Sistema Socio Sanitario
Regione Lombardia
ATS Pavia

ACCORDO IN MERITO AL TRATTAMENTO DI DATI PERSONALI
(art. 28 del Regolamento UE n. 2016/679)

TRA

Agenzia Territoriale della Salute di Pavia, con sede in Pavia (PVI), Viale Indipendenza n. 3, C.F./P.IVA . 02613260187, in persona del Direttore Generale *pro tempore* Dr.ssa Lorella Cecconami

TITOLARE

E

……, con sede in ……, C.F./P.IVA …….. in atto rappresentata dal…….. Direttore Generale/ Rappresentante Legale

RESPONSABILE ESTERNO

PREMESSO CHE

a) tra l' ATS di Pavia e ..... intercorrono i seguenti rapporti Giuridici: ……
……
……
……
……
……

b) il Titolare del trattamento ed il Responsabile del trattamento come sopra identificati **ACCETTANO** le clausole contrattuali tipo pubblicate il 07/06/2021 sulla Gazzetta ufficiale dell'Unione Europea e qui di seguito elencate al fine di garantire il rispetto dell'art. 28, paragrafi 3 e 4, del Regolamento UE 2016/679;

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

b) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato I

c) Gli allegati da I a III costituiscono parte integrante delle clausole.

d) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.

e) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

Clausola 2 - Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 — Clausola di adesione successiva

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando il presente accordo

b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II - OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato I.

Clausola 7 - Obblighi delle parti

7.1. Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato I, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato I.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato II per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

a) Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno **15 giorni**, dando così al titolare del trattamento tempo sufficiente

per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.

c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8 - Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

d) Le parti stabiliscono nell'allegato II le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 o degli articoli 34 e 35 del regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

2) le probabili conseguenze della violazione dei dati personali;

3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo. Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE).

SEZIONE III - DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679; 3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole del regolamento (UE).

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

* * * * * * *

Il Responsabile della Protezione dei Dati (RPD) dell'Agenzia di Tutela della Salute di Pavia è:
LTA S.r.l. PIVA 14243311009
Dott.ssa ROSA COPPOLA - Via della Conciliazione 10, 00193 Roma
coordinamento_privacy@ats-pavia.it

Il Responsabile del procedimento:
Direttore .....

DATA, _____

FIRMA DEL TITOLARE
ATS DI PAVIA
IL DIRETTORE GENERALE

_____

FIRMA DEL RESPONSABILE ESTERNO
…….
…….

_____

ALLEGATO I

DESCRIZIONE DEL TRATTAMENTO

CATEGORIE DI INTERESSATI I CUI DATI PERSONALI SONO TRATTATI

□ Pazienti / Utenti
□ Dipendenti
□ Collaboratori
□ Tirocinanti
□ Fornitori
□ Visitatori
□ Altri *[indicare]*
_____

CATEGORIE DI DATI PERSONALI TRATTATI

Dati personali comuni:

□ Identificativi e Anagrafici (es. *nome, cognome, età, indirizzo, codice fiscale*)
□ Di contatto (es. *email, telefono*)
□ Fiscali ed Economico / contabili (es. *codice fiscale / P.IVA, importi e metodi di pagamento, IBAN*)
□ Altri *[indicare]*
_____

Dati sensibili (se del caso):

□ Dati relativi alla salute dell'interessato
□ Dati relativi all'orientamento sessuale dell'interessato
□ Dati relativi alla vita sessuale dell'interessato
□ Dati genetici dell'interessato
□ Dati biometrici dell'interessato
□ Dati che rivelino l'origine razziale o etnica dell'interessato
□ Dati che rivelino l'appartenenza sindacale dell'interessato

È fatto divieto di trattare altre categorie di dati sensibili oltre quelle sopra elencate e selezionate.

Il trattamento dei dati sensibili da parte del Responsabile e dai soggetti da quest'ultimo autorizzati è consentito e limitato esclusivamente alle finalità previste dal presente accordo.

L'accesso ai dati sarà consentito esclusivamente a personale che abbia seguito una formazione specializzata e che abbia ricevuto specifiche istruzioni da parte del Responsabile.

Il Responsabile garantisce la tracciabilità degli accessi ai dati da parte dei propri incaricati.

