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
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

DECRETO n. 109 del 25/02/2021

Cl.: 1.1.02

OGGETTO: Nuove determinazioni in ordine al "Modello organizzativo privacy" in attuazione del Regolamento (UE) 27 aprile 2016, n. 2016/679.

Il DIRETTORE GENERALE – Dott. Claudio Vito Sileo
nominato con D.G.R. XI/1058 del 17.12.2018

Acquisiti i ***pareri*** del	
DIRETTORE SANITARIO	Dott.ssa Laura Emilia Lanfredini
del	
DIRETTORE SOCIOSANITARIO	Dott.ssa Frida Fagandini
e del	
DIRETTORE AMMINISTRATIVO	Dott.ssa Sara Cagliani

IL DIRETTORE GENERALE

Richiamato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 (di seguito GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
Atteso che detto Regolamento, entrato in vigore il 24 maggio 2016 e direttamente applicabile agli Stati dell'UE dal 25 maggio 2018, ha abrogato la direttiva 95/46/CE; non ha abrogato, invece, né il d.lgs. n. 196/2003 (codice della privacy) nè i provvedimenti del Garante privacy rimasti in vigore, nei limiti della compatibilità e sino ad eventuali differenti e specifichi interventi normativi;
Visto il d.lgs. n. 101 del 10 agosto 2018 (entrato in vigore il 19 settembre 2018) che ha introdotto specifiche disposizioni finalizzate ad armonizzare le norme di cui al codice privacy nazionale con quelle introdotte dal Regolamento europeo ed in particolare l'articolo 22 che detta una disciplina transitoria sino all'adozione dei prescritti provvedimenti del Garante;
Rilevata la necessità, in adeguamento alle disposizioni normative sopra richiamate, di definire un "Modello organizzativo privacy dell'Agenzia di Tutela della Salute di Brescia" attraverso l'individuazione dei soggetti, dei relativi compiti e responsabilità, Modello presentato dal Coordinatore del Gruppo di Lavoro Privacy dell'Agenzia e condiviso nell'Ufficio di Direzione del 29.08.2018;
Richiamato il Decreto D.G. n. 511 del 12.10.2018 con il quale erano state assunte specifiche determinazioni in ordine al "Modello organizzativo privacy" dell'Agenzia di Tutela della Salute di Brescia;
Rilevata la necessità di apportare alcuni correttivi al documento sopra indicato sia in ragione della modifica intervenuta, medio tempore, nella figura del Responsabile della Protezione dei Dati (c.d. Data Protection Officer o DPO) ex articoli 37-39 del GDPR sia per meglio allineare le previsioni ed i compiti delle figure soggettive coinvolte nell'attuazione del GDPR ai contenuti della normativa comunitaria;
Richiamata, pertanto la Determinazione dirigenziale n. 473 del 09.07.2020 con la quale è stato affidato, tra gli altri, il servizio di responsabile per la protezione dei dati alla società Liguria Digitale s.p.a per il periodo dal 24.07.2020 al 23.07.2022;
Richiamata, altresì, la nota DG del 27.04.2017, prot. 40566, con la quale è stato nominato l'Ing. Luca Chinotti quale Responsabile della Sicurezza delle Informazioni;
Vista la proposta della Dott.ssa Francesca Brun, quale titolare della "Funzione di gestione adempimenti in materia di protezione dei dati personali", che attesta, in qualità di Responsabile del procedimento, la regolarità tecnica del presente provvedimento;
Dato atto che dal presente provvedimento non discendono oneri per l'Agenzia;
Acquisiti i pareri del Direttore Sanitario, Dott.ssa Laura Emilia Lanfredini, del Direttore Sociosanitario, Dott.ssa Frida Fagandini 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 costituire ed approvare, per le motivazioni di cui in premessa, il seguente "Modello organizzativo privacy dell'Agenzia di Tutela della Salute di Brescia" in sostituzione di quello formalizzato con Decreto D.G. n. 511 del 12.10.2018:
   Titolare del trattamento dei dati personali (art. 24 GDPR): Agenzia di Tutela della Salute di Brescia nella persona del suo Rappresentante legale pro tempore;

Delegati al trattamento dei dati personali, quali soggetti interni all'Agenzia, ai quali sono attribuiti, con apposito atto, dal Titolare e sotto la sua responsabilità specifici compiti e funzioni connessi al trattamento di dati personali (art. 2 *quaterdecies* D.Lgs. 196/2003): Dirigenti titolari di struttura semplice e complessa, Direttori di Dipartimento e Direttori della Direzione Strategica per i rispettivi ambiti di competenza; Direttore del Servizio Pianificazione e Controllo in riferimento al trattamento dei dati da parte della Direzione Generale;

Autorizzati al trattamento dei dati personali, quali soggetti (dipendenti, tirocinanti, borsisti, personale somministrato, volontari, titolari di incarico gratuito, corsisti dei Corsi di Laurea, titolari di incarichi libero professionali e di collaborazione coordinata e continuativa che agiscono senza mezzi propri – personal computer e altre applicazioni di ATS, svolgimento dell'attività presso le sedi di ATS) che all'interno di ciascuna Struttura/Ufficio di ATS trattano dati personali sotto la diretta autorità dei Delegati al trattamento (art. 4 p.10 e 29 GDPR) e previa nomina da parte di questi;

sono altresì autorizzati al trattamento:

- Collegio Sindacale, organo di controllo previsto dall'articolo 3 ter del D.Lgs. n. 502/1992 e dalla L.R. n. 33/2009 all'articolo 12;
- Nucleo di Valutazione delle Prestazioni, organismo indipendente, costituito per le finalità ed i compiti di cui all'articolo 18 bis della L.R. n. 33/2009 in materia, per lo più, di valutazione del personale dipendente e di misurazione della performance organizzativa dell'Agenzia;
- Ufficio di Pubblica Tutela, ufficio indipendente, previsto dalla DGR n. 10884/2009, preposto alla tutela delle istanze sociali e civili dei cittadini per assicurare effettività dei diritti di informazione, rispetto delle libertà e della dignità personali;
- Consigliere di fiducia, figura soggettiva, prevista dalle Raccomandazioni della Commissione Europea e dalla Direttiva n. 2/2019 della Presidenza del Consiglio dei Ministri, posta a protezione della dignità personale e professionale dei dipendenti;

Amministratori di Sistema, quali figure previste dal Provvedimento del Garante del 27.11.2008 autorizzate al trattamento di dati personali per la gestione dei sistemi informativi/informatici e nominati dal Titolare;

Responsabile della sicurezza delle informazioni, figura richiesta da Regione Lombardia per il tramite di Lombardia Informatica (nota 30.03.2017, Atti ATS prot. n. 31232 del 31.03.2017) quale responsabile del coordinamento, dello sviluppo del mantenimento e del monitoraggio del programma di sicurezza delle informazioni dell'Agenzia, già individuato nell'Ing. Luca Chinotti con nota del 27.04.2017, prot. n. 40566;

Responsabile della protezione dei dati ("DPO/RPD"), quale figura di garanzia del rispetto della normativa privacy nell'ambito dell'Agenzia (art. 37 GDPR): servizio affidato alla società Liguria Digitale s.p.a. con Determinazione dirigenziale n. 473 del 09.07.2020 per il periodo dal 24.07.2020 al 23.07.2022;

Responsabili esterni al trattamento dei dati personali, quali soggetti esterni all'Agenzia (es. fornitori di beni e servizi, esecutori di lavori, titolari di incarichi libero professionali e di collaborazione coordinata e continuativa che utilizzano mezzi di trattamento propri – personal computer, archivi, svolgimento attività non presso sedi ATS) che trattano dati personali per conto del Titolare (art. 28 Reg. UE) e da questi nominati con specifico atto;

Titolari autonomi del trattamento (art. 24 GDPR) in ragione degli ampi poteri di azione e di controllo senza alcuna subordinazione al Titolare del Trattamento Agenzia di Tutela della Salute di Brescia:
- Avvocati del libero foro incaricati per attività stragiudiziale o di patrocinio legale (compresi eventuali incarichi per mediazione o accertamento tecnico preventivo o situazioni assimilabili caratterizzati da spiccata autonomia professionale e gestoria);
- Altre professioni liberali (es. ingegnere);

b) di approvare i seguenti modelli di nomina allegati al presente provvedimento:
- Delegato al trattamento di dati personali (Mod_Delegato 1/2021 di n. 5 pagine);
- Autorizzato al trattamento di dati personali (Mod_Autorizzato 1/2021 di n. 4 pagine);
- Amministratore di Sistema e di Rete dei server dell'Agenzia (Mod_Amministratore_di_Sistema 1/2021 di n. 17 pagine);
- Responsabile esterno al trattamento dei dati personali (Mod_Resp_Esterno 1/2021 di n. 18 pagine);

c) di demandare:
- in fase di prima applicazione alla Responsabile della "Funzione di gestione adempimenti in materia di protezione dei dati personali" ogni incombenza in ordine alla nomina, da parte del Titolare, dei Dirigenti titolari di struttura semplice e complessa, dei Direttori di Dipartimento quali Delegati al trattamento dei dati personali;
- al Direttore del Servizio Gestione Personale e Sviluppo Professionale ogni incombenza in ordine alla nomina, da parte del Titolare, dei Delegati al trattamento dei dati personali con riguardo a nuovi incarichi di direzione di struttura semplice, complessa e di dipartimento;
- al Direttore del Servizio Affari Generali e Legali ogni incombenza in ordine alla nomina, da parte del Titolare, dei Direttori della Direzione Strategica quali Delegati al trattamento dei dati personali;
- ad ogni Dirigente che verrà designato Delegato al trattamento di dati personali ogni incombenza in ordine alla nomina dei soggetti Autorizzati al trattamento;
- al Direttore del Servizio ICT e della U.O. Gestione Acquisti e Patrimonio ogni incombenza in ordine alla nomina, da parte del Titolare, degli Amministratori di Sistema;
- ad ogni Dirigente delegato in ragione dei rispettivi ambiti di competenza ogni incombenza in ordine alla predisposizione della documentazione atta alla designazione, da parte del Titolare, dei Responsabili esterni del trattamento (es. fornitori di beni e servizi, esecutori di lavori, titolari di incarichi libero professionali e di collaborazione coordinata e continuativa che utilizzano mezzi di trattamento propri – personal computer, archivi, svolgimento attività non presso sedi ATS);

d) di precisare che l'atto di nomina a Delegato al trattamento, Autorizzato al trattamento e Amministratore di Sistema debba essere conservato nel fascicolo personale dei dipendenti;

e) di pubblicare a cura della "Funzione di gestione delle relazioni interne ed esterne" il presente provvedimento nella sezione Privacy del sito web istituzionale;

f) di dare atto 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 del Servizio Affari Generali e Legali, la pubblicazione all'Albo on-line – 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

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Cl 1.7.03
Prot. n. _____del_____
Brescia

Oggetto: Nomina "Delegato al trattamento" dei dati personali ai sensi del Regolamento UE 2016/679 e del D.Lgs. n. 196/2003.

Egr. Sig.Dott./Gent.ma Sig.ra/Dott.ssa_____

Il Regolamento Europeo in materia di Dati Personali 2016/679 (di seguito anche Regolamento UE), stabilisce che il trattamento dei dati personali si debba svolgere nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, quale diritto fondamentale previsto dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea

VISTI

il Regolamento UE, con particolare riferimento agli artt. 4, n. 10 e 29 e l'art. 2-quaterdecies del D.Lgs. n. 196/2003 come novellato, da ultimo con D.Lgs. n. 101/2018

CONSIDERATO

che lo scrivente in qualità di Titolare del trattamento, Direttore Generale dell'Agenzia di Tutela della Salute di Brescia (di seguito ATS), ritiene che la S.V. abbia, per l'ambito di attribuzioni, funzioni e competenze conferite, i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza, la nomina

SOGGETTO DELEGATO AL TRATTAMENTO DI DATI PERSONALI

In qualità di Soggetto Delegato al trattamento dei dati personali (di seguito Delegato di Struttura), ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè di attenersi alle seguenti istruzioni impartite dal Titolare

PRINCIPI GENERALI DA OSSERVARE

in qualità di Delegato di Struttura, dovrà assicurare che nel corso del trattamento i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- raccolti e registrati per scopi determinati, espliciti e legittimi e successivamente trattati in modo compatibile con tali finalità
- conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione secondo le vigenti norme, anche regionali
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- esatti e se necessario aggiornati

Durante lo svolgimento del suo incarico dovranno essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati, in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita dalla distruzione o dal danno accidentale, mediante misure organizzative e tecniche adeguate.

