la gestione dei "data breach") con la collaborazione delle Strutture dell'amministrazione di volta in volta interessate, al fine di garantire adeguata sicurezza e protezione al trattamento dei dati personali;
  - b) attivazione di un costante monitoraggio del trattamento dati, predisposizione e aggiornamento delle procedure e dei Regolamenti;
  - c) predisposizione della necessaria modulistica con definizione delle modalità di utilizzo;
  - d) segnalazione a tutte le Strutture di ATS di novità, informative, indicazioni, prescrizioni e interpretazioni del Garante Privacy, nonché di pronunce giurisdizionali inerenti agli aspetti del trattamento dei dati personali;
  - e) formazione degli operatori di ATS, anche mediante l'elaborazione di piani e documenti prescritti dalle vigenti disposizioni normative, tenuto conto anche delle proposte dei Delegati al trattamento;
  - f) gestione della sezione "Privacy" del sito dell'ATS e della corrispondente sezione della intranet;
  - g) espressione di pareri ed interpretazioni in ordine ai quesiti in materia di privacy;
  - h) formulazione di richieste di pareri ai competenti uffici regionali, al Garante privacy e altre eventuali autorità;
  - i) gestione dei rapporti con il DPO di ATS per ogni ambito di sua competenza;
  - j) attivazione e gestione dei rapporti con le ASST del territorio, con altri Enti/Istituzioni al fine di condividere soluzioni operative ed organizzative per ambiti di comune interesse.



---

**ART. 8 - RESPONSABILE DEL TRATTAMENTO DEI DATI**

---

1. Il Responsabile del trattamento è il soggetto, pubblico o privato, che tratta dati personali, anche particolari, 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 del trattamento ai sensi dell'art. 28 del GDPR. La formalizzazione di detto ruolo avviene mediante atto giuridico avente natura negoziale bilaterale redatto in forma scritta da parte del Titolare.

La Struttura competente al trattamento per il quale è necessaria la nomina di un Responsabile predispone l'atto di nomina nel rispetto del modello allegato (Allegati 2 e 3 se anche Amministratore di Sistema per il quale si rinvia all'art. 11), lo sottopone al preventivo nulla osta del Tavolo Tecnico Privacy rappresentandone ogni modifica proposta anche dal soggetto nominando, con successivo inoltro al Titolare per acquisizione della sottoscrizione. Sul punto si rimanda allo Schema in calce al presente Regolamento.

Ad avvenuta sottoscrizione delle Parti (Titolare e Responsabile ed eventuali sub-responsabili), la Struttura competente procede a repertoriare l'atto nel sistema documentale in uso e lo condivide con il Tavolo Tecnico Privacy per la tenuta del Registro di cui all'art. 14 del presente Regolamento.

2. Il rapporto tra il Titolare ed il Responsabile è disciplinato dall'atto giuridico di cui al comma 1 del presente articolo, nel quale si specificano la finalità perseguita, la tipologia dei dati, la categoria degli Interessati, la durata del trattamento, gli obblighi e i diritti del Responsabile del trattamento e le modalità di trattamento. Tale atto può anche basarsi su clausole contrattuali tipo adottate dal Garante Privacy oppure dalla Commissione Europea.
3. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa ed ai compiti affidatigli con l'atto di nomina.

---

**ART. 9 - REFERENTE PER LA CYBERSICUREZZA**

---

Il Referente per la Cybersicurezza è il soggetto di comprovate professionalità e competenze in materia di Cybersicurezza individuato dal Titolare del trattamento cui competono le funzioni di cui all'art. 8 della Legge n. 90 del 28/06/2024 e che opera presso la Struttura che provvede agli adempimenti di cui allo stesso art. 8, comma 1 della Legge 90/2024 parimenti individuata dal Titolare del trattamento.

---

**ART. 10 - AUTORIZZATI AL TRATTAMENTO DEI DATI**

---

1. Il Titolare o i Delegati al trattamento dei dati personali individuano, nell'ambito della propria responsabilità, gli Autorizzati al trattamento quali persone ammesse a compiere operazioni sui dati personali.
2. Nella lettera di nomina, il cui modello è allegato al presente Regolamento (Allegato 4) vengono indicati per ciascun Autorizzato, gli ambiti di attività e/o l'elenco dei trattamenti di dati personali di competenza.
3. L'atto di nomina ad Autorizzato al trattamento relativo al personale dipendente viene registrato nel sistema di gestione documentale, condiviso con l'autorizzato, la Struttura di afferenza e la SC Gestione e Sviluppo delle Risorse Umane per inserimento nel fascicolo personale.



In caso di modifica di assegnazione dell'autorizzato deve essere predisposto nuovo atto di nomina nel rispetto dell'iter di cui sopra.

4. Per gli atti di nomina ad Autorizzati al trattamento diversi dal personale dipendente si rimanda allo Schema in calce al presente Regolamento.

---

#### **ART. 11 - AMMINISTRATORI DI SISTEMA**

---

1. Il Titolare provvede alla nomina degli Amministratori di sistema interni.
2. Il Titolare provvede, altresì, alla nomina degli Amministratori di Sistema esterni in concomitanza con la nomina a Responsabile nelle forme di cui all'art. 8 del presente Regolamento utilizzando il modello allegato (Allegato 3). Sul punto si rimanda anche allo Schema in calce al presente Regolamento.

---

### **CAPO III – SICUREZZA E PROTEZIONE DEI DATI**

---

#### **ART. 12 - SICUREZZA DEL TRATTAMENTO DEI DATI**

---

1. Il Titolare del trattamento e tutti i soggetti aventi i ruoli descritti al Capo II del presente Regolamento mettono in atto, per i distinti profili di responsabilità e di azione, misure tecniche ed organizzative per 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 del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre e a titolo esemplificativo e non esaustivo: 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.
2. 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.
3. ATS, attraverso i ruoli individuati nel presente Regolamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbiano accesso a dati personali.
4. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati particolari (ex sensibili) per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi adottati ai sensi del D. Lgs. 196/2003 nella versione antecedente alle modifiche apportate dal D. Lgs. 101/2018.

---

#### **ART. 13 - REGISTRO DEL TITOLARE DEL TRATTAMENTO DEI DATI**

---

1. Il Registro delle attività di trattamento svolte da ATS in qualità di Titolare reca almeno le seguenti informazioni, come previsto dall'art. 30, par. 1, del GDPR:
  - a) il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento e del Data Protection Officer (DPO);
  - b) le finalità del trattamento;



- c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
  - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  - e) l'eventuale trasferimento di dati personali verso un Paese terzo od un'organizzazione internazionale;
  - f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è conservato nel sistema di gestione documentale ed è pubblicato nella Sezione privacy del sito web.

---

#### **ART. 14 - REGISTRO DEL RESPONSABILE DEL TRATTAMENTO DEI DATI**

---

1. Il Registro delle attività di trattamento svolte da ATS in qualità di Responsabile del trattamento contiene almeno le seguenti informazioni, come previsto dall'art. 30, par. 2, del GDPR:
  - a) il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce ATS, del Rappresentante del Titolare del trattamento o del Responsabile del trattamento e ove applicabile, del relativo DPO;
  - b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
  - c) l'eventuale trasferimento di dati personali verso un Paese terzo od un'organizzazione internazionale;
  - d) il richiamo, ove possibile, alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è conservato nel sistema di gestione documentale.

---

#### **ART. 15 - VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI**

---

1. Il Titolare, prima di effettuare il trattamento, deve attuare 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, presenta un rischio elevato per i diritti e le libertà delle persone fisiche.
2. 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.
3. La DPIA non è necessaria nei casi seguenti:
  - a) se il trattamento non presenta un rischio elevato per i diritti e le libertà delle persone fisiche;
  - b) 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;
  - c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
  - d) 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;
  - e) 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.