NATURA DEL TRATTAMENTO

[descrizione dell'operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali eseguite per conto del Titolare (come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione)]

FINALITÀ PER LE QUALI I DATI PERSONALI SONO TRATTATI PER CONTO DEL TITOLARE DEL TRATTAMENTO

[descrizione delle finalità del trattamento eseguito per conto del Titolare (es. finalità di cura dell'interessato, gestione del rapporto di lavoro, assistenza e contabilità, marketing, assistenza e manutenzione di impianti o dei sw o del sito web)]

DURATA DEL TRATTAMENTO

Le prescrizioni di cui al presente atto hanno decorrenza dall'ultima data di sottoscrizione e scadenza congrua a quella indicata nel rispettivo contratto di fornitura di servizi o all'interno dell'atto di cui in Premessa. Il presente Accordo in merito al trattamento di dati personali ai sensi dell'art. 28 GDPR rimarrà in vigore fino a quando continueranno a svilupparsi le obbligazioni contrattuali del contratto di fornitura dei servizi o di cui l'atto di cui in Premessa disciplina gli aspetti inerenti la tutela dei dati personali.

Nota: Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

DATA, _____

FIRMA DEL TITOLARE
ATS DI PAVIA
IL DIRETTORE GENERALE

_____

FIRMA DEL RESPONSABILE ESTERNO
…….
…….

_____

ALLEGATO II

MISURE TECNICHE E ORGANIZZATIVE, COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

NOTE ESPLICATIVE:
Per ogni misura richiesta di seguito il RESPONSABILE deve definire e documentare specifiche istruzioni per assicurarne il rispetto da parte di tutti gli autorizzati che operano per suo conto.
Il RESPONSABILE può trovare validi riferimenti per la scelta dei controlli nel processo di attuazione delle Misure richieste dal TITOLARE nella norma UNI CEI ISO/IEC 27001 relativa alla Sicurezza delle informazioni e nella norma UNI CEI ISO/IEC 27002.
Per alcune misure è riportato, fra parentesi quadre, il riferimento all'Appendice della Norma UNI CEI ISO/IEC 27001 relativa alla Sicurezza delle informazioni e/o alla norma UNI CEI ISO/IEC 27002.

GIORNI DI ANTICIPO RICHIESTO PER LA COMUNICAZIONE DELL'AGGIUNTA O SOSTITUZIONE DEI SUB-RESPONSABILI (CLAUSOLA 7.7 A).

15 giorni.

MISURE DI PSEUDONIMIZZAZIONE E CIFRATURA DEI DATI PERSONALI

Tutti i dati sensibili saranno trattati dal RESPONSABILE mediante l'utilizzo di sistemi di pseudonomizzazione e cifratura.
Il RESPONSABILE deve definire, in caso di trasmissione di dati personali via mail, una politica sull'uso dei controlli crittografici per la protezione delle informazioni con standard che consentano adeguati livelli di sicurezza (es. protetti da password). [10.1.1]

MISURE PER ASSICURARE SU BASE PERMANENTE LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI DI TRATTAMENTO

Il RESPONSABILE deve tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento ai sensi dell'Art. 30 comma 2 del regolamento (UE) 2016/679 contenente, almeno, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del regolamento (UE) 2016/679.

MISURE PER ASSICURARE LA CAPACITÀ DI RIPRISTINARE TEMPESTIVAMENTE LA DISPONIBILITÀ E L'ACCESSO DEI DATI PERSONALI IN CASO DI INCIDENTE FISICO O TECNICO

Il RESPONSABILE deve assicurare che il tempo previsto di ripristino (in emergenza) dei sistemi informatici (RTO), sia inferiore al tempo massimo prima che gli interessati percepiscano conseguenze inaccettabili (MTPD) che si ritiene pari a 8 ore lavorative. [12.3.1]
Il RESPONSABILE deve assicurare che le strutture per l'elaborazione delle informazioni siano realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. [17.1.3]

PROCEDURE PER TESTARE, VERIFICARE E VALUTARE REGOLARMENTE L'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE AL FINE DI GARANTIRE LA SICUREZZA DEL TRATTAMENTO

Il RESPONSABILE deve effettuare, almeno annualmente, una verifica e valutazione dei Sistemi Informativi utilizzati per fornire il servizio per conto del Titolare, anche con il supporto di eventuali specialisti, per assicurare la corretta attuazione dei controlli relativi alla sicurezza delle informazioni.