Al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, in qualità di Delegato di Struttura dovrà osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti

In qualità di Delegato di Struttura è tenuto alla completa riservatezza sui dati di cui sia venuto a conoscenza in occasione dell'espletamento della sua attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal titolare del trattamento, nei soli casi previsti dalla legge e nello svolgimento dell'attività istituzionale dell'Agenzia

COMPITI PARTICOLARI DEL DELEGATO DI STRUTTURA

In qualità di Delegato di struttura, dovrà adempiere ai seguenti compiti:

- 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 dell'Agenzia;
- collaborare con il Titolare nel predisporre ed aggiornare il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità
- 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;
- collaborare con il Titolare nel condurre ogni valutazione atta a verificare la necessità dell'effettuazione della valutazione d'impatto sui trattamenti di competenza;
- ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati.
- adottare, tramite il supporto del Responsabile del Servizio ICT, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- attenersi alle previsioni previste da ATS in ordine alle procedure di *"data breach"* ed alle "richieste di esercizio dei diritti degli interessati";
- 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 il trattamento dei dati; assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- far osservare gli adempimenti previsti in caso di nuovi trattamenti e archiviazione di trattamenti;
- individuare, tra i propri collaboratori, 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 nonchè l'osservanza da parte degli stessi, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- gestire ogni adempimento istruttorio finalizzato alla formalizzazione della nomina, da parte del Titolare, di un Responsabile esterno al trattamento dei dati personali (art. 28 Reg. UE).

Il Delegato di Struttura risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

L'incarico di Delegato di Struttura è attribuito personalmente e non è suscettibile di delega.

Il rispetto e l'osservanza di quanto contenuto nella presente autorizzazione sono strettamente connessi al ruolo ricoperto all'interno dell'organizzazione aziendale.
Il non adempimento di quanto previsto nella presente autorizzazione può dare luogo, oltre ad altre forme di responsabilità, a sanzioni disciplinari.

Si ricorda che ai fini del Regolamento UE e del D.Lgs. n. 196/2003 e s.m.i., si intende:
- per Regolamento UE 2016/679 (GDPR), il Regolamento Generale per la Protezione dei dati che modifica l'approccio alla privacy in termini di maggiore tutela degli interessati, responsabilizzazione delle aziende ed inasprimento del sistema sanzionatorio;
- per Garante per la Protezione dei Dati Personali, l'Autorità amministrativa indipendente istituita da uno Stato al fine di assicurare la tutela dei diritti, delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali;
- per "Trattamento", qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali;
- per "Dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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; costituiscono dati personali anche quelli relativi a condanne penali o reati;

- per "Dato particolare", qualunque dato personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici o biometrici intesi a identificare univocamente l'interessato, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- per "Titolare del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- per "Responsabile esterno del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento e al quale il titolare assegna compiti di gestione o controllo sui dati personali fornendone le istruzioni e monitorando l'attività;
- per "Soggetto Autorizzato al trattamento", la persona fisica, facente parte dell'organizzazione aziendale, autorizzata a compiere operazioni di trattamento dal Titolare, dal Delegato o dal Responsabile e su istruzioni degli stessi;
- per "Delegato al trattamento", la persona fisica che viene designata dal Titolare o dal Responsabile del trattamento, sotto la loro responsabilità e nell'ambito del loro assetto organizzativo, all'esercizio di specifici compiti e funzioni connessi al trattamento di dati personali;
- per "Amministratore di sistema", la figura professionale, designata dal Titolare o dal Responsabile dedicata alla gestione e alla manutenzione di impianti informatici con cui vengono trattati dati personali, tra questi: sistemi di gestione dei database, software complessi, reti locali;
- per "Registro dei trattamenti", il registro indicante le attività di trattamento poste in essere per volere del Titolare/Responsabile del trattamento. Si tratta di uno strumento utile a comprovare la correttezza dell'operato dell'organizzazione;
- per "Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD)", la nuova figura di riferimento introdotta dal GDPR che ha la funzione di affiancare Titolare, Delegati, Responsabili e Autorizzati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo;
- per "Privacy by Design and by Default", l'obbligo di strutturare tutti i nuovi processi, servizi e prodotti aziendali in conformità alla normativa sulla Privacy sin dalla loro fase di progettazione;
- per "Data Protection Impact Assessment (DPIA)", l'obbligo di effettuare una valutazione d'impatto sui trattamenti di dati ad alto rischio;
- per "Misure di sicurezza adeguate", l'obbligo di adottare adeguate misure di sicurezza in base al livello di rischio rilevato;
- per "Data Breach", l'obbligo di registrare e di notificare all'Autorità di controllo tutte le violazioni di dati personali subite.

Per tutto quanto non espressamente previsto nel presente documento, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Il titolare del trattamento

ATS Brescia – Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.ats-brescia.it
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

Dott. Claudio Vito Sileo

Per presa visione ed accettazione
Data __/__/_____
Il Responsabile U.O.- Il Direttore del Servizio/Dipartimento
_____

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Cl 1.7.03
Prot. n. _____del_____
Brescia

Oggetto: Nomina "Soggetto Autorizzato al trattamento" dei dati personali ai sensi del Regolamento (UE) 2016/679.

Egr. Sig.Dott./Gent.ma Sig.ra/Dott.ssa_____

Il Regolamento Europeo in materia di Dati Personali 2016/679 (di seguito anche Regolamento UE), stabilisce che il trattamento dei dati personali si debba svolgere nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, quale diritto fondamentale previsto dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

VISTI

il Regolamento UE in materia di dati personali, con particolare riferimento agli artt. 4, n. 10 e 29 ed il D.Lgs. n. 196/2003 come novellato, da ultimo con D.Lgs. n. 101/2018

CONSIDERATO

che lo scrivente in qualità di (Rif. a Responsabile/Direttore U.O., Servizio, Dipartimento _____ dell'Agenzia di Tutela della Salute di Brescia (di seguito ATS), ricopre la funzione di Delegato al trattamento (di seguito Delegato di Struttura) ai sensi dell'articolo 2 quaterdecies d.lgs. 196/2003 e s.m.i., nomina la S.V. ai sensi e per gli effetti dell'art. 29 Regolamento UE

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

che Le sono comunicati e che Lei tratta durante lo svolgimento della Sua attività lavorativa, esclusivamente nei limiti delle mansioni a Lei affidate ed alle banche dati alle quali Lei è autorizzato ad accedere.

A tal fine la S.V. può consultare il Registro dei trattamenti pubblicato sul sito web dell'Agenzia alla Sezione Privacy.

In relazione alla nomina conferitale, la S.V. nell'espletamento delle proprie mansioni dovrà attenersi agli obblighi di riservatezza e di sicurezza imposti dal Regolamento UE, nonché alle specifiche istruzioni che saranno di volta in volta impartite dal Titolare e/o dal Delegato di Struttura.

Si richiamano, di seguito, le principali prescrizioni che la S.V tenuta a rispettare:

- trattare i dati personali che verranno comunicati in modo lecito e corretto, mantenendo assoluto riserbo sui dati stessi;
- utilizzare le sole banche dati ed i soli strumenti per i quali è stata preventivamente autorizzata ad utilizzare;
- trattare esclusivamente i dati necessari allo svolgimento della mansione lavorativa e non trattare al di fuori degli impegni lavorativi;
- non lasciare incustoditi o accessibili a terzi non autorizzati gli strumenti elettronici mentre è in corso una sessione di lavoro;
- custodire e non divulgare né cedere a terzi le proprie credenziali di autenticazione;

- procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni della consultazione;
- è fatto assoluto divieto di asportare i supporti informatici o cartacei contenenti dati personali degli Interessati, senza la preventiva autorizzazione del Titolare e/o dal Delegato di Struttura;
- osservare scrupolosamente tutte le misure di sicurezza già predisposte, o che saranno successivamente comunicate dal Titolare e/o dal Delegato di Struttura, in particolare per quanto riguarda i trattamenti dalla S.V. effettuati;
- non modificare i trattamenti in essere senza specifica indicazione del Titolare e/o del Delegato di Struttura;
- rispettare tutte le misure di sicurezza previste per poter garantire la confidenzialità, disponibilità, integrità dei dati trattati;
- informare il Titolare e/o il Delegato di Struttura nel caso si verifichino incidenti relativi alla sicurezza delle informazioni trattate;
- rispettare il "Regolamento per l'utilizzo dei sistemi informatici aziendali" di cui al Decreto DG ASL n. 179/2013 (in particolare i paragrafi 6 e da 8 a 11);
- attenersi alle istruzioni di seguito esplicitate in ordine all'utilizzo dei documenti cartacei contenenti dati personali:
    - stampare dati personali solo se strettamente necessario per l'esecuzione dei trattamenti
    - custodire il materiale cartaceo contenente dati personali e aziendali affinché nessuno ne prenda visione, possa manipolarlo o riprodurlo
    - custodire il materiale cartaceo contenente categorie particolari di dati personali in archivi e/o stanze dotati/e di chiusura a chiave
    - non lasciare documenti incustoditi presso la propria postazione (o comunque altre scrivanie, tavoli di lavoro) qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi non autorizzati
    - affidare i documenti oggetto di trattamento soltanto a soggetti appositamente autorizzati
    - custodire i dati oggetto del trattamento in luoghi non accessibili a personale non autorizzato
    - distruggere il materiale cartaceo in maniera corretta utilizzando l'apposito trita documenti oppure "stracciando" il materiale in modo da non rendere comprensibile il contenuto del documento. Nessuna pratica deve essere gettata nel cestino prima di averla distrutta secondo le modalità sopra indicate. (Es. se la fotocopia di un documento che contiene dati personali è "storta", se è troppo scura o se non si legge a sufficienza, non deve essere gettata nel cestino prima di averla distrutta)
    - adottare e rispettate le seguenti regole di "scrivania pulita": al termine del lavoro o durante lunghe pause, non deve essere lasciata alcuna documentazione riservata sulle scrivanie (documentazione cartacea) o su supporti rimovibili (documentazione digitale)."

Richieste non conformi o non adeguate rispetto all'incarico ricevuto dovranno essere prontamente segnalate al Titolare e/o al Delegato di Struttura.

Si fa presente che il Titolare e/o il Delegato di Struttura, anche tramite verifiche periodiche, hanno l'onere di esaminare la correttezza dell'operato della S.V.

Il rispetto e l'osservanza di quanto contenuto nella presente autorizzazione sono strettamente connessi al ruolo ricoperto all'interno dell'organizzazione aziendale.
Il non adempimento di quanto previsto nella presente autorizzazione può dare luogo, oltre ad altre forme di responsabilità, a sanzioni disciplinari.