---

**ART. 16 - RINVIO**

Per tutto quanto non espressamente disciplinato, si applicano le disposizioni del GDPR e tutte le norme vigenti in materia, nonché i Regolamenti/Procedure adottati da ATS.

FIGURE PRIVACY	SOGGETTI DA NOMINARE	CHI DEVE OCCUPARSI DELLA NOMINA	REGISTRAZIONE DOCUMENTALE
Delegati al trattamento Allegato 1	- Dirigenti Responsabili di SS, SSD, SC, Direttori di Dipartimento	SC Gestione Sviluppo Risorse Umane al momento del conferimento incarico ( <u>a firma Direttore Generale</u> )	<b>ARCHIVIO:</b> Protocollo ATS (In Partenza) – Class.: 1.7.03 <b>TIPO DOCUMENTO:</b> Lettera di nomina <b>OGGETTO:</b> "Nomina il Dott./Dott.ssa Cognome-Nome quale soggetto Delegato al Trattamento dei dati personali" <b>MITTENTE:</b> SC Gestione Sviluppo Risorse Umane (con annotazione "N.B.: nota a firma DG") <b>DESTINATARIO:</b> Dirigente nominato e condivisione con la Struttura di appartenenza del soggetto nominato
Delegati al trattamento Allegato 1	- Direttore Amministrativo - Direttore Sanitario - Direttore Sociosanitario	Responsabile SC Affari Generali e Legali ( <u>a firma Direttore Generale</u> )	<b>ARCHIVIO:</b> Protocollo ATS (In Partenza) – Class.: 1.7.03 <b>TIPO DOCUMENTO:</b> Lettera di nomina <b>OGGETTO:</b> "Nomina il Dott./Dott.ssa Cognome-Nome quale soggetto Delegato al Trattamento dei dati personali" <b>MITTENTE:</b> Direzione Generale <b>DESTINATARIO:</b> Direttore nominato e condivisione con la Direzione di riferimento e Direzione Generale
Autorizzati al trattamento Allegato 4	- Dipendenti Comparto e Dirigenza professionale di ogni Struttura - Personale somministrato - Tirocinanti - Borsisti - Volontari - Incarichi gratuiti - Liberi professionisti (3)	Dirigenti Responsabili della Struttura in ragione della rispettiva afferenza personale (dipendenti, tirocinanti, borsisti, volontari, incarichi gratuiti, liberi professionisti) ( <u>a firma Dirigente delegato</u> )	<b>ARCHIVIO:</b> Protocollo ATS (In Partenza) – Class.: 1.7.03 <b>TIPO DOCUMENTO:</b> Lettera di nomina <b>OGGETTO:</b> "Nomina il Sig./Sig.ra/Dott./Dott.ssa Cognome-Nome quale soggetto Autorizzato al Trattamento dei dati personali" <b>MITTENTE:</b> Struttura di afferenza <b>DESTINATARIO:</b> Soggetto autorizzato e condivisione con la Struttura di afferenza; per dipendenti condivisione anche con SC Gestione Sviluppo Risorse Umane
Autorizzati al trattamento Allegato 4	- Studenti Corsi di Laurea	Coordinatori del Corso di Laurea ( <u>a firma Direttore Sanitario</u> )	<b>ARCHIVIO:</b> Protocollo ATS (In Partenza) – Class.: 1.7.03 <b>TIPO DOCUMENTO:</b> Lettera di nomina <b>OGGETTO:</b> "Nomina il Sig./Sig.ra/Dott./Dott.ssa Cognome-Nome quale soggetto Autorizzato al Trattamento dei dati personali" <b>MITTENTE:</b> Direzione Sanitaria <b>DESTINATARIO:</b> Soggetto autorizzato e condivisione con il Corso di Laurea
Autorizzati al trattamento Allegato 4	- Collegio Sindacale - Nucleo Valutazione Prestazioni	Responsabile SC Affari Generali e Legali ( <u>a firma Direttore Generale</u> )	<b>ARCHIVIO:</b> Protocollo ATS (In Partenza) – Class.: 1.7.03 <b>TIPO DOCUMENTO:</b> Lettera di nomina <b>OGGETTO:</b> "Nomina il Sig./Sig.ra/Dott./Dott.ssa Cognome-Nome quale soggetto Autorizzato al Trattamento dei dati personali" <b>MITTENTE:</b> Direzione Generale

<sup>3</sup> Sono considerati Autorizzati al trattamento se agiscono **senza mezzi propri** – personal computer e altre applicazioni di ATS -e/o svolgono l'attività **presso le sedi di ATS**.

Autorizzati al trattamento Allegato 4	- Ufficio di Pubblica Tutela	Responsabile Gestione Relazioni Esterne ed Esterne (a firma Direttore Generale)	Soggetto autorizzato e condivisione con Direzione Generale Protocollo ATS (In Partenza) – Class.: 1.7.03 Lettera di nomina "Nomina il Sig./Sig.ra/Dott./Dott.ssa Cognome-Nome quale soggetto Autorizzato al Trattamento dei dati personali" Funzione Relazioni Interne e Esterne URP (con annotazione "N.B.: nota a firma DG") Soggetto autorizzato e condivisione con Direzione Generale
Autorizzati al trattamento Allegato 4	- Consigliere di Fiducia	Presidente CUG (a firma Direttore Generale)	Protocollo ATS (In Partenza) – Class.: 1.7.03 Lettera di nomina "Nomina il Sig./Sig.ra/Dott./Dott.ssa Cognome-Nome quale soggetto Autorizzato al Trattamento dei dati personali" Comitato Unico Garanzia [CUG] (con annotazione "N.B.: nota a firma DG") Soggetto autorizzato e condivisione con Direzione Generale
Responsabili al trattamento dei dati personali ai sensi dell'art. 28 GDPR Allegato 2	- Fornitori di beni e servizi (con contratto e/o convenzione) - Esecutori di lavori - Altri soggetti (persone fisiche/giuridiche) che a vario titolo trattano dati per conto di ATS - Liberi professionisti (4)	SC Gestione Acquisti e Tecnico Patrimoniale per beni/servizi/lavori e altri Dirigenti delegati per liberi professionisti e altri soggetti in ragione dello specifico ambito di competenza (a firma Direttore Generale)	Registro Contratti ATS – Class.: 1.7.03 Controparte/libero professionista nominata/o Accordi e Protocolli d'intesa Data formalizzazione accordo "Accordo di nomina a Responsabile al trattamento dei dati personali in merito a (oggetto gara o incarico)" Struttura competente (con annotazione "N.B.: nota a firma DG")
Amministratori di Sistema "interni" Allegato 5	- Dipendenti SC Sistemi Informativi	- SC Sistemi Informativi (a firma Direttore Generale)	Protocollo ATS (In Partenza) – Class.: 1.7.05 Lettera di nomina "Nomina il Sig./Sig.ra/Dott./Dott.ssa Cognome-Nome quale Amministratore di sistema" Struttura di appartenenza (con eventuale annotazione "N.B.: nota a firma DG") Soggetto nominato e condivisione con la SC Sistemi Informativi
Responsabili ex art. 28 GDPR - Amministratori di Sistema "esterni"	- Fornitori di servizi (con contratto e/o convenzione) - Liberi professionisti e (5)	SC Gestione Acquisti e Tecnico Patrimoniale e altri Dirigenti delegati per liberi professionisti	Registro Contratti ATS – Class.:1.6.03 (Fornitori)/1.4.15 (L.P.) Controparte/libero professionista nominata/o

4 Sono considerati Responsabili esterni al trattamento se agiscono con mezzi propri – personal computer, altre applicazioni, archivi - e/o svolgono l'attività non presso le sedi di ATS