MISURE DI IDENTIFICAZIONE E AUTORIZZAZIONE DELL'UTENTE

Il RESPONSABILE deve garantire che le persone autorizzate al trattamento dei dati, oltre ad essere impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, siano state istruite sulle indicazioni fornite dal TITOLARE in tal senso (Art. 29 del GDPR).
Il RESPONSABILE deve assicurare che gli autorizzati non effettuino copie dei dati se non per finalità differenti definite da altri TITOLARI e di cui sia data adeguata informativa agli interessati.
Il RESPONSABILE deve assicurare che solo gli autorizzati abbiano la disponibilità delle chiavi per accedere ai luoghi (Cassetti, Armadi, Stanze) nei quali sono conservati i dati.
Il RESPONSABILE deve assicurare che gli autorizzati potranno accedere ai sistemi per trattare i dati solo tramite autenticazione tramite password con complessità adeguata. [09.3.1]
Il RESPONSABILE deve assicurare che ogni autorizzato acceda con credenziali di accesso in uso esclusivo.
Il RESPONSABILE deve assicurare la rimozione delle credenziali di accesso in caso di cessazione dell'autorizzazione al trattamento dei dati. [09.2.6]
Il RESPONSABILE deve assicurare il riesame periodico dei diritti di accesso degli utenti. [9.2.5]

MISURE DI PROTEZIONE DEI DATI DURANTE LA TRASMISSIONE

Solo gli autorizzati dal RESPONSABILE possono ricevere i documenti in formato cartaceo o aprire buste contenenti informazioni relative trattamenti eseguiti per conto del titolare.
La casella di posta elettronica utilizzata per le comunicazioni tra titolare e responsabile deve essere accessibile unicamente a soggetti autorizzati dal RESPONSABILE.
Eventuale dati sensibili trasmessi a mezzo posta elettronica saranno cifrati e protetti da password da comunicarsi separatamente e con altro mezzo.
A tal fine le parti indicano sin d'ora che saranno utilizzati i seguenti indirizzi di posta elettronica.
Per ATS di Pavia: _____
Per il Responsabile esterno: _____
Sarà cura delle parti comunicare tempestivamente - e comunque con un preavviso non inferiore a giorni 7 - l'eventuale variazione degli indirizzi di pota elettronica utilizzati per le comunicazioni.

MISURE DI PROTEZIONE DEI DATI DURANTE LA CONSERVAZIONE

I dati ricevuti dovranno essere adeguatamente protetti ed in particolare:

Dati in formato cartaceo:

Devono essere conservati all'interno di archivi (cassetti, armadi, stanze) chiusi che impediscano l'accesso ai non autorizzati. I locali nei quali sono conservati i documenti cartacei devono essere dotati di sistemi antincendio.
Il RESPONSABILE deve individuare luoghi sicuri ove sono di norma custoditi i documenti in formato cartaceo contenenti i dati particolari; tali documenti non devono essere asportati da tali luoghi sicuri e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento. Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario. Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro. Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, la persona autorizzata al trattamento non deve mai perderli di vista o eseguire copie non necessarie, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
L'accesso da parte del personale autorizzato a documenti in formato cartaceo contenenti i dati particolari deve essere selezionato e tracciabile.

Dati in formato elettronico:

Devono essere conservati unicamente su sistemi nella disponibilità del RESPONSABILE (non su dispositivi personali dei dipendenti/collaboratori del RESPONSABILE). [06.2.1]
Devono essere conservati su sistemi protetti da software anti-virus, anti-malware, anti-spyware sui quali vengono eseguite operazioni di backup isolati dall'esterno o comunque protetti da firewall ed altri dispositivi di sicurezza.
Se i dati sono conservati in aree in cloud i fornitori dei servizi devono essere certificati secondo la norma UNI CEI ISO/IEC 27001 e ISO/IEC 27018.
Non devono essere archiviati su dispositivi mobili se non precedentemente crittografati. [06.2.1]
Devono essere conservati in aree di memorizzazione alle quali hanno accesso solo gli autorizzati al trattamento.