Si ricorda che ai fini del Regolamento UE e del D.Lgs. n. 196/2003 e s.m.i., si intende:

- per Regolamento UE 2016/679 (GDPR), il Regolamento Generale per la Protezione dei dati che modifica l'approccio alla privacy in termini di maggiore tutela degli interessati, responsabilizzazione delle aziende ed inasprimento del sistema sanzionatorio;
- per Garante per la Protezione dei Dati Personali, l'Autorità amministrativa indipendente istituita da uno Stato al fine di assicurare la tutela dei diritti, delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali;
- per "Trattamento", qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali;
- per "Dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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; costituiscono dati personali anche quelli relativi a condanne penali o reati;
- per "Dato particolare", qualunque dato personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici o biometrici intesi a identificare univocamente l'interessato, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- per "Titolare del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- per "Responsabile esterno del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento e al quale il titolare assegna compiti di gestione o controllo sui dati personali fornendone le istruzioni e monitorando l'attività;
- per "Soggetto Autorizzato al trattamento", la persona fisica, facente parte dell'organizzazione aziendale, autorizzata a compiere operazioni di trattamento dal Titolare, dal Delegato o dal Responsabile e su istruzioni degli stessi;
- per "Delegato al trattamento", la persona fisica che viene designata dal Titolare o dal Responsabile del trattamento, sotto la loro responsabilità e nell'ambito del loro assetto organizzativo, all'esercizio di specifici compiti e funzioni connessi al trattamento di dati personali;
- per "Amministratore di sistema", la figura professionale, designata dal Titolare o dal Responsabile dedicata alla gestione e alla manutenzione di impianti informatici con cui

vengono trattati dati personali, tra questi: sistemi di gestione dei database, software complessi, reti locali;
- per "Registro dei trattamenti", il registro indicante le attività di trattamento poste in essere per volere del Titolare/Responsabile del trattamento. Si tratta di uno strumento utile a comprovare la correttezza dell'operato dell'organizzazione;
- per "Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD)", la nuova figura di riferimento introdotta dal GDPR che ha la funzione di affiancare Titolare, Delegati, Responsabili e Autorizzati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo;
- per "Privacy by Design and by Default", l'obbligo di strutturare tutti i nuovi processi, servizi e prodotti aziendali in conformità alla normativa sulla Privacy sin dalla loro fase di progettazione;
- per "Data Protection Impact Assessment (DPIA)", l'obbligo di effettuare una valutazione d'impatto sui trattamenti di dati ad alto rischio;
- per "Misure di sicurezza adeguate", l'obbligo di adottare adeguate misure di sicurezza in base al livello di rischio rilevato;
- per "Data Breach", l'obbligo di registrare e di notificare all'Autorità di controllo tutte le violazioni di dati personali subite.

Si ricorda, altresì, che la responsabilità in ordine alla gestione di eventuali copie analogiche/cartacee di documenti digitali – se non accuratamente conservate – è in capo alla S.V.

Gli obblighi relativi al mantenimento della confidenzialità delle informazioni trattate, dovranno essere osservati anche in caso di modifica dell'incarico e/o cessazione del rapporto di lavoro.

Firma del Delegato al trattamento

_____

Per presa visione ed accettazione
Data __/__/____
Firma dell'Autorizzato
_____

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Cl 1.7.03
Prot. n. _____del_____

Oggetto: **Nomina autorizzato al trattamento quale "Amministratore di sistema" ai sensi ai sensi del Regolamento (UE) 679/2016 e del Provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - del 27 novembre 2008 e successive modifiche" del Garante privacy.**

Egr. Sig.Dott./Gent.ma Sig.ra/Dott.ssa_____

PREMESSO CHE

- il Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "Regolamento"), che abroga la Direttiva 95/46/CE e le implementazioni della stessa, fissa le modalità da adottare ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dal Regolamento;
- il considerando 171 del Regolamento prevede che le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate;
- l'Autorità di Controllo italiana (Garante per la protezione dei dati personali) ha introdotto con provvedimento del 27 novembre 2008, come successivamente modificato con provvedimento del 25 giugno 2009 ("Provvedimento Amministratori di Sistema"), una serie di obblighi per il Titolare del Trattamento concernenti l'individuazione e la designazione di Persone Autorizzate che svolgono all'interno dell'Agenzia di Tutela della Salute di Brescia (di seguito ATS) il ruolo di amministratore di sistema, così come definito nel provvedimento richiamato;
- l'osservanza di tali obblighi costituisce una misura di sicurezza che ATS è tenuta ad osservare e la cui inosservanza può determinare conseguenze sanzionatorie di tipo amministrativo come anche responsabilità civilistica;
- ATS è tenuta all'osservanza ed all'applicazione delle prescrizioni della Circolare Agid 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni;
- deve essere considerato Amministratore di sistema chiunque, in maniera non occasionale, si occupa della gestione e della 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 (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire, anche accidentalmente, sui Dati Personali;
- le mansioni della Persona Autorizzata in epigrafe svolte all'interno di ATS richiedono la preventiva autorizzazione al trattamento dei dati personali in qualità di Amministratore di Sistema;
- l'autorizzazione ad operare in qualità di Amministratore di Sistema è individuale e deve indicare in maniera analitica gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato all'Amministratore di Sistema;

- tutte le operazioni di login, logout e tentativi di login ai sistemi informativi aziendali effettuati dall'Amministratore di Sistema saranno tracciati in osservanza del Provvedimento e i relativi log saranno resi inalterabili;
- si intende, pertanto, procedere all'individuazione e autorizzazione al trattamento dei dati personali della persona in epigrafe in qualità di amministratore di sistema;

TUTTO CIÒ PREMESSO

ATS, quale Titolare del trattamento, autorizza la Persona in epigrafe al trattamento dei dati personali in qualità di "Amministratore di Sistema" ai sensi del citato Provvedimento, impartendole i seguenti obblighi, in funzione del ruolo ricoperto, del profilo attribuito in Allegato 1, parte integrante della presente autorizzazione, e nell'ambito delle attività assegnatele per lo svolgimento del suo lavoro:

a) osservare scrupolosamente le regole di utilizzo dei sistemi di tracciamento delle operazioni degli amministratori di sistema posti in essere da ATS e in adempimento al citato Provvedimento;
b) segnalare qualsiasi anomalia di funzionamento in merito alla sicurezza, disponibilità e riservatezza dei dati personali al DPO aziendale avvisando il proprio superiore gerarchico e il Delegato di Struttura (Direttore Servizio ICT/Responsabile UO Gestione Acquisti e Patrimonio);
c) collaborare alla verifica periodica dell'attività di Amministrazione di Sistema fatta da ATS o dal DPO;
d) osservare le ulteriori istruzioni impartite da ATS per il tramite del relativo Delegato di Struttura per un corretto svolgimento dell'attività di Amministratore di Sistema.

E' compito dell'Amministratore di sistema (intendendo con tale termine l'amministratore del sistema operativo, l'amministratore del sistema database, l'amministratore di rete, l'amministratore di sottosistema applicativo complesso o una combinazione delle precedenti funzioni tecniche), in funzione del ruolo ricoperto, del profilo attribuito in Allegato 1, parte integrante della presente autorizzazione, e nell'ambito delle attività assegnatele per lo svolgimento del suo lavoro:

a) Attivarsi per tutelare, nei limiti delle proprie competenze e capacità professionali, la protezione dei dati, il buon funzionamento dei sistemi e la continuità operativa dei medesimi;
b) Seguire le indicazioni aziendali su quanto contenuto nel provvedimento del Garante in merito a "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008";
c) Applicare le regole di gestione dei sistemi medesimi e le misure di sicurezza minime ed idonee individuate o comunque comunicate da ATS;
d) Monitorare, ove possibile, le risorse di sistema operativo e le basi dati in modo tale da garantire l'efficienza del sistema tecnologico e l'aderenza delle configurazioni ai profili di autorizzazione stabiliti;
e) Assegnare e gestire, ove possibile gli identificativi di utente, in modo che siano univoci sul sistema e quindi adeguati ad identificare l'utente che accede ed opera sul sistema;
f) Predisporre, ove possibile i meccanismi di corretta gestione delle parole chiavi;
g) Predisporre, ove non già presenti ed attivati, meccanismi di protezione da accessi indesiderati e meccanismi di protezione nei confronti di attacchi da virus;

h) Facilitare il processo di registrazione degli accessi degli amministratori, ove possibile, verificando la predisposizione dei sistemi gestiti a tale attività, evitando ogni operazione che possa inficiare detta raccolta;
i) Segnalare i sistemi per i quali non è possibile procedere agli aggiornamenti di sicurezza al DPO aziendale, avvisando il proprio superiore gerarchico e il Delegato di Struttura;
j) Individuare, nei limiti del possibile, accessi indebiti ai sistemi; in tale caso attivare immediatamente la procedura di Gestione degli incidenti di sicurezza e di Gestione delle violazioni di dati personali;
k) Attuare, nell'ambito delle proprie mansioni e degli incarichi ricevuti, tutte le iniziative che contribuiscano a fare in modo che i dati personali oggetto di trattamento vengano trattati in modo lecito e secondo correttezza;
l) Evitare, ove non strettamente indispensabile per lo svolgimento delle operazioni tecniche connesse al proprio ruolo, di entrare in contatto, visualizzare, maneggiare o mettere a rischio dati personali;
m) Segnalare eventuali usi scorretti o impropri dei sistemi da parte dei tecnici che operano, a vario titolo, sul sistema e sulle sue componenti periferiche e da parte di altre persone autorizzate; attivare nell'evenienza la procedura di gestione delle violazioni di dati personali;
n) Richiedere ed utilizzare soltanto i dati necessari alla normale attività lavorativa adottando le necessarie cautele nel caso si tratti di categorie particolari di dati personali e dati personali relativi a condanne penali e reati;
o) Custodire i dati oggetto del trattamento in luoghi non accessibili a soggetti non autorizzati;
p) Non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;
q) Non lasciare incustoditi e accessibili a terzi gli strumenti elettronici mentre è in corso una sessione di lavoro;
r) Conservare e custodire le chiavi di accesso agli archivi cartacei con la massima cura e non lasciarle incustodite al fine di garantire che l'accesso all'archivio sia consentito solo ai soggetti autorizzati;
s) Procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti informatici da lei eventualmente utilizzati una volta terminate le ragioni di consultazione (in particolare gli archivi cartacei contenenti categorie particolari di dati personali o dati personali relativi a condanne penali o reati dovranno essere chiusi a chiave);
t) Custodire e non divulgare la propria password di amministratore per l'accesso agli strumenti elettronici;
u) Accertarsi che i terzi abbiano l'autorizzazione per l'uso dei dati richiesti;
v) Accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
w) Non fornire telefonicamente, a mezzo fax o per via telematica dati senza specifica autorizzazione e/o identificazione del richiedente;
x) Comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare e/o dal Delegato di Struttura;
y) Limitare l'accesso ai dati all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro (comprendendo nell'orario i periodi di reperibilità o altre attività specificatamente autorizzate dal proprio responsabile gerarchico);
z) Nel caso si verifichi un incidente di sicurezza e si sospetti una violazione di dati personali (Data Breach) attivare immediatamente la procedura aziendale di Gestione degli incidenti di sicurezza e Gestione delle violazioni;

aa) Accertarsi che le informazioni riportate nel Registro dei Trattamenti e relativi ai sistemi/applicazioni di propria competenza siano aggiornate, con particolare riguardo a:
   a. Supporti
   b. Misure di sicurezza da applicare
   c. Impatti prevedibili sugli interessati

L'autorizzato deve eseguire tutte le operazioni di trattamento di dati personali, attenendosi alle istruzioni impartite dal Titolare o dal Delegato di Struttura. L'autorizzazione è effettuata in relazione a tutte le operazioni di trattamento dei dati, censite nel Registro dei Trattamenti, che siano strettamente necessarie per adempiere ai compiti assegnati in relazione alle attività svolte nell'ambito della Struttura di appartenenza e per le finalità strettamente pertinenti all'esecuzione della prestazione lavorativa.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico ricevuto.
Nel caso di cessazione dall'attività lavorativa, Lei non sarà più autorizzato ad effettuare alcun tipo di trattamento sui dati.
Sono parte integrante delle istruzioni impartite mediante questa autorizzazione al trattamento dei dati personali in qualità di Amministratore di Sistema: le procedure "Gestione dei beni aziendali informatici", "Gestione delle violazioni di dati personali" e "Gestione dell'esercizio dei diritti dell'Interessato", pubblicate sul sito internet di ATS – sezione Privacy.
Ogni dipendente ha il dovere di prenderne visione e conoscerne il contenuto.
Tale documentazione è oggetto di aggiornamenti periodici; pertanto si raccomanda di controllare costantemente la documentazione in materia di privacy e sicurezza sul sito di ATS.
Il Delegato di Struttura potrà impartire ulteriori e specifiche istruzioni che saranno allegate alla presente nomina.
Per qualsiasi altra informazione o dubbio è possibile rivolgersi al suo Superiore gerarchico, al Delegato di Struttura, nonché al DPO aziendale.
Le ricordiamo infine che il provvedimento del Garante sopracitato, obbliga l'Amministrazione alla "verifica" almeno annuale delle attività svolte dall'Amministratore di Sistema in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalla normativa vigente.