Allegato 3		in ragione dello specifico ambito di competenza (a <u>firma Direttore Generale</u> )	<p><b>CATEGORIA:</b> Accordi e Protocolli d'intesa</p> <p><b>DATA DI STIPULA:</b> Data formalizzazione accordo</p> <p><b>OGGETTO:</b> "Accordo di nomina a Responsabile al trattamento dei dati personali in merito a (oggetto gara o incarico) ..."</p> <p><b>ISTRUTTORIA A CURA DI:</b> Struttura competente (con annotazione "N.B.: nota a firma DG")</p>	Accordi e Protocolli d'intesa Data formalizzazione accordo "Accordo di nomina a Responsabile al trattamento dei dati personali in merito a (oggetto gara o incarico) ..." Struttura competente (con annotazione "N.B.: nota a firma DG")
Accordi di contitolarità per il trattamento dei dati	- Ente/Soggetto contitolare del trattamento dei dati	Dirigente delegato in ragione dello specifico ambito di competenza (a <u>firma Direttore Generale</u> )	<p><b>ARCHIVIO:</b> Registro Contratti ATS - Class.: 1.7.03</p> <p><b>CONTRAENTE:</b> Controparte nominata</p> <p><b>CATEGORIA:</b> Accordi e Protocolli d'intesa</p> <p><b>DATA DI STIPULA:</b> Data formalizzazione accordo</p> <p><b>OGGETTO:</b> "Accordo di nomina a Soggetto Contitolare del trattamento dei dati personali in merito a ..."</p> <p><b>ISTRUTTORIA A CURA DI:</b> Struttura competente e condivisione con Direzione Generale</p>	Registro Contratti ATS - Class.: 1.7.03 Controparte nominata Accordi e Protocolli d'intesa Data formalizzazione accordo "Accordo di nomina a Soggetto Contitolare del trattamento dei dati personali in merito a ..."



CI: 1.7.03

**Oggetto: Nomina a Delegato al trattamento dei dati personali.**

Gent.ma/Gent.mo \_\_\_\_\_

In conformità a quanto disposto dall'articolo 2-quaterdecies del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss.mm. ed al principio di libertà organizzativa interna prevista dal Regolamento 679/2016/UE, il Titolare del trattamento dei dati personali, **Agenzia di Tutela della Salute di Brescia**, sulla scorta di quanto previsto ai sensi dell'art. 6 del Regolamento sul Modello Organizzativo in materia di Protezione dei Dati Personali (MOP) approvato dal Titolare del trattamento con (*inserire estremi Decreto D.G. di approvazione*), attribuisce il ruolo di **Delegato al trattamento dei dati** personali a:

Soggetto	Ruolo	Descrizione	Descrizione dei Trattamenti
<i>Dati identificativi del dipendente (nome, cognome, codice fiscale, qualifica e struttura)</i>	Delegato al trattamento dei dati personali	<ul style="list-style-type: none"> <li>• supervisione, programmazione e coordinamento delle attività di trattamento dei dati personali svolti nell'ambito della struttura/direzione di competenza, nonché relativamente a specifiche attività istituzionali, nella misura e nei limiti delle mansioni e del ruolo funzionale svolto presso le strutture ed i locali del Titolare del trattamento;</li> <li>• nomina autorizzati al trattamento dei dati personali nell'ambito di competenza.</li> </ul>	Tutti i trattamenti di dati personali, inerenti alla struttura/direzione di competenza, nonché per specifiche attività istituzionali, così come mappati all'interno del Registro delle attività di Trattamento in uso

Il Delegato al trattamento dei dati personali dichiara di avere ricevuto 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 Regolamento 679/2016/UE), ed in particolare:

- Istruzioni per trattamento dati personali (reperibile nella intranet alla Sezione Privacy);
- Introduzione al Regolamento 679/2016/UE (reperibile nella intranet alla Sezione Privacy);
- Regolamento sul Modello Organizzativo in materia di Protezione dei dati personali (MOP) (reperibile nella intranet alla Sezione Privacy);
- Informativa Privacy Regolamento 679/2016/UE – Informativa Interessati (Personale dipendente, collaboratori e personale non strutturato) anche reperibile nella intranet alla Sezione Privacy.
- Modello di nomina Autorizzato (reperibile nella intranet alla Sezione Privacy).

Altra documentazione in essere presso ATS di Brescia in materia di trattamento dei dati personali è reperibile sulla rete intranet aziendale nella sezione Privacy, così come eventuali e successivi aggiornamenti.



Il Delegato al trattamento dei dati personali dichiara inoltre di attenersi rigorosamente alle istruzioni impartite dal Titolare del trattamento, eventualmente anche attraverso incontri formativi e/o in forma scritta.

Secondo quanto previsto dall'art. 6.4 del Regolamento sul Modello Organizzativo in materia di Protezione dei Dati Personali (MOP) approvato dal Titolare del trattamento, ai Delegati al trattamento dei dati personali sono attribuiti i seguenti compiti, relativi ai trattamenti di dati personali di propria competenza:

- a) collaborare con il Titolare nell'identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività di ATS;
- b) collaborare con il Titolare nel predisporre ed aggiornare il registro delle attività di trattamento, procedendo alla comunicazione delle modifiche intervenute ai trattamenti di competenza al Tavolo Tecnico Privacy, al fine di aggiornare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria struttura, nonché il registro dei trattamenti;
- c) collaborare con il Titolare nel definire, per ciascun trattamento di dati personali, la durata del trattamento, l'archiviazione e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- d) collaborare con il Titolare nel condurre ogni valutazione atta a verificare la necessità dell'effettuazione della valutazione d'impatto sui trattamenti di competenza;
- e) collaborare con il Titolare nella predisposizione delle informative relative alle competenze della struttura e provvedere a che siano rese disponibili ai soggetti interessati;
- f) disporre l'attuazione dei provvedimenti emessi dal Garante Privacy sulla scorta delle indicazioni del Titolare;
- g) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- h) individuare, tra gli operatori assegnati alla Struttura o ai collaboratori/professionisti alla stessa afferenti, designandoli per iscritto, gli Autorizzati al trattamento e adoperarsi al fine di rendere effettive le istruzioni cui devono attenersi gli stessi, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati – anche presenti nelle banche dati e sulle piattaforme informatiche disponibili - nonché l'osservanza da parte degli stessi, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- i) gestire ogni adempimento istruttorio finalizzato alla formalizzazione della nomina di un Responsabile del trattamento dei dati personali o della nomina di ATS a Responsabile del trattamento dei dati personali;
- j) per l'istruttoria che precede, lett. i), coordinarsi con la S.C. Sistemi Informativi con riferimento alle necessarie valutazioni ed identificazioni (che confluiranno nel relativo atto di nomina) rispetto all'eventuale ruolo di Amministratore di sistema assunto dal Responsabile del trattamento dei dati personali o assunto da ATS quale Responsabile del trattamento dei dati personali;
- k) far osservare gli adempimenti previsti in caso di nuovi trattamenti e archiviazione di trattamenti;
- l) individuare il personale della propria struttura organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
- m) adottare, con il supporto del Tavolo Tecnico Privacy e della S.C. Sistemi Informativi aziendali soluzioni di privacy "by design e by default", ovvero di protezione dei dati personali 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, riducendo al minimo i rischi di distruzione o



perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- n) collaborare con il Titolare nel definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti al trattamento dei dati e assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- o) attenersi alle previsioni previste dal Titolare in ordine alle procedure di "data breach" ed a quelle relative all'esercizio dei diritti da parte degli interessati.