MISURE PER GARANTIRE LA SICUREZZA FISICA DEI LUOGHI IN CUI I DATI PERSONALI SONO TRATTATI

I luoghi dove il RESPONSABILE tratta i dati devono essere protetti da sistemi antintrusione. [11.1.1]
I luoghi dove risiedono le apparecchiature fisiche utilizzate per il trattamento dei dati digitali devono essere protetti da sistemi antintrusione. [11.1.1]
Il RESPONSABILE deve assicurare che solo il personale autorizzato possa accedere alle aree dove vengono trattati i dati. [11.1.2]
Il RESPONSABILE deve assicurare la sicurezza fisica agli uffici, ai locali ed agli impianti. [11.1.3]

MISURE PER GARANTIRE LA REGISTRAZIONE DEGLI EVENTI

Il RESPONSABILE deve tenere una registrazione degli eventi fisici rilevanti ai fini del trattamento.
Il RESPONSABILE deve conservare i log sugli accessi ai dati in formato digitale da parte di eventuali Amministratori di Sistema.

MISURE PER GARANTIRE LA CONFIGURAZIONE DEL SISTEMA, COMPRESA LA CONFIGURAZIONE PER IMPOSTAZIONE PREDEFINITA

Il RESPONSABILE deve assicurare la corretta configurazione dei dispositivi elettronici utilizzati per fornire i servizi per conto del Titolare (tutte le password di fabbrica o di default vengono modificate).

I sistemi sui quali il RESPONSABILE tratta i dati in formato elettronico devono essere correttamente configurati per evitare che l'operatore possa modificare in autonomia le configurazioni impostate. [12.5.1]
Il RESPONSABILE deve assicurare che sia disabilitato l'avvio automatico di software caricato su supporto esterno per i dispositivi che permettono tale funzionalità (tipicamente personal computer).

MISURE DI INFORMATICA INTERNA E DI GESTIONE E GOVERNANCE DELLA SICUREZZA INFORMATICA

Il RESPONSABILE si impegna ad attuare le seguenti misure qualora ritenga necessario nominare amministratori di sistema:
Scegliere gli amministratori di sistema tra quei soggetti dotati di esperienza, capacità ed affidabilità, in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza.
Nominare gli amministratori di sistema individualmente, elencando analiticamente gli ambiti di operatività consentiti a ciascun amministratore di sistema in relazione al proprio profilo di autenticazione.
Fornire, su richiesta del TITOLARE, l'elenco dei soggetti nominati amministratori di sistema.
Adottare software/sistemi idonei a registrare gli accessi degli amministratori di sistema; le predette registrazioni degli accessi logici (access log) devono essere complete, inalterabili e consentire verifiche di integrità; devono essere conservate per un congruo periodo non inferiore a 6 mesi.
Eseguire verifiche periodiche (con cadenza almeno annuale) relative al rispetto da parte degli amministratori di sistema delle misure organizzative, tecniche e di sicurezza previste dalla normativa in materia di protezione dei dati personali. [09.2.3]
Il RESPONSABILE deve aver predisposto e mantenere aggiornate procedure: per Disaster Recovery e/o Business Continuity; per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; per la rilevazione e la gestione di eventuali violazioni. [17.1.1]

MISURE DI CERTIFICAZIONE/GARANZIA DI PROCESSI E PRODOTTI

Il RESPONSABILE deve essere assistito da consulenti in grado di fornire costantemente la conoscenza delle migliori prassi in tema di sicurezza delle informazioni, informazioni circa allarmi e patch relativi a vulnerabilità e fornire punti di contatto per incidenti relativi alla sicurezza delle informazioni. [06.1.4]
Il RESPONSABILE deve aver formato gli autorizzati su: il controllo degli accessi; la sicurezza fisica e ambientale; per il controllo degli accessi ai sistemi; per la scrivania e lo schermo puliti; per il trasferimento delle informazioni; per l'utilizzo dei dispositivi mobili e il telelavoro. [05.1.1]
Il RESPONSABILE deve richiedere a tutto il personale ed ai collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi. [16.1.3]
Il RESPONSABILE deve assicurare una corretta gestione degli incidenti (compresi quelli che non comportano una violazione dei dati) stabilendo apposite procedure e responsabilità per il monitoraggio, la rilevazione, la registrazione, l'analisi e la segregazione degli eventi. [16.1.1]
Il RESPONSABILE mantiene log relativamente alle principali operazioni eseguite sui propri sistemi informatici. [12.4.1]