Il rispetto e l'osservanza di quanto contenuto nella presente autorizzazione sono strettamente connessi al ruolo ricoperto all'interno dell'organizzazione aziendale.
Il non adempimento di quanto previsto nella presente autorizzazione può dare luogo, oltre ad altre forme di responsabilità, a sanzioni disciplinari.

La presente autorizzazione annulla e sostituisce le precedenti nomine Privacy.

TITOLARE DEL TRATTAMENTO
DIRETTORE GENERALE
Dott. Claudio Vito Sileo

PERSONA AUTORIZZATA/AMMINISTRATORE DI SISTEMA
Sig./Sig.ra – Dott./Dott.ssa_____

Brescia _____

Allegato 1: Amministratore di Sistema – ambiti di operatività.

La sua autorizzazione comprende i seguenti profili e piattaforme:

Profilo	**Tecnologia**	**Autorizzato**
Sistemista	Gestione sistemi, application server e storage	SI/NO
Apparati di rete e sicurezza perimetrali	Networking (Gestione infrastruttura di Rete)	SI/NO
Gestione Database	Database (Gestione base dati)	SI/NO
Cybersecurity	Cybersecurity (Gestione e monitoraggio strumenti di sicurezza informatica)	SI/NO
Gestione Back up	Back up e Restore	SI/NO
Gestione Client e stampanti	Gestione Client, stampanti, fonia e VDC	SI/NO
Infrastruttura tecnologica	Gestione e monitoraggio Infrastruttura Data Center	SI/NO
Gestione impianto di Videosorveglianza	Videosorveglianza	SI/NO
Assistenza	Assistenza tecnica applicazioni	SI/NO
Sviluppatore	Progettista e Sviluppatore di applicazioni	SI/NO
Tester	Progettista ed esecutore di test per applicazioni	SI/NO

ATS Brescia – Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.ats-brescia.it
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

Tutte le risorse in possesso o meno di un profilo specifico

Tali istruzioni valgono per tutte le figure che non rientrano pienamente nei profili specifici di seguito individuati e nella misura in cui risultano concretamente applicabili al profilo indicato.

Ella dovrà attenersi pertanto alle seguenti istruzioni, in funzione del ruolo ricoperto e nell'ambito delle attività assegnate per lo svolgimento del suo lavoro:

1. Installare unicamente software autorizzati, ovvero:
    1. Utili allo svolgimento della propria attività lavorativa;
    2. Distribuiti ufficialmente dalle società che ne detengono i diritti e che producano aggiornamenti di sicurezza almeno una volta l'anno;
    3. Che non siano comprese nell'elenco delle tipologie di sw non autorizzato (Cfr. Blacklist);
    4. Su esplicita indicazione del Titolare e del Delegato di Struttura;
    5. Nei limiti delle licenze in possesso di ATS:
        I. Di cui si è certi che ATS abbia la relativa licenza nella configurazione e nelle quantità idonee oppure;
        II. Software che non necessiti di licenza a pagamento per uso aziendale.
2. Chi installa e gestisce (amministra) un sw (applicativo o di ambiente) si prende la responsabilità di seguire costantemente gli aggiornamenti (vulnerabilità, fine del supporto) del SW installato;
3. Per i Software amministrati, monitorare l'emissione di aggiornamenti (vulnerabilità, fine del supporto e fine vita) e gli annunci di fine vita dei prodotti gestiti, tramite la sottoscrizione dei servizi di notifica applicabili, e comunque almeno trimestralmente verificare la disponibilità di aggiornamenti e la fine vita dei prodotti.
4. Segnalare la disponibilità degli aggiornamenti (vulnerabilità, fine del supporto e fine vita) al DPO aziendale per concordare un piano di aggiornamento nei limiti temporali previsti mettendo a conoscenza, a proprio giudizio, il proprio responsabile gerarchico e il Delegato di Struttura; Rimuovere i software amministrati non più utili e che non rispettano più le condizioni per l'installazione;
5. Monitorare, ove possibile, il corretto funzionamento dei servizi erogati tramite la verifica dei log e dei messaggi prodotti dal sistema/applicazioni e dei sistemi di diagnostica applicabili;
6. Segnalare eventuali problematiche dei sistemi o situazioni anomale al proprio responsabile gerarchico;
7. Intervenire prontamente in situazioni di emergenza o in caso di manutenzione ordinaria o straordinaria, seguendo, per quanto necessario, gli interventi relativi;
8. Cooperare all'installazione dei sistemi e al monitoraggio della loro continuità operativa e della fruibilità continuativa dei servizi da parte degli utenti, alla verifica delle funzionalità delle interfacce e attivare/disattivare i singoli processi software per garantire detta continuità di servizio in relazione agli specifici contesti operativi;

9. Effettuare operazioni di tuning dei parametri di configurazione del sistema/applicazione gestito applicando il principio del privilegio minimo e della minimizzazione dei servizi erogati, per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità di gestione ed il mantenimento nel tempo delle funzioni; Provvedere, su richiesta del Titolare o del Delegato di Struttura, alla gestione delle credenziali di autenticazione e alla modifica o disattivazione delle utenze (ad es. User ID e PW) su cui dovesse risultare qualche problema;
10. Inviare ai soggetti deputati all'autorizzazione delle persone autorizzate, secondo quanto definito nelle procedure aziendali, l'elenco degli utenti del sistema/applicazione e delle relative autorizzazioni per consentire la verifica dell'autorizzazione;
11. Definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dai soggetti deputati all'autorizzazione delle persone autorizzate;
12. Custodire tutti i supporti di memorizzazione contenenti dati personali sotto chiave;
13. Non lasciare mai la propria postazione di lavoro incustodita e, in caso di allontanamento, provvedere a bloccare la postazione prima di allontanarsi dal proprio posto di lavoro;
14. Segnalare eventuali interventi ritenuti necessari per migliorare gli aspetti legati alla sicurezza dei dati, al trattamento e alla loro conservazione al DPO aziendale, avvisando il proprio responsabile gerarchico e Delegato di Struttura. Tali migliorie verranno vagliate dalle strutture tecniche e comunicate al Titolare.
15. Segnalare al DPO aziendale mettendo a conoscenza il proprio responsabile gerarchico e il Delegato di Struttura, tutti i casi conosciuti di non rispetto delle misure minime di sicurezza di cui Allegato B del Codice Privacy, anche se formalmente abrogato dal D.lgs. n.101/2018 e delle misure necessarie (Provvedimenti del Garante), delle normative aziendali attinenti, nonché della presente disposizione.

Inoltre Lei è altresì autorizzato all'amministrazione della postazione di lavoro personale, attenendosi alle seguenti istruzioni:

1. Installare unicamente software autorizzati, ovvero:

    1. Utili allo svolgimento della propria attività lavorativa;
    2. Distribuiti ufficialmente dalle società che ne detengono i diritti e che producano aggiornamenti di sicurezza almeno una volta l'anno;
    3. Che non siano comprese nell'elenco delle tipologie di sw non autorizzato (Cfr. Blacklist);
    4. Su esplicita indicazione del Titolare e del Delegato di Struttura;
    5. Nei limiti delle licenze in possesso di ATS:
        I. Di cui si è certi che ATS abbia la relativa licenza nella configurazione e nelle quantità idonee oppure;

II. Software che non necessiti di licenza a pagamento per uso aziendale.

2. Chi installa e gestisce (amministra) un sw (applicativo o di ambiente) si prende la responsabilità di seguire costantemente gli aggiornamenti (vulnerabilità, fine del supporto) del SW installato;
3. Rimuovere i software non più utili e che non rispettano più le condizioni per l'installazione;
4. Applicare in ogni caso le misure di sicurezza minime e necessarie definite dalla normativa di settore;
5. Applicare in ogni caso le disposizioni aziendali in materia;
6. L'attività lavorativa con la propria postazione di lavoro deve essere svolta con la stessa attestata al dominio Windows di riferimento.

Profilo Gestione Database

1. Intervenire ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi e sulle basi dati installati sui medesimi, sui servizi erogati per diagnosticare il problema e ripristinare il corretto funzionamento dei sistemi, coinvolgendo per quanto necessario e possibile gli altri amministratori, cercando di rispettare i livelli di servizio;

Profilo Analista/Progettista

1. Seguire i principi di "Privacy fin dalla progettazione" e "Privacy per impostazione predefinita";
2. Se richiesto, partecipare alla Valutazione d'impatto sulla protezione dei dati ed in ogni caso applicare i requisiti prescritti dalla documentazione del processo di valutazione;
3. Tener conto dei requisiti collegati all'esercizio dei diritti dell'interessato (Accesso, Rettifica, Cancellazione, Limitazione) nel corso della progettazione;
4. Rispettare il principio di minimizzazione del trattamento nella progettazione del sistema, con particolare, riferimento alla progettazione della base dati;
5. Determinare le funzionalità di supporto per la gestione del periodo di conservazione dei dati in ossequio al principio di minimizzazione del trattamento;
6. Individuare, in cooperazione con le strutture tecniche aziendali (Sviluppatori, Sistemisti, Tester, ecc), il DPO aziendale, i requisiti di Sicurezza nell'ambito dell'attività di definizione dei requisiti;
7. Definire le tipologie di dati e di configurazioni da salvare, le modalità di salvataggio (back-up) e le eventuali modifiche e darne comunicazione alla specifica struttura di gestione back-up;
8. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed

applicando i seguenti principi di sicurezza (Rif. Security by Design Principles - OWASP™ Foundation https://www.owasp.org/index.php/Security_by_Design_Principles):

I. Responsabilizzazione
II. Privilegio Minimo
III. Minimizzazione della superficie di attacco
IV. Separazione dei doveri per le operazioni critiche

9. Analizzare i requisiti di sicurezza, verificandone la chiarezza e la fattibilità;
10. Individuare le componenti atte ad effettuare le operazioni di verifica sui dati in input ai moduli di competenza ("sanitization") e utilizzarle in modo sistematico durante lo sviluppo;
11. Utilizzare le indicazioni delle migliori pratiche (es. NIST), algoritmi adeguati (vedi, ad esempio, indicazioni di ECRYPT e FIPS-140) nella progettazione di procedure crittografiche;
12. Segnalare la disponibilità degli aggiornamenti (vulnerabilità, fine del supporto e fine vita) al DPO aziendale per concordare un piano di aggiornamento nei limiti temporali previsti mettendo a conoscenza, a proprio giudizio, il proprio responsabile gerarchico e il Referente Privacy;
13. Se gestisce attività di delivery e deploy di nuove release di Software applicativo, deve richiedere l'esecuzione dei test di non regressione delle applicazioni;
14. Se gestisce attività di delivery e deploy deve richiedere un adeguato test funzionale, di carico e di sicurezza, a seconda delle proprie competenze, utilizzando dati personali palesemente fittizi;
15. Sottoporre all'approvazione del DPO aziendale la necessità di effettuare test con dati di esercizio. In tali casi adottare le stesse cautele utilizzate in esercizio per le configurazioni di sistema ed applicativi;
16. Controllare il corretto funzionamento dell'applicazione, verificando lo stato delle risorse HW e SW.