Secondo quanto disposto dall'articolo 5 comma 1) del Regolamento 679/2016/UE i dati personali oggetto del trattamento devono essere:

- trattati in modo lecito corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il loro utilizzo non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati (devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati);
- conservati nel rispetto dei termini di conservazione stabiliti dal Massimario di Scarto approvato da Regione Lombardia attualmente in vigore e ss.mm.ii. e, comunque, in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati medesimi sono trattati, in ossequio alla data retention stabilita dal Titolare;
- trattati in maniera da garantire un'adeguata sicurezza di dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti o dalla perdita, dalla distruzione o dal danno accidentali.

Con la presente il Delegato al trattamento dei dati personali dichiara di essere a conoscenza che tutti i dati personali di cui lo stesso verrà a conoscenza in virtù della propria attività esercitata per conto del Titolare del trattamento non potranno in alcun modo essere divulgati a terzi, se non nei termini ed alle condizioni prescritte dalle norme vigenti e comunque nel rispetto dei principi di necessità ed indispensabilità e dovranno essere utilizzati esclusivamente per finalità attinenti all'attività esercitata per conto del Titolare. La violazione di tale divieto renderà il soggetto passibile anche di sanzione disciplinare, impregiudicata ogni altra responsabilità di natura civile, penale, amministrativa e dirigenziale.

La nomina è correlata alla durata dell'incarico dirigenziale di struttura ricoperto.

L'attività di trattamento individuata nel presente atto potrebbe essere soggetta ad aggiornamento; 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 a tre mesi.

Sistema Socio Sanitario



Regione  
Lombardia

ATS Brescia

Il presente atto di nomina sostituisce ogni precedente atto della stessa natura sottoscritto dal Delegato al trattamento dei dati personali.

Brescia, \_\_\_\_\_

**Firma Titolare del trattamento ATS Brescia**

\_\_\_\_\_

**Firma del Delegato**

\_\_\_\_\_



CI: 1.7.03

**Oggetto: Nomina Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE/679/2016 sulla protezione dei dati e la loro libera circolazione.**

**Agenzia di Tutela della Salute di Brescia** con sede in Brescia, in Viale Duca degli Abruzzi n. 15 – P.IVA/C.F. 03775430980 in qualità Titolare del trattamento dei dati personali (d'ora in avanti anche "Titolare") attribuisce il ruolo di **Responsabile del trattamento dei dati personali** a:

.....

con sede in ....., ..... in ..... (.....) - P.IVA ....., C.F. ....

**Trattamento:** ..... (*indicare riferimenti contratto/atto*)

**Finalità del trattamento**

Compilare.....  
.....

**Natura del trattamento**

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.

Altro .....

**Tipologia dei dati personali trattati**

- comuni identificativi (nome, cognome, dati anagrafici, recapiti di posta elettronica, recapiti telefonici, residenza, etc.).
- appartenenti a categorie particolari ai sensi dell'art. 9 del Regolamento 679/2016/UE e idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

**Categoria dei soggetti interessati**

- personale dipendente e collaboratore;
- fornitori;
- clienti;
- utenti;
- membri del Consiglio di Amministrazione (CdA);
- soci (di società di persone e/o capitali);
- associati (per le associazioni di volontariato e/o fondazioni);
- volontari;
- altro.....

Tale incarico viene attribuito ai sensi dell'articolo 28 del Regolamento 679/2016/UE (d'ora in avanti denominato semplicemente "Regolamento"). Il presente documento rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dal paragrafo 3 del citato articolo 28.



Garanzie generali di sicurezza prestate dal Responsabile (Art. 28.1 Regolamento)

Il Responsabile del trattamento (d'ora in avanti anche "Responsabile") garantisce l'attuazione di misure tecniche ed organizzative tali da soddisfare, nella loro totalità, i requisiti posti dal Regolamento.

Autorizzazione nomina Sub-Responsabili (Art. 28.2 – 28.4 Regolamento)

Ai sensi dell'art. 28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub-responsabili". A fronte di tale autorizzazione, si richiede al Responsabile di comunicare alla scrivente l'elenco di tutti gli eventuali soggetti individuati in qualità di Sub-Responsabili. La scrivente provvederà a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei Sub-Responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla scrivente al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.

Si precisa come è obbligo del Responsabile individuare e nominare in forma scritta i propri Sub-Responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del Sub-Responsabile i medesimi obblighi posti a carico del Responsabile e specificati nel presente documento; in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.

Si evidenzia come il Responsabile conservi nei confronti della scrivente, Titolare del trattamento, ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal Sub-Responsabile.

Prescrizioni poste a carico del Responsabile (art. 28.3 Regolamento)

Per lo svolgimento delle attività di trattamento dati personali conseguenti al servizio affidato al Responsabile, lo stesso dovrà:

- a. comunicare preventivamente l'eventuale trasmissione dei dati personali verso paese terzo (non appartenente alla Unione Europea); in tali casistiche il Titolare si riserva la facoltà di esprimere apposita autorizzazione alla trasmissione a meno che tale trasmissione non sia espressamente richiesta dell'Unione o dal diritto nazionale;
- b. autorizzare espressamente al trattamento dei dati personali i propri dipendenti/collaboratori/soci/volontari attraverso modalità che garantiscano che tali soggetti siano obbligati al rispetto della riservatezza nei confronti dei dati che si troveranno a trattare in funzione del proprio incarico/ruolo;
- c. garantire di aver effettuato una analisi dei rischi sui trattamenti oggetto della responsabilità e assistere il Titolare nella valutazione di impatto ai sensi dell'art. 35 del Regolamento tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile; i documenti comprovanti l'analisi del rischio e l'eventuale valutazione di impatto dovranno essere messi a disposizione del Titolare su richiesta di quest'ultimo;
- d. garantire la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
- e. garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
- f. garantire la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;



- g. garantire che tutti i soggetti che agiscono sotto l'autorità del Responsabile e che abbiano accesso ai dati non trattino tali dati se non sono stati istruiti in tal senso dal Responsabile stesso;
- h. garantire il necessario apporto al Titolare del trattamento qualora nei confronti di questo vengano esercitati i diritti che il Regolamento (al capo III) riconosce agli interessati i quali impattino sui dati personali oggetto della presente nomina;
- i. garantire la comunicazione al Titolare (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali al fine di consentire al Titolare stesso il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del Regolamento. La comunicazione da parte del Responsabile al Titolare dovrà avvenire senza ingiustificato ritardo e comunque entro 24 ore, all'indirizzo PEC istituzionale ([protocollo@pec.ats-brescia.it](mailto:protocollo@pec.ats-brescia.it)) e dovrà contenere almeno i seguenti punti:
- natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  - il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
  - descrivere le probabili conseguenze della violazione dei dati personali;
  - descrivere le misure adottate da parte del Responsabile per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
- Il Responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite;
- j. cancellare e/o restituire al Titolare tutti i dati personali una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il Titolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione;
- k. rendersi disponibile a sottoporsi ad attività di auditing da parte del Titolare, o di un delegato di quest'ultimo, qualora questo ne ravvisasse la necessità;
- l. comunicare al Titolare l'adesione ad eventuali codici di condotta di cui all'articolo 40 o ad un meccanismo di certificazione di cui all'articolo 42 del Regolamento;
- m. attenersi ai criteri di durata del trattamento comunicati dal Titolare, nel rispetto dei termini di conservazione stabiliti dal Massimario di Scarto approvato dalla Regione Lombardia attualmente in vigore e ss.mm.ii..

### Responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile. Il Responsabile risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi posti dal Regolamento specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare nel presente atto.

In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.

Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli artt. 82, 83 e 84 del Regolamento.

In caso di accertata violazione delle disposizioni del Regolamento o del presente atto negoziale, il Titolare si riserva il diritto di mettere in atto le misure ritenute corrette nei confronti del Responsabile.