MISURE PER GARANTIRE LA MINIMIZZAZIONE DEI DATI

Qualora il RESPONSABILE riceva per conto del TITOLARE documenti contenenti informazioni non necessarie a nessuno dei trattamenti di Sua competenza dovrà provvedere ad oscurarle e ad informare il TITOLARE.

MISURE PER GARANTIRE LA CONSERVAZIONE LIMITATA DEI DATI

I dati in formato cartaceo devono essere conservati con modalità che ne permettano l'eliminazione alla notizia della conclusione del servizio o, comunque, trascorso il termine previsto per la conservazione.
Il Responsabile dovrà assicurare la distruzione con apposita apparecchiatura di ogni dato cartaceo.
Il Responsabile dovrà assicurare la cancellazione di ogni dato in formato elettronico (es. file contenenti la scannerizzazione dei documenti) e la cancellazione, con rimozione anche dalla posta eliminata, di ogni mail contenente dati trattati per conto del Titolare.

MISURE PER GARANTIRE LA RESPONSABILITÀ

Il RESPONSABILE deve, attraverso programmi di formazione e di sensibilizzazione alla sicurezza delle informazioni, rendere tutti gli autorizzati consapevoli delle loro responsabilità. [07.2.2]
Gli utenti devono essere tenuti a seguire le prassi definite dal RESPONSABILE nell'uso di informazioni segrete di autenticazione. [09.3.1]

MISURE PER CONSENTIRE LA PORTABILITÀ DEI DATI E GARANTIRE LA CANCELLAZIONE

[Descrivere se del caso]

MISURE TECNICHE E ORGANIZZATIVE SPECIFICHE CHE IL RESPONSABILE DEL TRATTAMENTO DEVE PRENDERE PER ESSERE IN GRADO DI FORNIRE ASSISTENZA AL TITOLARE DEL TRATTAMENTO

[Descrivere se del caso]

MISURE TECNICHE E ORGANIZZATIVE SPECIFICHE CHE IL SUB-RESPONSABILE DEL TRATTAMENTO DEVE PRENDERE PER ESSERE IN GRADO DI FORNIRE ASSISTENZA AL TITOLARE DEL TRATTAMENTO
[Descrivere se del caso]

DATA, _____

FIRMA DEL TITOLARE
ATS DI PAVIA
IL DIRETTORE GENERALE

_____

FIRMA DEL RESPONSABILE ESTERNO
……
……

_____

ALLEGATO III

ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

NOTE ESPLICATIVE:
Il presente Elenco deve essere compilato con tutti gli altri Responsabili (sub-responsabili) del trattamento ai quali il Responsabile ritiene di dover ricorrere.
Il Livello indica la gerarchia dei rapporti: Livello 1 indica i sub-responsabili nominati direttamente dal Responsabile, Livello 2 indica i sub-responsabili nominati dai sub-responsabili di Livello 1 precedente e così via.
Il Responsabile ha l'obbligo di richiedere ai sub-responsabili di essere informato di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento e di informare di tali modifiche il Titolare dando così allo stesso l'effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate in tutto o in parte le attività di trattamento dei dati personali e l'opportunità di opporsi a tali modifiche.
Nel prosieguo del rapporto, se l'elenco dei sub-responsabili dovesse essere modificato, sarà cura del RESPONSABILE integrare lo presente scheda o, alternativamente, effettuare specifica comunicazione al Titolare entro i termini definiti nella Clausola 7.7 a).

Livello	**SUB-RESPONSABILE** (Nome / Denominazione e dati di contatto)	**Descrizione trattamento**

DATA, _____

FIRMA DEL TITOLARE
ATS DI PAVIA
IL DIRETTORE GENERALE

_____

FIRMA DEL RESPONSABILE ESTERNO
…….
…….

_____