Profilo Sistemista (Gestione sistemi, application server e storage)

1. Seguire i principi di "Privacy fin dalla progettazione" e "Privacy per impostazione predefinita";
2. Se richiesto, partecipare alla Valutazione d'impatto sulla protezione dei dati ed in ogni caso applicare i requisiti prescritti dalla documentazione del processo di valutazione;
3. Tener conto dei requisiti collegati all'esercizio dei diritti dell'interessato (Accesso, Rettifica, Cancellazione, Limitazione) nel corso della progettazione;
4. Rispettare il principio di minimizzazione del trattamento nella progettazione del sistema, con particolare, riferimento alla progettazione della base dati;
5. Determinare le funzionalità di supporto per la gestione del periodo di conservazione dei dati in ossequio al principio di minimizzazione del trattamento;

6. Definire le tipologie di dati e di configurazioni da salvare, le modalità di salvataggio (back-up) e le eventuali modifiche e darne comunicazione alla specifica struttura di gestione back-up;
7. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed applicando i seguenti principi di sicurezza:
    I. Responsabilizzazione
    II. Privilegio Minimo
    III. Minimizzazione della superficie di attacco
    IV. Separazione dei doveri per le operazioni critiche
8. Effettuare operazioni di tuning dei parametri di configurazione del sistema gestito (HW e sistema operativo e relativo middleware per i profili "Unix", "Linux", "Windows", "Gestione Client" e "Apparati di rete e sicurezza perimetrale", il database server e i relativi strumenti di supporto per i profili "Mysql", "Postgress", "Oracle", "Sqlserver", il software di gestione dello storage e degli apparati di rete FC per il profilo "Tecnologie di virtualizzazione dello Storage" , l'ipervisore e i relativi strumenti di contorno per quanto riguarda il profilo "VmWare ed altre tecnologie di virtualizzazione", il sistema di controllo dell'antivirus per il profilo "Gestione antivirus", la piattaforma di gestione dei backup per il profilo "Gestione del backup", il sistema di monitoraggio per il profilo "Monitoraggio sistemi e reti", i sistemi di gestione e controllo degli apparati di alimentazione e condizionamento per il relativo profilo, il sistema di gestione dei log per l'omologo profilo) applicando il principio del privilegio minimo e della minimizzazione dei servizi erogati, per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità di gestione ed il mantenimento nel tempo delle funzioni;
9. Controllare il corretto funzionamento dei sistemi, verificando lo stato delle risorse HW (cpu, ram, sottosistema di storage, etc) e delle risorse SW;
10. Configurare i sistemi in modo che la parte riservata delle credenziali e i dati sanitari siano sempre gestiti tramite tecniche crittografiche rispondenti allo standard FIPS 140;
11. Verificare almeno una volta l'anno l'efficacia e l'efficienza delle procedure di backup;
12. Predisporre e controllare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi, sulla base delle altre istruzioni aziendali; tali registrazioni (access log) devono avere caratteristiche di completezza e possibilità di verifica adeguate allo scopo per cui sono richieste;
13. Attuare operazioni sui file dei file system e sui file system stessi (delle strutture interne del DB per i relativi profili) (installazione, add, move, change, copy, ecc.) per soli scopi di manutenzione del sistema, indagine diagnostica, installazione di applicazioni o di tool diagnostici o gestionali, tuning, salvataggio, anche temporaneo, di dati e configurazioni, ripristino di condizioni normali di funzionamento;

14. Controllare il corretto funzionamento dell'applicazione, verificando lo stato delle risorse HW e SW;
15. Assicurare che prima della dismissione del dispositivo tutte le informazioni riservate e tutti i dati personali siano state cancellate in modo permanente;
16. Concorre per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Inoltre gli Amministratori di Sistema con profilo di autorizzazione di "Gestione caselle postali" sono autorizzati ad operare sulle caselle postali con particolare riferimento allo svolgimento delle seguenti attività:

1. Creazione, attribuzione diritti agli utenti delle caselle postali personali e logiche di funzione;
2. Gestione delle quote di spazio per le caselle postali;
3. Configurazione dei parametri delle caselle postali.

Profilo CyberSecurity

1. Individuare i requisiti di Sicurezza nel rispetto della normativa vigente nell'ambito dell'attività di definizione dei requisiti di progetto;
2. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed applicando i seguenti principi di sicurezza:
    i. Responsabilizzazione
    ii. Privilegio Minimo
    iii. Minimizzazione della superficie di attacco
    iv. Separazione dei doveri per le operazioni critiche
3. Predisporre e controllare sistemi idonei alla registrazione centralizzata dei log dei sistemi, degli apparati e degli accessi logici, sulla base della normativa vigente e dei requisiti di sicurezza; tali registrazioni devono avere caratteristiche di completezza e possibilità di verifica adeguate allo scopo per cui sono richieste;
4. Verificare periodicamente la sicurezza di tutta l'infrastruttura informatica in gestione e verificare l'uso di configurazioni standard sicure per la protezione dei sistemi;
5. Eseguire regolari scansioni per la ricerca di vulnerabilità sia dei sistemi che delle applicazioni, anche in modalità privilegiata, localmente o da remoto;
6. Predisporre strumenti atti a rilevare la presenza e bloccare l'esecuzione di software malevolo o non ammesso sui sistemi aziendali;
7. Assicurare che gli strumenti utilizzati siano aggiornati ed in grado di rilevare tutte le più significative vulnerabilità di sicurezza;
8. Monitorare e Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali;
9. Registrarsi a uno o più servizi che siano in grado di fornire informazioni sulle nuove minacce e vulnerabilità di sicurezza;

10. Verificare che vengano implementante opportune misure di sicurezza e le vulnerabilità segnalate vengano risolte, mitigate o documentate accettando un ragionevole rischio;
11. Implementare ed assicurare la corretta funzionalità di una procedura di gestione degli incidenti di sicurezza;
12. Concorre per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di Sistema con profilo di autorizzazione di Gestione back-up sono autorizzati ad operare sui sistemi utilizzati per la produzione di tutti i back-up, con particolare riferimento allo svolgimento delle seguenti attività (Back up e Restore):

1. Sorvegliare il corretto funzionamento dei sistemi che sono utilizzati per la produzione dei back-up;
2. Predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
3. Verificare giornalmente l'esito positivo delle procedure di back-up;
4. Verificare l'esito positivo degli eventuali restore richiesti;
5. Provvedere all'archiviazione delle copie su nastro, come da procedura;
6. Monitorare, tramite gli appositi strumenti aziendali, lo stato dei servizi, della rete e dei server;
7. Verificare il corretto funzionamento delle applicazioni e dei siti, anche accedendo alle medesime;
8. Raccogliere le segnalazioni degli utenti, effettuare una prima diagnosi;
9. Attivare gli specialisti a fronte dell'insorgenza di problemi;
10. Ricevere i visitatori secondo le indicazioni contenute nel documento aziendale in proposito;
11. Concorre per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di Sistema con profilo di autorizzazione di "Apparati di rete e sicurezza perimetrale" (Networking – Gestione Infrastruttura di Rete) sono autorizzati a.

1. Provvedere alla segmentazione delle reti in funzione delle utenze dei servizi;
2. Mantenere l'isolamento dei segmenti, collocando tra essi solo apparati di sicurezza;
3. Fornire periodicamente al Titolare o al Delegato di Struttura e al DPO aziendale i seguenti elenchi:
   I. Elenco delle LAN con indicazione della tipologia di utenza
   II. Elenco degli apparati di rete
   III. Elenco degli utenti abilitati sui singoli apparati;
4. Concorre per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di Sistema con profilo di autorizzazione di "Infrastruttura tecnologica (alimentazione elettrica, condizionamento)" sono autorizzati a richiedere e coordinare gli interventi sugli apparati di alimentazione, sui cablaggi, sul sistema di condizionamento, dei manutentori esterni. (Gestione e monitoraggio Infrastruttura e Data Center) In particolare:

1. Verificare che le manutenzioni programmate e i controlli periodici vengano effettuati alle scadenze prestabilite;
2. Monitorare il funzionamento tramite gli strumenti di supervisione;
3. Verificare che il carico elettrico di nuovi apparati siano compatibili con i parametri di impianto;
4. Attivare prontamente le ditte esterne in caso di malfunzionamenti;
5. Verificare che gli interventi siano stati effettuati come richiesto;
6. Concorre per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di sistema con profilo di autorizzazione "Windows" sono inoltre responsabili dell'aggiornamento automatico dei software installati sulle postazioni utente per quei software la cui gestione è stata centralizzata.

Gli Amministratori di Sistema con profilo di autorizzazione di "Gestione Client e stampanti" sono autorizzati ad operare sui client Windows con particolare riferimento allo svolgimento delle seguenti attività:

1. Assistenza tecnica ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia sulle postazioni di lavoro (hardware, sistema operativo, middleware e prodotti installati) per diagnosticare il problema e ripristinare il corretto funzionamento, coinvolgendo per quanto necessario e possibile gli altri amministratori e i fornitori terzi;
2. Supporto all'intervento svolto dagli altri amministratori nel caso venga evidenziato un malfunzionamento, un guasto, una anomalia sulla infrastruttura tecnologica (server e reti) o sulle applicazioni;

3. Installazione di nuove postazioni di lavoro, reinstallazione di postazioni già attive a seguito di malfunzionamenti;
4. Installazione/reinstallazione dei pacchetti software standard e delle procedure applicative;
5. Modifiche ad una postazione di lavoro a seguito della configurazione di periferiche aggiuntive e del relativo software (ad esempio: stampanti, scanner, lettori …);
6. Segnalazione di eventuali problematiche o di situazioni anomale dei client al proprio responsabile.

Gli Amministratori di Sistema con profilo di autorizzazione di "Gestione impianto di videosorveglianza" sono autorizzati ad operare sui sistemi di videosorveglianza con le seguenti particolari istruzioni:

Esplicitazione finalità
Ciascuna videocamera, monitor e registrazione deve essere rivolta ad una finalità esplicita e legittima**:**

1. Difesa del bene pubblico: obbligo di ogni PA a proteggere il proprio patrimonio da furti e danneggiamenti. Deve esserci una proporzione tra valore dei beni da proteggere e invasività della ripresa;
2. Difesa della salute del lavoratore: i lavoratori in situazione di particolare rischio (teorico o registrato) possono/debbono essere protetti, sempre nel rispetto del bilanciamento degli interessi;
3. Difesa dell'incolumità pubblica, in particolare in luoghi ad alto affollamento e con stati emotivi alterati.

Soggetti interessati
Vanno individuate almeno le categorie di soggetti interessati:

1. Lavoratori (a qualunque titolo). Per essi va seguito quanto previsto dall'Art.4 L. 300/1970 (Statuto dei lavoratori);
2. Visitatori: deve essere posta particolare attenzione a valutare la percentuale di interessati vulnerabili (es. minori).

Minimizzazione
L'angolo di ripresa delle videocamere deve essere minimizzato rispetto alla finalità dichiarata.

Informativa
Vanno collocate una o più informative. Tutte le persone devono poter leggere l'informativa prima di essere riprese.

Diritti Interessati
Gli interessati possono esercitare i loro diritti, in particolare:

- Accesso
- Cancellazione
- Opposizione

Dato il breve periodo di conservazione del dato tali diritti sono difficilmente esercitabili.
Occorre valutare la lesione di diritti di terzi (riservatezza).

Periodo di conservazione

1. Deve essere proporzionato alle finalità del trattamento e deve essere giustificato;
2. Il provvedimento del Garante prevede fino a 7 giorni, oltre tale periodo va fortemente giustificato;
3. Il periodo di conservazione dichiarato deve essere configurato su tutti i componenti del sistema;
   (telecamere, videorecorder, software centralizzato di gestione).

Sicurezza del dato

- **Segregazione:**

1. La rete di raccolta e registrazione va segregata. Essa può avvenire logicamente (VLAN, IPSEC) oppure fisicamente (cablaggio dedicato);
2. La rete di visualizzazione potrebbe essere anche essa segregata (esempio via accesso IPSEC/VPN);
3. Gli apparati di registrazione dovrebbero essere contenuti in rack chiusi e in locali chiusi a chiave. I cablaggi non dovrebbero essere facilmente accessibili (a soffitto, in canale, in cavedi chiusi). Le videocamere e soprattutto i registratori dovrebbero essere dotati di allarmi antieffrazione;
4. I monitor di visualizzazione devono essere anche essi in luogo ad accesso limitato e posizionati in modo che eventuali visitatori non possono vedere le immagini;

- **Accesso logico:**

1. Deve essere minimizzato il numero di addetti;
2. Ciascun addetto deve avere una sua credenziale, ove possibile diversa da quella standard su tutti i dispositivi (videocamere, videoregistratori, software centralizzato di gestione);

3. Le password devono essere cambiate ogni 90 giorni. A tal fine ove possibile dovrebbero essere centralizzate tramite protocolli quali LDAP, Radius.