### Durata e risoluzione

Le prescrizioni di cui al presente atto hanno decorrenza dall'ultima data di sottoscrizione e scadenza coincidente a quella indicata nel *contratto/atto* cui il presente atto negoziale accede.

### **Privacy by design e by default**

Si richiama il rispetto dei principi di privacy by design art 25.1 e privacy by default art 25.2 del Regolamento. Tali principi garantiscono la protezione dei dati dalla fase di ideazione e progettazione di un trattamento o di un sistema e l'adozione di comportamenti che consentano di prevenire possibili problematiche.

Il principio di privacy by design ex art 25.1 del Regolamento, descrive i criteri necessari a garantire la protezione dei dati personali sin dall'avvio del trattamento ed in particolare:

- la necessità di minimizzare l'uso del dato;
- la necessità di tutelare i diritti dell'interessato.

L'applicazione della privacy by default, ex art 25.2 del Regolamento implica, invece, l'adozione di misure tecniche ed organizzative che garantiscano, per impostazione predefinita, che siano trattati solo i dati necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati raccolta, la portata del trattamento, il periodo di conservazione e l'accessibilità. Non deve essere consentito l'accesso di dati personali a un numero indefinito di persone fisiche senza l'intervento di una persona fisica.

Nell'applicazione dei principi della privacy by design e della privacy by default, in riferimento alle misure tecniche e organizzative, il considerando 78 del Regolamento dispone che *"al fine di poter dimostrare la conformità con il presente regolamento, il Titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default."* Inoltre il medesimo considerando 78 dispone che *"i produttori dei prodotti dei servizi e delle applicazioni, in fase di sviluppo, progettazione selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattando dati personali per svolgere le loro funzioni i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i Titolari del trattamento e i Responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati"*.

In considerazione di quanto sopra esposto risulta necessario essere in grado di dimostrare in termini di accountability che i trattamenti di dati personali sviluppati mediante i prodotti o servizi forniti dalla vostra azienda siano conformi ai citati principi di privacy by design e privacy by default.

Pertanto, con la presente il Responsabile garantisce che i prodotti ed i servizi forniti dalla propria azienda rispettano i principi della privacy by design e della privacy by default in particolar modo per quanto concerne:

- la minimizzazione nella durata del trattamento dati (art. 5.1.f - art. 25.2 del Regolamento);
- la minimizzazione nella tipologia di dati trattati (art. 5.1.f - art. 25.2 del Regolamento);
- la minimizzazione nella quantità di dati trattati (art. 5.1.f - art. 25.2 del Regolamento);
- la minimizzazione negli accessi ai dati (art. 5.1.f - art. 25.2 del Regolamento);
- la limitazione del trattamento (considerando 67 - art. 4.3 - art. 18 del Regolamento);
- la cancellazione dei dati (art. 17 del Regolamento);
- la possibilità di individuare una tempistica di conservazione dei dati (art. 13.2.a - art. 30.1.f del Regolamento).

Brescia, \_\_\_\_\_

Sistema Socio Sanitario



Regione  
Lombardia

ATS Brescia

**Firma del Titolare del trattamento  
ATS Brescia**

\_\_\_\_\_

**Firma del Responsabile del trattamento**

\_\_\_\_\_

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

CI: 1.6.03 (FORNITORI DI BENI E SERVIZI – ESECUTORI DI LAVORI)

oppure

CI: 1.4.15 (L.P.)

**Oggetto: Nomina Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE/679/2016 e nomina ad Amministratore di Sistema "esterno" ai sensi e per gli effetti del Provvedimento a carattere generale dell'Autorità Garante per la Protezione dei Dati Personali del 27 Novembre 2008 e ss.mm.ii.**

**Agenzia di Tutela della Salute di Brescia** con sede in Brescia, in Viale Duca degli Abruzzi n. 15 – P.IVA/C.F. 03775430980 in qualità Titolare del trattamento dei dati personali (d'ora in avanti anche "Titolare") attribuisce il ruolo di **Responsabile del trattamento dei dati personali e Amministratore di Sistema** a:

.....

con sede in ....., ..... in ..... (.....) - P.IVA ....., C.F. ....

**Trattamento:** ..... (*indicare riferimenti contratto/atto*)

**Finalità del trattamento**

Compilare.....

.....

**Natura del trattamento**

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.

Altro .....

**Tipologia dei dati personali trattati**

- comuni identificativi (nome, cognome, dati anagrafici, recapiti di posta elettronica, recapiti telefonici, residenza, etc.).
- appartenenti a categorie particolari ai sensi dell'art. 9 del Regolamento 679/2016/UE e idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

**Categoria dei soggetti interessati**

- personale dipendente e collaboratore;
- fornitori;
- clienti;
- utenti;
- membri del Consiglio di Amministrazione (CdA);
- soci (di società di persone e/o capitali);
- associati (per le associazioni di volontariato e/o fondazioni);
- volontari
- altro.....

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

--	--

Tale incarico viene attribuito ai sensi dell'articolo 28 del Regolamento UE/679/2016 (d'ora in avanti denominato semplicemente "Regolamento") e ai sensi e per gli effetti del Provvedimento a carattere generale dell'Autorità Garante per la Protezione dei Dati Personali del 27 Novembre 2008 e ss.mm.ii. (d'ora in avanti anche Provvedimento). Il presente documento rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dal paragrafo 3 del citato articolo 28 e dalle disposizioni contenute nel Provvedimento.

Garanzie generali di sicurezza prestate dal Responsabile (Art. 28.1 Regolamento)

Il Responsabile del trattamento (d'ora in avanti anche "Responsabile") garantisce l'attuazione di misure tecniche ed organizzative tali da soddisfare, nella loro totalità, i requisiti posti dal Regolamento.

Autorizzazione nomina Sub-Responsabili (Art. 28.2 - 28.4 Regolamento)

Ai sensi dell'art. 28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "Sub-Responsabili". A fronte di tale autorizzazione, si richiede al Responsabile di comunicare alla scrivente l'elenco di tutti gli eventuali soggetti individuati in qualità di Sub-Responsabili. La scrivente provvederà a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei Sub-Responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla scrivente al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.

Si precisa come è obbligo del Responsabile individuare e nominare in forma scritta i propri Sub-Responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del Sub-Responsabile i medesimi obblighi posti a carico del Responsabile e specificati nel presente documento; in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate a garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.

Si evidenzia come il Responsabile conservi nei confronti della scrivente, Titolare del trattamento, ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal Sub-Responsabile.

Prescrizioni poste a carico del Responsabile (art. 28.3 Regolamento)

Per lo svolgimento delle attività di trattamento dati personali conseguenti al servizio affidato al Responsabile, lo stesso dovrà:

- a. comunicare preventivamente l'eventuale trasmissione dei dati personali verso paese terzo (non appartenente alla Unione Europea); in tali casistiche il Titolare si riserva la facoltà di esprimere apposita autorizzazione alla trasmissione a meno che tale trasmissione non sia espressamente richiesta dell'Unione o dal diritto nazionale;
- b. autorizzare espressamente al trattamento dei dati personali i propri dipendenti/collaboratori/soci/volontari attraverso modalità che garantiscano che tali soggetti siano obbligati al rispetto della riservatezza nei confronti dei dati che si troveranno a trattare in funzione del proprio incarico/ruolo;