Si ricorda che ai fini del Regolamento UE e del D.Lgs. n. 196/2003 e s.m.i. si intende:

- per Regolamento UE 2016/679 (GDPR), il Regolamento Generale per la Protezione dei dati che modifica l'approccio alla privacy in termini di maggiore tutela degli interessati, responsabilizzazione delle aziende ed inasprimento del sistema sanzionatorio;
- per Garante per la Protezione dei Dati Personali, l'Autorità amministrativa indipendente istituita da uno Stato al fine di assicurare la tutela dei diritti, delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali;
- per "Trattamento", qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali;
- per "Dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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; costituiscono dati personali anche quelli relativi a condanne penali o reati;
- per "Dato particolare", qualunque dato personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici o biometrici intesi a identificare univocamente l'interessato, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- per "Titolare del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- per "Responsabile esterno del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento e al quale il titolare assegna compiti di gestione o controllo sui dati personali fornendone le istruzioni e monitorando l'attività;
- per "Soggetto Autorizzato al trattamento", la persona fisica, facente parte dell'organizzazione aziendale, autorizzata a compiere operazioni di trattamento dal Titolare, dal Delegato o dal Responsabile e su istruzioni degli stessi;
- per "Delegato al trattamento", la persona fisica che viene designata dal Titolare o dal Responsabile del trattamento, sotto la loro responsabilità e nell'ambito del loro assetto organizzativo, all'esercizio di specifici compiti e funzioni connessi al trattamento di dati personali;
- per "Amministratore di sistema", la figura professionale, designata dal Titolare o dal Responsabile dedicata alla gestione e alla manutenzione di impianti informatici con cui vengono trattati dati personali, tra questi: sistemi di gestione dei database, software complessi, reti locali;

- per "Registro dei trattamenti", il registro indicante le attività di trattamento poste in essere per volere del Titolare/Responsabile del trattamento. Si tratta di uno strumento utile a comprovare la correttezza dell'operato dell'organizzazione;
- per "Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD)", la nuova figura di riferimento introdotta dal GDPR che ha la funzione di affiancare Titolare, Delegati, Responsabili e Autorizzati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo;
- per "Privacy by Design and by Default", l'obbligo di strutturare tutti i nuovi processi, servizi e prodotti aziendali in conformità alla normativa sulla Privacy sin dalla loro fase di progettazione;
- per "Data Protection Impact Assessment (DPIA)", l'obbligo di effettuare una valutazione d'impatto sui trattamenti di dati ad alto rischio;
- per "Misure di sicurezza adeguate", l'obbligo di adottare adeguate misure di sicurezza in base al livello di rischio rilevato;
- per "Data Breach", l'obbligo di registrare e di notificare all'Autorità di controllo tutte le violazioni di dati personali subite.

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Cl 1.7.03
Prot. n. _____del_____
Brescia

Oggetto: **Nomina "Responsabile esterno del trattamento dei dati personali" ai sensi dell'articolo 28, paragrafo 3, del Regolamento UE 2016/679.**

TRA

Agenzia Tutela della Salute di Brescia, di seguito denominata "ATS di Brescia" o "ATS", in persona del Legale Rappresentante pro tempore, Direttore Generale Dott. Claudio Vito Sileo;
Codice Fiscale e Partita IVA: 03775430980
Sede Legale: Viale Duca degli Abruzzi, 15
25124 Brescia - Italia
In qualità di **Errore. Il segnalibro non è definito.**Titolare del trattamento

E

[**NOME**] Denominazione (denominazione della persona giuridica o fisica nel caso di professionista), in persona del legale rappresentante/procuratore (in caso di persone giuridiche), di seguito "Responsabile" o "Responsabile del trattamento" o "Società/Ente" [In caso di RTI vanno indicate tutte le aziende mandanti e l'atto deve essere sottoscritto dall'azienda mandataria]
[ISCRIZIONE REGISTRO DELLE IMPRESE/P.IVA]

[INDIRIZZO] (sede legale)

[CODICE POSTALE E CITTÀ]

[PAESE]

In qualità di Responsabile esterno del trattamento

PREMESSO CHE:

- L'**Agenzia di Tutela della Salute di Brescia** e …….**Società/Ente/Persona fisica**…… **……** hanno stipulato una Convenzione/Contratto (di seguito "Convenzione/Contratto") di "**……**", a seguito di Decreto DG/Determinazione dirigenziale numero **……** del **……** al fine di**……**;
- In virtù di tale rapporto contrattuale, è posto in essere un trattamento di dati personali di **……** *(specificare le categorie di dati trattati);*
- Il rapporto contrattuale di cui sopra integra fattispecie rilevante ai sensi del Regolamento UE e, pertanto, si rende necessario disciplinare il rapporto intercorrente fra le Parti prevedendo specifici compiti e le istruzioni nei confronti del soggetto incaricato;

- La "Società/Ente" possiede l'esperienza, la capacità, l'affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e modalità delle operazioni di trattamento;
- Il presente documento, e i relativi allegati, formano parte integrante e sostanziale della predetta Convenzione;
- In caso di controversia tra i termini e le definizioni della presente nomina e il contratto prevarranno i termini e le definizioni della presente nomina;

VISTO

il Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (RGDP - Regolamento Generale sulla Protezione dei Dati), con particolare riferimento agli artt. nn. 4, 8, 28, 30, 32, 33;

CONSIDERATO

che ATS Brescia**,** nella persona del Legale Rappresentante *pro tempore*, ricopre la funzione di Titolare del trattamento* dei dati personali – ex art. 4 del suddetto RGDP;

SONO STATE CONVENUTE

le seguenti clausole contrattuali (le "Clausole"), al fine di soddisfare i requisiti del RGPD e garantire la tutela dei diritti dell'interessato:

1. Indice

2. Preambolo

1. Le presenti clausole contrattuali (le Clausole) stabiliscono i diritti e gli obblighi del Titolare del trattamento e del Responsabile del trattamento, qualora quest'ultimo effettui il trattamento dei dati personali per conto del Titolare del trattamento.
2. Le Clausole sono state concepite per garantire che le Parti rispettino l'articolo 28, paragrafo 3, del RGDP sopra richiamato.
3. Nell'esecuzione della Convenzione/Contratto di cui in premessa, il Responsabile del trattamento tratterà i dati personali per conto del Titolare del trattamento in conformità alle Clausole.
4. Le Clausole hanno priorità rispetto a qualunque disposizione simile contenuta in altri accordi tra le Parti.
5. Le Clausole comprendono quattro appendici, che ne costituiscono parte integrante.
6. L'appendice A contiene dettagli sul trattamento dei dati personali, tra cui la finalità e la natura del trattamento, il tipo di dati personali, le categorie di interessati e la durata del trattamento.

7. L'appendice B riporta le condizioni in base alle quali il Responsabile del trattamento può avvalersi di sub-responsabili del trattamento.
8. L'appendice C comprende le istruzioni del Titolare del trattamento relativamente al trattamento dei dati personali, alle misure minime di sicurezza che il Responsabile del trattamento deve attuare ed alle attività di revisione del Responsabile.
9. L'appendice D (FACOLTATIVA) include le disposizioni per altre attività che non sono contemplate dalle Clausole.
10. Le Parti conservano per iscritto ed elettronicamente le Clausole e relative appendici.
11. Le Clausole non esentano il Responsabile del trattamento dagli obblighi cui è soggetto ai sensi del RGPD o di altra normativa.

3. Diritti e obblighi del Titolare del trattamento

1. Il Titolare del trattamento è responsabile di garantire che il trattamento dei dati personali sia effettuato conformemente al RGPD (cfr. articolo 24, RGPD), alle disposizioni applicabili relative alla protezione dei dati dell'UE o degli Stati membri [1] e alle Clausole.
2. Il Titolare del trattamento ha il diritto e l'obbligo di prendere decisioni sulle finalità e sui mezzi del trattamento dei dati personali.
3. Spetta al Titolare del trattamento, tra l'altro, di assicurare che il trattamento dei dati personali del quale è incaricato il Responsabile del trattamento abbia una base giuridica.

4. Il Responsabile del trattamento agisce secondo le istruzioni

1. Il Responsabile del trattamento effettua il trattamento dei dati personali soltanto su istruzione documentata del Titolare del trattamento, salvo ove richiesto dal diritto dell'Unione o dal diritto nazionale dello stato membro cui è soggetto il Responsabile del trattamento. Il Titolare del trattamento può impartire istruzioni successive durante il periodo di trattamento dei dati personali, ma queste devono essere sempre documentate e conservate per iscritto, anche elettronicamente, unitamente alle Clausole.
   Sono considerate istruzioni documentate le prescrizioni previste dal Contratto/Convenzione, degli eventuali allegati, dell'eventuale capitolato di gara e dalla presente designazione nonché dalla "Misure minime di sicurezza ICT per le pubbliche amministrazioni" e dalle "Linee guida per lo sviluppo del software sicuro" in quanto applicabili e ogni altra eventuale comunicazione scritta del Titolare concernente le modalità di trattamento dei dati.
2. Il Responsabile del trattamento è tenuto a informare tempestivamente il Titolare del trattamento se ritiene che le istruzioni impartite da quest'ultimo violino il RGPD o le disposizioni applicabili relative alla protezione dei dati dell'UE o degli Stati membri.

5. Riservatezza

1. Il Responsabile del trattamento concede l'accesso ai dati personali trattati per conto del Titolare del trattamento soltanto alle persone sotto la propria autorità che si sono impegnate

[1] Nelle clausole, il termine «Stati membri» si riferisce agli «Stati membri del SEE» (Spazio Economico Europeo)

alla riservatezza o abbiano un adeguato obbligo legale di riservatezza ed esclusivamente nei casi di effettiva necessità. L'elenco delle persone a cui è stato concesso l'accesso deve essere sottoposto a revisione periodica. Sulla base di tale revisione, l'accesso ai dati personali può essere revocato se non è più necessario e, di conseguenza, i dati personali non dovranno più essere accessibili a queste persone.

2. Il Responsabile del trattamento, su richiesta del Titolare del trattamento, è tenuto a dimostrare che le persone interessate sotto la sua autorità sono soggette alla succitata riservatezza.

6. Sicurezza del trattamento

1. L'articolo 32 del RGPD prevede che, 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, il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio.
2. Il Titolare del trattamento deve valutare i rischi per i diritti e le libertà delle persone fisiche inerenti al trattamento e attuare misure per attenuare tali rischi.
   A seconda della loro pertinenza, le misure possono comprendere quanto segue:
   a. la pseudonimizzazione e la cifratura dei dati personali;
   b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Ai sensi dell'articolo 32 del RGPD, il Responsabile del trattamento valuta anche, indipendentemente dal Titolare del trattamento, i rischi per i diritti e le libertà delle persone fisiche inerenti al trattamento e attua misure per attenuare tali rischi. A tal fine, il Titolare del trattamento fornisce al Responsabile del trattamento tutte le informazioni necessarie per identificare e valutare tali rischi.
4. Inoltre, il Responsabile del trattamento assiste il Titolare del trattamento nel garantire il rispetto degli obblighi imposti a quest'ultimo ai sensi dell'articolo 32 del RGPD, fornendogli, tra l'altro, le informazioni riguardanti le misure tecniche e organizzative da questi già attuate ai sensi dell'articolo 32 medesimo, unitamente a tutte le altre informazioni necessarie al Titolare del trattamento per conformarsi agli obblighi a lui imposti a norma del predetto articolo 32.

7. Impiego di sub-responsabili del trattamento

1. Al fine di poter incaricare un altro Responsabile del trattamento (sub-responsabile), il Responsabile del trattamento deve soddisfare i requisiti di cui all'articolo 28, paragrafi 2 e 4, RGPD.