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

- c. garantire di aver effettuato una analisi dei rischi sui trattamenti oggetto della responsabilità e assistere il Titolare nella valutazione di impatto ai sensi dell'art. 35 del Regolamento tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile; i documenti comprovanti l'analisi del rischio e l'eventuale valutazione di impatto dovranno essere messi a disposizione del Titolare su richiesta di quest'ultimo;
- d. garantire la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
- e. garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
- f. garantire la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
- g. garantire che tutti i soggetti che agiscono sotto l'autorità del Responsabile e che abbiano accesso ai dati non trattino tali dati se non sono stati istruiti in tal senso dal Responsabile stesso;
- h. garantire il necessario apporto al Titolare del trattamento qualora nei confronti di questo vengano esercitati i diritti che il Regolamento (al capo III) riconosce agli interessati i quali impattino sui dati personali oggetto della presente nomina;
- i. garantire la comunicazione al Titolare (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali al fine di consentire al Titolare stesso il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del Regolamento. La comunicazione da parte del Responsabile al Titolare dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC istituzionale ([protocollo@pec.ats-brescia.it](mailto:protocollo@pec.ats-brescia.it)) e dovrà contenere almeno i seguenti punti:
  - a. natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  - b. il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
  - c. descrivere le probabili conseguenze della violazione dei dati personali;
  - d. descrivere le misure adottate da parte del Responsabile per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
 Il Responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite;
- j. cancellare e/o restituire al Titolare tutti i dati personali una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il Titolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione;
- k. rendersi disponibile a sottoporsi ad attività di auditing da parte del Titolare, o di un delegato di quest'ultimo, qualora questo ne ravvisasse la necessità;
- l. comunicare al Titolare l'adesione ad eventuali codici di condotta di cui all'articolo 40 o ad un meccanismo di certificazione di cui all'articolo 42 del Regolamento;
- m. attenersi ai criteri di durata del trattamento comunicati dal Titolare nel rispetto dei termini di conservazione stabiliti dal Massimario di Scarto approvato dalla Regione Lombardia attualmente in vigore e ss.mm.ii..

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

Prescrizioni poste a carico del Responsabile ai sensi del Provvedimento a carattere generale del 27 Novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali

Ai sensi del Provvedimento il Responsabile è stato individuato dal Titolare del trattamento dei dati personali in base ad una scrupolosa valutazione dell'esperienza, della capacità, dell'affidabilità e preparazione e fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

Il Responsabile ha quindi, il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle vigenti disposizioni in materia di trattamento dei dati personali ivi compreso il profilo relativo alla sicurezza.

Il Responsabile garantisce al Titolare del trattamento che ciascun incaricato quale Amministratore di Sistema accede alle risorse informatiche con credenziali di autenticazione nominative (*username* e *password*).

Con la sottoscrizione di questa nomina il Responsabile si impegna a nominare individualmente ai sensi del Provvedimento a carattere generale del 27 Novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali pubblicato nella Gazzetta Ufficiale N. 300 del 24 dicembre 2008, così come modificato dal successivo Provvedimento dell'Autorità Garante del 25 giugno 2009 pubblicato nella Gazzetta Ufficiale N. 149 del 30 giugno 2009 - gli incaricati della propria struttura che rivestono il ruolo di Amministratori del Sistema informativo. La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Annualmente il Responsabile fornisce al Titolare del trattamento l'elenco aggiornato nominativo degli Amministratori di Sistema e provvede a verificare l'attività dei soggetti individuati, come indicato dall'Autorità Garante.

Il Responsabile o il Titolare adotta sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici effettuati da parte dell'Amministratore di Sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Il Responsabile è tenuto a:

- garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto a seguito di apposita comunicazione in tal senso del Titolare del trattamento, utilizzando gli opportuni meccanismi di identificazione e autenticazione allo scopo di incrementare il livello di protezione e sicurezza dei trattamenti di dati personali effettuati con strumenti elettronici;
- essere Responsabile della gestione dei sistemi di identificazione ed autenticazione, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge, eseguendo controlli periodici sull'efficacia delle misure di sicurezza adottate;
- collaborare con il Titolare del trattamento dei dati alla definizione di idonee regole in ambito di sicurezza del trattamento dei dati afferente ai sistemi oggetto della presente nomina;
- sovrintendere all'operato dei soggetti terzi idoneamente designati, qualora sia necessario, interni o esterni alla organizzazione del Titolare, in caso di interventi tecnici che abbiano impatto sul sistema informativo del Titolare e sulla sicurezza del trattamento di dati;

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

- suggerire, curare e sovrintendere l'adozione e l'aggiornamento delle più ampie misure di sicurezza volte a far sì che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- aggiornare periodicamente, con frequenza adeguata, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti o assicurarsi che ciò venga effettuato da soggetti terzi idoneamente designati;
- coadiuvare il Titolare del trattamento, il Delegato, gli altri Responsabili e gli Amministratori di Sistema interni, se designati dal Titolare nell'attuazione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura e dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- svolgere un ruolo di primaria interfaccia nella scelta delle dotazioni informatiche, nessuna esclusa, quali *hardware* di qualsiasi genere, *software* e qualsiasi altro dispositivo elettronico e di tutti i processi tecnologici del Titolare, coadiuvando le singole articolazioni aziendali nel processo decisionale sulle suddette dotazioni informatiche;
- svolgere un ruolo di primaria interfaccia coadiuvando il Titolare del trattamento, il Delegato, gli altri Responsabili e gli Amministratori di Sistema interni della struttura informatica, se designati dal Titolare, nel caso di incidenti/malfunzionamenti di qualsiasi genere che riguardino la rete, le attrezzature informatiche e l'utenza e preoccuparsi di erogare una corretta informazione verso gli utenti supportando il processo di indagine e diagnosi dei problemi ed essere in grado di produrre le necessarie informazioni a tal riguardo;
- svolgere un ruolo di primaria interfaccia coadiuvando il Titolare del trattamento, il Delegato, gli altri Responsabili e gli Amministratori di Sistema interni della struttura informatica, se designati dal Titolare nell'innovazione della struttura di Information Technology (IT) nel suo complesso, proseguendo l'innovazione tecnologica al fine di dotare il Titolare di un moderno sistema di gestione informatica ottimizzandone i processi;
- sovrintendere alle operazioni di coordinamento e funzionamento della rete informatica interna;
- eseguire direttamente o assicurarsi che vengano realizzate da soggetti terzi idoneamente designati le copie di sicurezza e ripristino, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge;
- assegnare e gestire il sistema di autenticazione informatica e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;
- procedere, più in particolare, alla disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali per oltre 6 (sei) mesi;
- adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità alle linee guida AGID;

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di backup, vigilando sulle procedure attivate dal Titolare; l'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
- cooperare nella predisposizione del registro dei trattamenti supportando adeguatamente il DPO del Titolare per la parte concernente il sistema informatico ed il trattamento informatico dei dati;
- vigilare sugli interventi informatici diretti al sistema informatico del Titolare e sull'impianto di videosorveglianza, effettuati da vari operatori esterni; in caso di anomalie sarà sua cura segnalarle direttamente al DPO e al Direttore della SC Sistemi Informativi;
- predisporre ed implementare le eventuali ulteriori misure di sicurezza imposte dalle misure minime di sicurezza AGID per il trattamento informatico dei dati comuni e particolari e per la conseguente tutela degli strumenti elettronici;
- coordinare assieme al Titolare (e/o al RTD) le attività operative degli autorizzati al trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico;
- collaborare con il Titolare (e/o al RTD) e con il DPO per l'attuazione delle prescrizioni impartite dal Garante;
- comunicare prontamente al Titolare (e/o al RTD) e al DPO qualsiasi situazione di cui sia venuta a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;
- verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore utilizzati dal Titolare.

Il Titolare provvederà, con cadenza almeno semestrale e per il tramite della SC Sistemi Informativi, a svolgere le dovute verifiche sulle attività compiute dall'Amministratore di sistema. È obbligo di quest'ultimo prestare al Titolare la sua piena collaborazione per il compimento delle verifiche stesse; in ogni caso, è tenuto a predisporre, con cadenza annuale, una relazione scritta delle attività svolte in esecuzione delle incombenze affidatigli in forza del presente atto.

#### Responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile. Il Responsabile risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi posti dal Regolamento specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare nel presente atto.

In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.

Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli art. 82, 83 e 84 del Regolamento.

In caso di accertata violazione delle disposizioni del Regolamento o del presente atto negoziale, il Titolare si riserva il diritto di mettere in atto le misure ritenute corrette nei confronti del Responsabile.

#### Durata e risoluzione

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

Le prescrizioni di cui al presente atto hanno decorrenza dall'ultima data di sottoscrizione e scadenza coincidente a quella indicata nel *contratto/atto* cui il presente atto negoziale accede.

### **Privacy by design e by default**

Si richiama il rispetto dei principi di privacy by design art 25.1 e privacy by default art 25.2 del Regolamento. Tali principi garantiscono la protezione dei dati dalla fase di ideazione e progettazione di un trattamento o di un sistema e l'adozione di comportamenti che consentano di prevenire possibili problematiche.

Il principio di privacy by design ex art 25.1 del Regolamento, descrive i criteri necessari a garantire la protezione dei dati personali sin dall'avvio del trattamento ed in particolare:

- la necessità di minimizzare l'uso del dato;
- la necessità di tutelare i diritti dell'interessato.

L'applicazione della privacy by default, ex art 25.2 del Regolamento, implica, invece, l'adozione di misure tecniche ed organizzative che garantiscano, per impostazione predefinita, che siano trattati solo i dati necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati raccolta, la portata del trattamento, il periodo di conservazione e l'accessibilità. Non deve essere consentito l'accesso di dati personali a un numero indefinito di persone fisiche senza l'intervento di una persona fisica. Nell'applicazione dei principi della privacy by design e della privacy by default, in riferimento alle misure tecniche e organizzative, il considerando 78 del Regolamento dispone che *"al fine di poter dimostrare la conformità con il presente regolamento, il Titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default."* Inoltre il medesimo considerando 78 dispone che *"i produttori dei prodotti dei servizi e delle applicazioni, in fase di sviluppo, progettazione selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattando dati personali per svolgere le loro funzioni i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati"*. In considerazione di quanto sopra esposto risulta necessario essere in grado di dimostrare in termini di accountability che i trattamenti di dati personali sviluppati mediante i prodotti o servizi forniti dalla vostra spett. azienda siano conformi ai citati principi di privacy by design e privacy by default.

Pertanto, con la presente il Responsabile garantisce che i prodotti ed i servizi forniti dalla propria azienda rispettano i principi della privacy by design e della privacy by default in particolar modo per quanto concerne:

- la minimizzazione nella durata del trattamento dati (art. 5.1.f - art. 25.2 del Regolamento);
- la minimizzazione nella tipologia di dati trattati (art. 5.1.f - art. 25.2 del Regolamento);
- la minimizzazione nella quantità di dati trattati (art. 5.1.f - art. 25.2 del Regolamento);
- la minimizzazione negli accessi ai dati (art. 5.1.f - art. 25.2 del Regolamento);
- la limitazione del trattamento (considerando 67 - art. 4.3 - art. 18 del Regolamento);
- la cancellazione dei dati (art. 17 del Regolamento);
- la possibilità di individuare una tempistica di conservazione dei dati (art. 13.2.a - art. 30.1.f del Regolamento).

Brescia, \_\_\_\_\_

Sistema Socio Sanitario



Regione  
Lombardia

ATS Brescia

**Firma del Titolare del trattamento ATS  
Brescia**

\_\_\_\_\_

**Firma del Responsabile del  
trattamento e Amministratore di  
Sistema**

\_\_\_\_\_

Sistema Socio Sanitario

Regione  
Lombardia

ATS Brescia

**Allegato A****ELENCO NOMINATIVO DEI SOGGETTI CHE OPERANO IN QUALITÀ DI AMMINISTRATORI DI SISTEMA REDATTO DAL RESPONSABILE**

<b>Cognome e Nome e codice fiscale</b>

Il presente Allegato deve essere costantemente aggiornato dal responsabile in caso di modifiche e-comunicato senza ritardo (e comunque non oltre le 48 ore) al Titolare.

**Luogo e data** \_\_\_\_\_

**Firma del Titolare del trattamento ATS  
Brescia**

\_\_\_\_\_

**Firma del Responsabile del trattamento  
e Amministratore di Sistema**

\_\_\_\_\_



Cl: 1.7.03

**Oggetto: Nomina Autorizzato al trattamento dei dati personali.**

Gent.ma/Gent.mo \_\_\_\_\_

In conformità a quanto disposto dall'articolo 2-quaterdecies del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss.mm. ed al principio di libertà organizzativa interna prevista dal Regolamento 679/2016/UE, il Titolare del trattamento, **Agenzia di Tutela della Salute di Brescia** oppure il Dott./la Dott.ssa \_\_\_\_\_ Delegato al trattamento dei dati personali e individuato ai sensi dell'art. 6 del Regolamento sul Modello Organizzativo in materia di Protezione dei Dati Personali (MOP), approvato dal Titolare del trattamento con (*inserire estremi Decreto D.G. di approvazione*) nomina **Autorizzato al trattamento dei dati personali:**

Soggetto	Ruolo	Descrizione	Descrizione dei Trattamenti
<i>Dati identificativi del dipendente (nome, cognome, codice fiscale, qualifica)</i>	Autorizzato al trattamento dei dati personali	accesso e trattamento dei dati personali, nella misura e nei limiti delle mansioni e del ruolo funzionale svolto presso le strutture e i locali del Titolare del trattamento	Tutti i trattamenti di dati personali, inerenti alla struttura di appartenenza del dipendente, oppure del personale somministrato, dei tirocinanti, dei borsisti, dei volontari, dei titolari di incarichi gratuiti, dei liberi professionisti, così come mappati all'interno del Registro delle attività di Trattamento in uso.

L'Autorizzato dichiara di avere ricevuto 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 Regolamento 679/2016/UE) ed in particolare:

- Istruzioni per Trattamento dati personali (reperibile nella intranet alla Sezione Privacy);
- Introduzione al Regolamento 679/2016/UE (reperibile nella intranet alla Sezione Privacy);
- Regolamento sul Modello Organizzativo in materia di Protezione dei dati personali (MOP); (reperibile nella intranet alla Sezione Privacy);
- Informativa Privacy Regolamento 679/2016/UE – Informativa Interessati (Personale dipendente, collaboratori e personale non strutturato) anche reperibile nella intranet alla Sezione Privacy.

Altra documentazione in essere presso ATS di Brescia in materia di trattamento dei dati personali è, altresì, reperibile sulla rete intranet aziendale nella sezione Privacy così come eventuali e successivi aggiornamenti.

Il soggetto dichiara, inoltre, di attenersi rigorosamente alle istruzioni impartite dal Titolare del trattamento o dal Delegato, eventualmente anche attraverso incontri formativi e/o in forma scritta.

Secondo quanto disposto dall'articolo 5 comma 1) del Regolamento 679/2016/UE, i dati personali oggetto del trattamento devono essere:

- trattati in modo lecito corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il loro utilizzo non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;



- esatti e, se necessario, aggiornati (devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati medesimi sono trattati, in ossequio alla data retention stabilita dal Titolare;
- trattati in maniera da garantire un'adeguata sicurezza di dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti o dalla perdita, dalla distruzione o dal danno accidentali.

Con la sottoscrizione del presente atto l'Autorizzato dichiara di aver compreso che tutti i dati personali di cui lo stesso verrà a conoscenza in virtù della propria attività esercitata per conto del Titolare del trattamento e/o del Delegato non potranno in alcun modo essere divulgati a terzi e dovranno essere utilizzati esclusivamente per finalità attinenti all'attività esercitata per conto del Titolare o del Delegato. La violazione di tale divieto renderà il soggetto passibile anche di sanzione disciplinare, impregiudicata ogni altra responsabilità di natura civile, penale, amministrativa e, con riguardo al personale dirigente, dirigenziale.