2. Il Responsabile del trattamento non può, pertanto, incaricare un sub-responsabile per l'adempimento delle Clausole, senza la previa autorizzazione specifica scritta del Titolare del trattamento.
3. Il Responsabile del trattamento incarica i sub-responsabili del trattamento esclusivamente con la previa autorizzazione specifica del Titolare del trattamento. Il Responsabile del trattamento inoltra la richiesta di autorizzazione specifica almeno 30 giorni prima del conferimento dell'incarico al sub-responsabile del trattamento interessato.
4. Quando un Responsabile del trattamento ricorre a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale sub-responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione europea o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nelle Clausole, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti delle Clausole e del RGPD.
   Spetta quindi al Responsabile del trattamento esigere che il sub-responsabile del trattamento adempia almeno agli obblighi cui è soggetto il Responsabile stesso, secondo le Clausole e il RGPD.
5. Una copia di tale accordo relativo al sub-responsabile del trattamento e ogni successiva modifica dello stesso è inviata al Titolare del trattamento, su sua richiesta, così da permettergli di garantire che al sub-responsabile del trattamento siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nelle Clausole. Le clausole commerciali che non pregiudicano i contenuti giuridici in materia di protezione dei dati di cui all'accordo relativo al sub-responsabile del trattamento non necessitano di essere trasmesse al Titolare del trattamento.
6. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi di tale sub-responsabile del trattamento. Ciò non pregiudica i diritti degli interessati ai sensi del RGPD (in particolare quelli previsti negli articoli 79 e 82, RGPD) nei confronti del Titolare del trattamento e del Responsabile del trattamento, incluso il sub-responsabile.

8. Trasferimento di dati a Paesi terzi o Organizzazioni internazionali

1. Qualsiasi trasferimento di dati personali verso Paesi terzi o Organizzazioni internazionali avviene soltanto sulla base di istruzioni documentate del Titolare del trattamento e ha luogo sempre in conformità con il Capo V del Reg. UE.
2. Qualora trasferimenti di dati a Paesi terzi o organizzazioni internazionali, per i quali il Titolare del trattamento non ha fornito istruzioni al Responsabile del trattamento, siano richiesti dal diritto dell'UE o dello Stato membro cui è soggetto il Responsabile del trattamento, quest'ultimo informa il Titolare di tale obbligo giuridico prima del trattamento, a meno che il diritto dell'UE o dello Stato membro vieti tale informazione per rilevanti motivi di interesse pubblico.
3. Nel quadro delle Clausole, il Responsabile del trattamento, se non dispone di istruzioni documentate da parte del Titolare del trattamento, non può quindi:

a. trasferire dati personali a un Titolare del trattamento o a un Responsabile del trattamento in un Paese terzo o in un'Organizzazione internazionale;
b. trasferire il trattamento dei dati personali a un sub-responsabile del trattamento in un Paese terzo;
c. far trattare i dati personali dal Responsabile del trattamento in un Paese terzo.

9. Assistenza al Titolare del trattamento

1. Tenendo conto della natura del trattamento, il Responsabile del trattamento assiste il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare gli obblighi del Titolare di dare seguito alle richieste di esercizio dei diritti dell'interessato di cui al capo III del RGPD.
   Ciò significa che il Responsabile del trattamento, nella misura in cui ciò sia possibile, deve assistere il Titolare del trattamento a ottemperare a quanto segue:
   a. diritto di essere informato all'atto della raccolta dei dati personali presso l'interessato;
   b. diritto di essere informato quando i dati non sono stati raccolti presso l'interessato;
   c. diritto di accesso dell'interessato;
   d. diritto di rettifica;
   e. diritto alla cancellazione («diritto all'oblio»);
   f. diritto di limitazione di trattamento;
   g. obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
   h. diritto alla portabilità dei dati;
   i. diritto di opposizione;
   j. diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione.

Qualora al Responsabile del trattamento pervenissero richieste degli interessati per l'esercizio dei diritti sopra indicati, lo stesso deve darne tempestiva comunicazione al Titolare, e comunque entro e non oltre 48 ore dal ricevimento della richiesta.

2. Il Responsabile del trattamento, oltre all'obbligo di assistere il Titolare del trattamento secondo quanto previsto dalla clausola 6.4, tenendo conto della natura del trattamento e delle informazioni a sua disposizione, assiste il Titolare del trattamento nel garantire la conformità a quanto segue:
   a. l'obbligo del Titolare del trattamento di notificare la violazione dei dati personali al Garante per la protezione dei dati personali, quale Autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
   b. l'obbligo del Titolare del trattamento di comunicare la violazione dei dati personali all'interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

c. l'obbligo del Titolare del trattamento di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (valutazione d'impatto sulla protezione dei dati);
d. l'obbligo del Titolare del trattamento di consultare il Garante per la protezione dei dati personali, quale Autorità di controllo competente, prima del trattamento, laddove una valutazione di impatto sulla protezione dei dati indichi che il trattamento comporterebbe un alto rischio in assenza di misure adottate dal Titolare del trattamento per mitigare il rischio.

10. Notifica di violazione dei dati personali

1. In caso di incidente di sicurezza, di una violazione o sospetta violazione dei dati personali, il Responsabile del trattamento ne dà prontamente notifica tramite PEC (protocollo@pec.ats-brescia.it) al Titolare del Trattamento.
2. Per "violazione" dei dati personali ("Data Breach") si intende qualsiasi distruzione, perdita, alterazione, divulgazione o acquisizione non autorizzata dei dati personali trattati dal Responsabile del trattamento, ivi incluse quelle che abbiano riguardato i propri sub-fornitori e/o sub-agenti.
3. La notifica del Responsabile del trattamento al Titolare del trattamento avviene nel minore tempo possibile, e comunque non oltre 24 ore dal momento in cui il primo è venuto a conoscenza della violazione o presunta violazione dei dati personali, per permettere al Titolare del trattamento di rispettare il suo obbligo di notifica della violazione stessa al Garante per la protezione dei dati personali, quale Autorità di controllo competente.
4. Ai sensi della clausola 9.2.a., il Responsabile del trattamento assiste il Titolare del trattamento nel notificare la violazione dei dati personali al Garante per la protezione dei dati personali, il che significa che egli è tenuto ad assisterlo nel reperire le informazioni elencate nel prosieguo, le quali sono riportate nella notifica del Titolare del trattamento al Garante, ai sensi dell'articolo 33, paragrafo 3 del Reg. UE.
   a. la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati dalla violazione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b. le probabili conseguenze della violazione dei dati personali;
   c. le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

11. Cancellazione e restituzione dei dati

1. Al termine della prestazione dei servizi relativi al trattamento dei dati personali, il Responsabile del trattamento ha l'obbligo di cancellare tutti i dati personali trattati per conto del Titolare del trattamento, certificando a quest'ultimo l'avvenuta distruzione, salvo che si tratti di dati per i quali, ai sensi di legge (nazionale o dell'Unione Europea), è prevista la conservazione. In tale ultimo caso, il Responsabile del trattamento ha l'obbligo di restituire tutti i dati personali al Titolare, e di cancellare tutte le eventuali copie esistenti.

2. Il Responsabile del trattamento s'impegna a trattare i dati personali esclusivamente per le finalità contrattuali e per un periodo di tempo non superiore a quello necessario ad eseguire le operazioni affidate dal Titolare.

12. Attività di revisione e ispezione

1. Il Responsabile del trattamento mette a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 e alle Clausole e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.
2. Il Responsabile del trattamento è tenuto a fornire alle Autorità di controllo, le quali ai sensi della normativa vigente hanno accesso alle strutture del Responsabile e del Titolare del trattamento, o ai rappresentanti che agiscono per conto di tali Autorità, l'accesso alle strutture fisiche del Responsabile del trattamento, previa presentazione di documentazione atta a identificarli come tali.

13. Accordo delle Parti su altri termini

Le Parti possono concordare altre clausole riguardanti la prestazione del servizio relativo al trattamento dei dati personali, specificando ad esempio ulteriori profili di responsabilità, purché esse non siano incompatibili, direttamente o indirettamente, con le Clausole o ledano i diritti o le libertà fondamentali dell'interessato e la protezione prevista dal RGPD.

14. Inizio e risoluzione

1. Le Clausole sono efficaci dalla data della firma a opera di entrambe le Parti.
2. Le Parti hanno il diritto di richiedere la rinegoziazione delle Clausole laddove una modifica alla legge o l'inadeguatezza delle Clausole stesse dovessero dare luogo a tale rinegoziazione. In particolare, nel caso di modifiche e/o integrazioni alle misure di sicurezza da parte del Titolare è necessario che tali modifiche vengano concordate e comunicate ufficialmente per iscritto al Responsabile del trattamento.
3. Le Clausole sono valide per la durata della prestazione dei servizi relativi al trattamento dei dati personali. Per la durata della prestazione dei servizi relativi al trattamento dei dati personali le Clausole non possono essere risolte, a meno che le Parti abbiano concordato altre clausole che disciplinino tale prestazione.
4. Se la prestazione dei servizi relativi al trattamento dei dati personali cessa e i dati personali sono cancellati o restituiti al Titolare del trattamento ai sensi della clausola 11.1 e dell'appendice C.4., le Clausole possono essere risolte per iniziativa di una delle due Parti con preavviso scritto.

15. Contatti/punti di contatto del Titolare e del Responsabile del trattamento

1. Le Parti possono mettersi in contatto tra di loro utilizzando i seguenti contatti/punti di contatto:
   - per il Titolare del trattamento:

Nominativo	[NOME COGNOME]
Qualifica	[POSIZIONE]
Telefono	[TELEFONO]
E-mail	[E-MAIL]

- per il Responsabile del trattamento:

Nominativo	[NOME COGNOME]
Qualifica	[POSIZIONE]
Telefono	[TELEFONO]
E-mail	[E-MAIL]

2. Le Parti sono tenute a informarsi costantemente di ogni modifica riguardante i suddetti contatti/punti di contatto.

Brescia,

Firmato digitalmente
[OPPURE, APPORRE DATA E FIRME AUTOGRAFE, SE DOCUMENTO ANALOGICO]

Per il Titolare del trattamento:

ATS DI BRESCIA
IL DIRETTORE GENERALE
Dott. Claudio Vito Sileo

Per il Responsabile del trattamento:

NOME	[RAGIONE SOCIALE/NOMINATIVO]
QUALIFICA	[POSIZIONE]
Firmatario	[Nominativo]

Appendice A – Informazioni sul trattamento

[NOTA: IN CASO DI PLURIME ATTIVITÀ DI TRATTAMENTO, QUESTI ELEMENTI DEVONO ESSERE COMPLETATI PER CIASCUNA DI ESSE]

La finalità del trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento è:

[DESCRIVERE LA FINALITÀ DEL TRATTAMENTO]

Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento si riferisce principalmente a (natura del trattamento):

[DESCRIVERE IL TRATTAMENTO: es assistenza nell'utilizzo dell'applicazione XX]

Il trattamento comprende le seguenti tipologie di dati personali sugli interessati:

[DESCRIVERE LE TIPOLOLOGIE DI DATI PERSONALI TRATTATI]

[AD ESEMPIO]

«Nome, indirizzo di posta elettronica, numero di telefono, numero di identificazione nazionale, dettagli di pagamento, numero di tessera, tipo di affiliazione, presenze, ecc.».

[NOTA: QUESTA DESCRIZIONE DOVREBBE ESSERE IL PIÙ DETTAGLIATA POSSIBILE E, IN OGNI CASO, L'INDICAZIONE DELLE TIPOLOGIE DI DATI PERSONALI DEVE ESSERE ULTERIORE RISPETTO AL SEMPLICE RINVIO A «DATI PERSONALI DEFINITI NELL'ARTICOLO 4, PARAGRAFO 1, DEL RGPD» OPPURE ALL'INDICAZIONE DELLE CATEGORIE ("ARTICOLI 6, 9 O 10 DEL RGPD") DI DATI PERSONALI OGGETTO DI TRATTAMENTO.]

Il trattamento comprende le seguenti categorie di interessati:

[DESCRIVERE LA CATEGORIA DI INTERESSATI]

Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento può essere effettuato dalla data di entrata in vigore delle Clausole. Il trattamento ha la seguente durata:

[INDICARE LA DURATA DEL TRATTAMENTO]

Appendice B – Sub-responsabili del trattamento

B.1. Sub-responsabili del trattamento approvati

Il Responsabile del trattamento non ricorre ad un altro Responsabile senza la previa autorizzazione scritta del Titolare.

ATS Brescia – Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.ats-brescia.it
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

Appendice C – Istruzioni relative all'uso dei dati personali

C.1. Oggetto del/istruzioni per il trattamento

Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento è effettuato dal Responsabile del trattamento che svolge quanto segue (a titolo esemplificativo e non esaustivo):

[DESCRIVERE IL TRATTAMENTO CHE IL RESPONSABILE DEL TRATTAMENTO È STATO INCARICATO DI ESEGUIRE]

C.2. Sicurezza del trattamento

Il Responsabile del trattamento s'impegna a mettere in opera tutte le misure di sicurezza previste dall'art. 32 del Reg. UE ed in generale tutte quelle previste da norme e migliori prassi attuali e future, a cui si impegna a conformarsi (senza ulteriori oneri per il Titolare)

Il livello di sicurezza tiene conto di quanto segue:

[TENUTO CONTO DELLA NATURA, DELL'AMBITO DI APPLICAZIONE, DEL CONTESTO E DELLE FINALITÀ DELL'ATTIVITÀ DI TRATTAMENTO NONCHÉ DEL RISCHIO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE, DESCRIVERE GLI ELEMENTI CHE SONO ESSENZIALI PER IL LIVELLO DI SICUREZZA]

[AD ESEMPIO:]

«del fatto che il trattamento prevede un grande volume di dati personali disciplinati dall'articolo 9, RGPD, sulle categorie particolari di dati personali, cosicché si dovrebbe stabilire un alto livello di sicurezza».

C.3. Assistenza al Titolare del trattamento

Il Responsabile del trattamento, attraverso misure tecniche e organizzative adeguate alla natura del trattamento, assiste il Titolare nell'adempimento dei propri obblighi derivanti dall'esercizio, da parte degli interessati, dei diritti di cui agli articoli da 12 a 22 del Reg. UE.

Il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi concernenti la sicurezza dei dati personali (in particolare: sicurezza del trattamento, notifica della violazione dei dati personali al Garante privacy e relativa comunicazione all'interessato), la valutazione d'impatto sulla sicurezza dei dati e la consultazione preventiva con il Garante, ai sensi degli articoli da 32 a 36 del Reg. UE.

C.4. Periodo di conservazione/procedure di cancellazione

Il Responsabile del trattamento deve, richiesta del Titolare, cancellare o restituire al medesimo tutti i dati personali al termine della convenzione/contratto o comunque alla prestazione di servizi relativi al trattamento nonché cancellare le copie esistenti, salvo che il diritto dell'Unione o la normativa nazionale prevedano la conservazione dei dati.

Il Titolare ha il diritto di verificare che il Responsabile abbia completato in modo appropriato la restituzione o la cancellazione dei dati.

C.5. Luogo del trattamento

Il trattamento dei dati personali ai sensi delle Clausole non può essere effettuato in luoghi diversi da quelli che seguono, senza la previa autorizzazione scritta da parte del Titolare del trattamento:

[INDICARE DOVE HA LUOGO IL TRATTAMENTO]

Il trasferimento da parte del Responsabile dei dati personali in un Paese terzo o a un'organizzazione internazionale può avvenire solo a seguito di specifica autorizzazione scritta del Titolare.

C.6. Procedure per le attività di revisione da parte del Titolare del trattamento, comprese le ispezioni, relativamente al trattamento di dati personali da parte del Responsabile

Il Responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui alla presente designazione e di cui all'art. 28 del Reg. UE nonché consente e contribuisce alle attività di revisione, comprese le ispezioni, eseguite dal Titolare o da altro soggetto da questi incaricato.

Appendice D – Termini dell'accordo delle Parti su altri aspetti
[FACOLTATIVA: PER INDIVIDUARE E DISCIPLINARE ALTRI ASPETTI, QUALI I SEGUENTI:]

AFFIDAMENTO A RETI TEMPORANEE DI IMPRESA (RTI)

In caso di RTI specificare chi ricopre il ruolo di mandataria e chi di mandante/i, come indicato nelle Clausole.

Si richiede alla RTI di comunicare i contenuti delle Clausole alle mandanti e si richiede l'attestazione della ricezione delle istruzioni contenute nell'atto di nomina. La mandataria è responsabile del coordinamento delle procedure Privacy e deve specificare i ruoli delle mandanti indicando i flussi di dati e le relative modalità. Per ogni flusso devono essere indicate le misure di sicurezza previste.

REGISTRO DEI TRATTAMENTI

Il Responsabile del trattamento, qualora non rientri nelle casistiche definite dall' art. 30, comma 2 e 5, GDPR, tiene per iscritto un Registro delle attività relative al trattamento svolte per conto del Titolare e delle applicazioni informatizzate utilizzate, nel pieno rispetto del GDPR.

AUTORIZZATI

Persone autorizzate
Il Responsabile del trattamento si impegna a produrre – su richiesta del Titolare - ed aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente ed opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati ai sensi dell'art.29 del GDPR. Inoltre, il Responsabile del trattamento si impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre deve garantire che le persone autorizzate siano state istruite sulla procedura di gestione degli incidenti di sicurezza e la gestione delle violazione di dati personali. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.

Persone autorizzate in qualità di Amministratori di Sistema
Il Responsabile, qualora siano presenti Amministratori di Sistema, si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.

CLAUSOLA SERVIZI PUBBLICI

Nel caso in cui l'oggetto del contratto sia finalizzato all'erogazione di servizi pubblici (essenziali) il fornitore dovrà procedere con quanto previsto dal contratto stesso, mettendo in atto le cautele che a suo giudizio salvaguardino i diritti e le libertà fondamentali delle persone fisiche, senza causare maggiore lesione ai diritti stessi anche da parte del Titolare stesso e di altri soggetti, dandone immediata comunicazione all'azienda.
PRIVACY BY DESIGN & BY DEFAULT
Il Responsabile garantisce l'applicazione dei principi di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (art. 25 del GDPR). (Vedi allegato C.3.)
[AGGIUNGERE EVENTUALI ULTERIORI INDICAZIONI] [ESEMPIO:]: "Qualora venissero meno una o più delle misure di sicurezza previste, il Responsabile del trattamento, a sua cura e spese, dopo aver informato il Direttore dell'Esecuzione del Contratto, dovrà provvedere al relativo ripristino anche in modalità alternative."
INFORMATIVA
[AGGIUNGERE EVENTUALI ULTERIORI INDICAZIONI] [ESEMPIO:] "Nel raccogliere i dati personali il fornitore deve fare riferimento all'informativa fornita dal Titolare. L'informativa deve essere pubblicata in qualsiasi contesto in cui saranno raccolti i dati personali degli utenti. Se presente, viene messa a disposizione una versione offline fornita prima della raccolta dei dati, debitamente datate."
[ESEMPIO:] "Il Responsabile del trattamento, al momento della raccolta dei dati, deve fornire alle persone interessate dalle operazioni del trattamento le informazioni relative ai trattamenti dei dati che realizza, tra le quali anche l'eventuale uso di strumenti di profilazione. La formulazione ed il formato dell'informazione deve essere concordata con il Titolare del trattamento prima della raccolta dei dati".
GESTIONE DIRITTI DEGLI INTERESSATI
Qualora al Responsabile del trattamento pervenissero richieste degli interessati per l'esercizio dei diritti di cui agli artt. 15, 16, 17, 18, 20 (qualora possibile) e 21 del GDPR, lo stesso deve darne tempestiva comunicazione al Titolare, e comunque entro e non oltre 24 ore dal ricevimento della richiesta. Tenendo conto della natura del trattamento dei dati personali svolti dal Responsabile, quest'ultimo si impegna, su richiesta del Titolare, ad assisterlo nella misura in cui ciò sia ragionevolmente possibile, approntando le adeguate misure tecniche e organizzative, ai fini dell'adempimento da parte del Titolare all'obbligo di permettere ai terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.
CODICI DI CONDOTTA E MECCANISMI DI CERTIFICAZIONE
[ESEMPIO:] "E' facoltà della Società aderire a codici di condotta o a meccanismi di certificazione di cui agli artt. 40 e 42 del Regolamento. Il Responsabile deve comunicare

ATS Brescia – Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.ats-brescia.it
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

preventivamente al Titolare l'eventuale adesione ai predetti Codici di condotta o il probabile conseguimento di certificazioni".

POLIZZA ASSICURATIVA

[ESEMPIO:] "Richiesta di attestazione di possesso di idonea polizza assicurativa per il risarcimento di danni inerenti /derivanti dall'attività in parola e per quelli inerenti/derivanti da eventuali violazioni della Privacy".

ULTERIORI RICHIESTE

Il Responsabile deve comunicare al Titolare entro 48 ORE (dalla eventuale richiesta):

- le misure di sicurezza adottate comprese quelle di nuova adozione al fine di consentire a quest'ultimo la verifica del mantenimento di un livello di sicurezza adeguato ai rischi ed alla natura dei dati trattati;
- il luogo fisico di archiviazione dei dati nonché le modalità di loro conservazione e il loro ripristino (backup e architetture di Disaster Recovery) ovvero, fermo restando quanto precede, le eventuali allocazioni su cloud, i relativi dati di sicurezza, declinando le generalità del provider/ gestore per la relativa autorizzazione e designazione preventiva a Responsabile del trattamento dei dati.

REGISTRO DATA BREACH E INCIDENTI INFORMATICI

Il Responsabile deve mantenere un Registro degli incidenti di sicurezza e Data Breach, anche qualora non vi siano violazioni, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR.
A seguito del verificarsi di detti incidenti il Titolare potrà:

- fare attività di Audit, anche senza preavviso e avvalendosi di soggetti terzi;
- prescrivere ulteriori misure di sicurezza anche apportando modifiche a quelle in essere con particolare riferimento al presente accordo;
- attivare azioni di rivalsa nei confronti del Responsabile;
- applicare le penali contrattuali;
- risolvere il contratto.

RESPONSABILITÀ

Fermo restando che il Regolamento Europeo (UE) 2016/679 conferma nel trattamento dei dati personali l'attività pericolosa di cui all'art. 2050 del C.C., la relativa responsabilità per danni, patrimoniali e non, provocati all'interessato in conseguenza del trattamento stesso grava in capo a chi detiene i mezzi per gestire le modalità di trattamento (ossia al Titolare del trattamento o ad entrambi in solido). Il Responsabile del trattamento risponde direttamente per il danno causato dal trattamento qualora non abbia adempiuto agli obblighi previsti dal Regolamento e dalle norme di armonizzazione, ovvero, abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare del trattamento, manlevando Titolare per eventuali violazioni di norme, inadempimenti giuridici, inosservanza regolamentari, nonché per i danni inerenti/derivanti dai trattamenti dati di cui trattasi, per i quali il Titolare possano essere chiamati a rispondere, sia civilmente, sia in punto privacy. Identico riparto si configura in ipotesi di sanzioni amministrative. Qualora il Responsabile violi una delle disposizioni del presente atto, determinando le finalità e i mezzi del trattamento, è considerato Titolare delle attività di trattamento per le quali ha determinato in autonomia finalità e mezzi del trattamento e come tale risponde a sensi di legge.

L'inadempimento di quanto previsto nel presente atto nella sua interezza comporta la revoca di diritto del presente incarico con contestuale caducazione del rapporto contrattuale sostanziale per violazione privacy, fatte le responsabilità inerenti e /o derivanti da tali violazioni ed il relativo ristoro di eventuali danni. In caso di contrasto con le disposizioni contrattuali prevalgono quelle del presente atto. Eventuali accordi in contrasto ovvero in deroga con le disposizioni del presente atto debbono essere concordate per iscritto tra le Parti, richiamando espressamente quelle derogate avvertendo che ciò connota responsabilità diretta dei contraenti.

FORO COMPETENTE

Per qualunque controversia inerente alla corretta applicazione delle Clausole ed alle connesse responsabilità concernenti le modalità di trattamento dei dati è competente il Foro di Brescia.