L'attività di trattamento individuata nel presente atto potrebbe essere soggetta ad aggiornamento; 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 o dal Delegato.

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 a tre mesi.

Il presente atto di nomina sostituisce ogni precedente atto della stessa natura sottoscritto dall'Autorizzato.

Brescia, \_\_\_\_\_

**Firma del Titolare del Trattamento  
ATS Brescia**

oppure

**Firma del Delegato del Trattamento**

**Firma dell'Autorizzato**

CI: 1.7.03

**Oggetto: Nomina dell'Amministratore di Sistema "interno".**

In conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale n. 300 del 24 dicembre 2008 recante le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", **Agenzia di Tutela della Salute di Brescia**, nomina:

**Amministratore di sistema**

....., C.F. ...., (indicare ruolo ricoperto in organico)

Il Soggetto designato è stato individuato dal Titolare del trattamento dei dati personali in base ad una scrupolosa valutazione dell'esperienza, della capacità e dell'affidabilità dello stesso.

Il Soggetto designato ha il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle vigenti disposizioni in materia di trattamento dei dati personali ivi compreso il profilo relativo alla sicurezza.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

L'Amministratore di Sistema viene designato quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione 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, le reti locali e gli apparati di sicurezza, i sistemi hardware e software che consentono di utilizzare la rete internet e il servizio di posta elettronica nella misura in cui consentano di intervenire sui dati personali.

L'Amministratore di sistema opererà nei seguenti ambiti:

- a. gestione dei sistemi operativi;
- b. gestione delle credenziali di autenticazione;
- c. gestione dei data base;
- d. gestione delle reti;
- e. gestione degli strumenti e apparati di sicurezza, comprese le copie di sicurezza e ripristino;
- f. manutenzione hardware e software;
- g. gestione dei locali adibiti a contenere database e archivi aziendali.

In relazione a tale incarico l'Amministratore di sistema avrà il compito di sovrintendere alle risorse del sistema informatico e, in particolare, dovrà:



- garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto a seguito di apposita comunicazione in tal senso del Titolare del trattamento, utilizzando gli opportuni meccanismi di identificazione e autenticazione allo scopo di incrementare il livello di protezione e sicurezza dei trattamenti di dati personali effettuati con strumenti elettronici;
- essere responsabile della gestione dei sistemi di identificazione ed autenticazione, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge, eseguendo controlli periodici sull'efficacia delle misure di sicurezza adottate;
- collaborare con il Titolare del trattamento dei dati alla definizione di idonee regole in ambito di Sicurezza del trattamento dei dati afferente ai sistemi oggetto della presente nomina;
- sovrintendere all'operato dei soggetti terzi idoneamente designati, qualora sia necessario, interni o esterni al Titolare, in caso di interventi tecnici che abbiano impatto sul sistema informativo del Titolare e sulla sicurezza del trattamento di dati;
- suggerire, curare e sovrintendere l'adozione e l'aggiornamento delle più ampie misure di sicurezza volte a far sì che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- aggiornare periodicamente, con frequenza adeguata, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti o assicurarsi che ciò venga effettuato da soggetti terzi idoneamente designati;
- coadiuvare il Titolare del trattamento, il Delegato, i Responsabili e gli altri Amministratori di Sistema interni, se designati, nell'attuazione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- svolgere un ruolo di primaria interfaccia nella scelta delle dotazioni informatiche, nessuna esclusa, quali hardware di qualsiasi genere, software e qualsiasi altro dispositivo elettronico, e di tutti i processi tecnologici del Titolare, coadiuvando le singole unità organizzative nel processo decisionale sulle suddette dotazioni informatiche;
- svolgere un ruolo di primaria interfaccia, coadiuvando il Titolare del trattamento, il Delegato, i Responsabili e gli altri Amministratori di Sistema interni, se designati, nel caso di incidenti/malfunzionamenti di qualsiasi genere che riguardino la rete, le attrezzature informatiche e l'utenza, e preoccuparsi di erogare una corretta informazione verso gli utenti; dovrà inoltre supportare il processo di indagine e diagnosi dei problemi ed essere in grado di produrre le necessarie informazioni a tal riguardo;
- svolgere un ruolo di primaria interfaccia coadiuvando il Titolare del trattamento, il Delegato, i Responsabili e gli altri Amministratori di Sistema interni, nell'innovazione della struttura IT, proseguendo l'innovazione tecnologica al fine di dotare il Titolare di un moderno Sistema di gestione informatica, ottimizzandone i processi;
- sovrintendere alle operazioni di coordinamento e funzionamento della rete informatica interna;
- eseguire direttamente o assicurarsi che venga fatto da soggetti terzi idoneamente designati le copie di sicurezza e ripristino, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge;
- avere la responsabilità tecnica delle risorse di rete;



- effettuare o assicurarsi che vengano effettuati da soggetti terzi idoneamente designati, interni o esterni all'Organizzazione, interventi di manutenzione hardware e software su sistemi operativi ed applicativi;
- sovrintendere all'operato dei soggetti terzi idoneamente designati in caso di interventi tecnici che abbiano impatto sul sistema informativo e sulla sicurezza del trattamento di dati;
- controllare l'accesso e la protezione dei locali adibiti a contenere database e archivi informatici;
- collaborare con il Titolare del trattamento dei dati alla definizione di idonee regole in ambito di Sicurezza del trattamento dei dati e di Gestione del Sistema Informativo ed alla pianificazione ed attuazione di adeguate attività di sensibilizzazione, istruzione, formazione, addestramento e aggiornamento periodico sulle politiche di sicurezza delle informazioni, in modo pertinente alla specifica attività lavorativa svolta dal personale e dai collaboratori ( a titolo esemplificativo tramite istruzioni, regolamenti, vademecum, incontri formativi);
- predisporre un piano di controlli periodici, da eseguirsi con cadenza adeguata, dell'efficacia delle misure di sicurezza adottate dall'Ente.

L'Amministratore di sistema deve garantire, secondo le procedure definite dal Titolare del trattamento, la comunicazione al Responsabile della Protezione dei dati, qualora venga rilevata una violazione dei dati personali (data breach), ossia una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, e collaborare con il Titolare del trattamento e il Responsabile della Protezione dei dati affinché possano essere attivate le procedure di notifica nelle modalità e nei tempi previsti per legge.

Il soggetto si impegna ad eseguire i compiti affidati, nel rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e delle regole di sicurezza dei dati personali stabilite dall'Ente e dichiara di essere informato che il suo operato in qualità di Amministratore di Sistema sarà sottoposto a verifica da parte del Titolare del trattamento dei dati, anche attraverso l'adozione di sistemi per la registrazione degli accessi logici (autenticazioni informatiche).

Secondo quanto disposto dall'Articolo 5 comma 1) del Regolamento 679/2016/UE i dati personali oggetto del trattamento devono essere:

- trattati in modo lecito corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il loro utilizzo non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati (devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati medesimi sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza di dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti o dalla perdita, dalla distruzione o dal danno accidentali.

Con la presente il soggetto è autorizzato esclusivamente all'accesso e al trattamento dei dati personali oggetto dei trattamenti sopra indicati, nella misura e nei limiti delle mansioni e del ruolo funzionale svolto presso le strutture ed i locali del Titolare del trattamento.

Sistema Socio Sanitario



Regione  
Lombardia

ATS Brescia

**Firma del Titolare del Trattamento  
ATS Brescia**

\_\_\_\_\_

**Firma dell'Amministratore di Sistema**

\_\_\_\_\_