

ACCORDO TRA CONTITOLARI PER IL TRATTAMENTO DATI

(Ex art. 26 Regolamento U.E. 679/2016 e norme di armonizzazione)

Parti

Il presente accordo è concluso tra ASL 3, direttamente, in persona del legale rappresentante pro tempore e con delega alla sottoscrizione dello stesso da parte del dirigente responsabile della S.C....., da ora in avanti anche Titolare e [*****], in persona di...../ del legale rappresentante pro tempore....., da ora in avanti anche Contitolare.

Premessa

Con deliberazione [*****]

Oggetto del presente Accordo è l'instaurazione di un rapporto di Contitolarità in riferimento ai trattamenti afferenti il rapporto sostanziale contrattuale/convenzionale conseguente alla suddetta deliberazione.

Ciascuno dei Contitolari necessita dei dati strettamente necessari alle finalità di trattamento di cui all'Allegato A ed ivi individuati al fine di dar corso alle prestazioni oggetto di rapporto contrattuale/convenzionale;

ASL 3 e....., quali Contitolari di tali dati, sono necessitati a conferirli, al fine di consentire la corretta erogazione delle prestazioni di cui trattasi.

L'attività sostanziale, sottesa al presente Accordo, resta nell'esclusiva responsabilità di ciascuno dei Contitolari per quanto di rispettiva competenza, ai sensi del sopra citato rapporto contrattuale/convenzionale.

Tramite il presente accordo le parti intendono regolare il proprio rapporto in relazione alle attività di trattamento di dati personali e categorie particolari di dati personali, con particolare attenzione alla protezione dei dati.

Gli allegati formano parte integrante del presente Accordo.

Definizioni

La terminologia del Data Processing Agreement si rifà a quanto definito dal Regolamento UE 679/2016 ed alle relative norme di armonizzazione

In particolare si forniscono le seguenti definizioni:

«Regolamento»: 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);

«Titolare o 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;

«Responsabile o 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;

«Subresponsabile o Subresponsabile esterno del Trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di un Responsabile o Subresponsabile;

«Autorizzati o Autorizzati al trattamento»: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal responsabile;

«Contitolari del Trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, con conseguente esercizio di potere decisorio, scelte, potere di ordine, di direttiva vincolante e di controllo;

«Accordo»: il presente atto.

Obblighi dei contitolari.

Principi generali

I Contitolari mettono in atto misure tecniche e organizzative affinché i trattamenti svolti sotto la rispettiva responsabilità, in funzione e nel rispetto dei relativi scopi anche istituzionali, ma **in condivisione di dati, finalità e mezzi di trattamento**, soddisfino i requisiti della normativa di settore, con particolare attenzione alla tutela dei diritti e libertà dell'interessato.

Essi utilizzano i dati personali e categorie particolari di dati personali oggetto di trattamento solo per le **finalità** indicate **nell'Allegato A** "Attività di trattamento" in forza del rapporto contrattuale/convenzionale sopra citato, se necessari ed indispensabili a dar corso allo stesso e con i **mezzi, strumenti e le modalità** evidenziati in esso.

Con la sottoscrizione del presente Accordo i Contitolari si assumono gli impegni a garantire e garantiscono quanto di seguito riportato, mantenendo autonomi poteri decisorii, di direttiva e di controllo nei propri ambiti di competenza.

Obblighi generali

I Contitolari si impegnano a garantire e garantiscono:

1. di trattare i dati in ottemperanza ai principi sanciti:
 - dall'ordinamento nazionale ed europeo in materia di protezione dei dati;
 - dall'articolo 5 del Regolamento UE 679/2016 e norme di armonizzazione;

2. di inviarsi reciprocamente, con cadenza annuale, l'elenco aggiornato degli eventuali Amministratori di Sistema e degli eventuali terzi affidatari, designati Responsabili del trattamento dei dati afferenti al presente Accordo ;
3. di comunicarsi reciprocamente il luogo fisico di archiviazione dei dati sottoposto ad allocazione vincolante all'interno del territorio italiano, nonché le modalità di loro conservazione (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 responsabile esterno;
4. di attenersi ai criteri di segretezza e tutela nella gestione dei dati di cui trattasi, utilizzandoli al solo scopo di erogare le prestazioni di cui trattasi;
5. di non trattare i dati dell'interessato/utente oltre al tempo strettamente necessario ad espletare l'attività di competenza ed i connessi adempimenti amministrativo-contabili inerenti/derivanti;
6. di somministrare all'interessato/utente adeguata informativa e registrarne/acquisirne il consenso, ove previsto dalla vigente normativa nazionale e/o europea, con obbligo di condivisione preventiva con il Contitolare e conservazione insieme alla documentazione relativa all'interessato/utente per le prestazioni di afferenza e di dare ivi informativa relativamente alla Contitolarità di cui al presente Accordo, con particolare riguardo alle modalità di esercizio dei diritti dell'interessato/utente ed ai dati di contatto del R.P.D e/o referente privacy.

Ciascun Contitolare è tenuto a rispondere direttamente, a tutti gli effetti di legge, con manleva totale del Contitolare per eventuali violazioni di norme, inadempimenti giuridici, inosservanze regolamentari, nonché per i danni inerenti / derivanti dai trattamenti dati di cui trattasi di rispettiva competenza, per i quali l'altro Contitolare possa essere chiamato a rispondere, sia civilmente, sia in punto privacy.

Collaborazione

Ciascun Contitolare mette a disposizione dell'altro tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente accordo.

Tenuta del registro delle attività di trattamento

Ciascun Contitolare si impegna a redigere per iscritto, se previsto per legge, un registro delle attività di trattamento di cui trattasi per i trattamenti di afferenza, che contenga almeno le informazioni di cui all'art 30.2 del Regolamento UE 679/2016.

Comunicazione a terzi

Ciascun Contitolare deve rispettare il divieto assoluto di diffusione, condivisione, comunicazione a terzi e di trasferimento dati a soggetti situati in paesi terzi (extra UE), con particolare attenzione a soggetti giuridici afferenti l'indotto delle prestazioni sanitarie e sociali ovvero la fornitura/commercializzazione di beni e servizi ad essa afferenti.

Se il Contitolare intendesse comunque trasferire tutti o alcuni dati personali oggetto dell'Accordo verso un paese terzo o un'organizzazione internazionale, si impegna ad informare il Contitolare prima di procedere al trasferimento, fornendo indicazioni sulla base legale che legittima il trasferimento.

Ricorso a Responsabili esterni

Ciascun Contitolare può nominare responsabili esterni in relazione ai trattamenti di cui trattasi, nel rispetto delle previsioni di cui al regolamento europeo 679/2016 e norme di armonizzazione, mettendo a disposizione a richiesta del Contitolare i relativi dati di contatto.

Riservatezza dei dati trattati

Ciascun Contitolare ***si impegna a garantire e garantisce*** di mantenere la segretezza e riservatezza riguardo a dati e informazioni personali e non ai quali abbia avuto accesso in virtù del presente Accordo anche dopo il termine dello stesso.

Ciascun Contitolare ***si impegna a garantire e garantisce*** che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza od abbiano un adeguato obbligo legale di riservatezza.

Autorizzati al trattamento

Ciascun Contitolare ***si impegna a garantire e garantisce*** di:

- individuare tra i propri collaboratori, quelli che compiono operazioni di trattamento dati personali e categorie particolari di dati personali e nominarli quali persone autorizzate al trattamento;
- dare le istruzioni agli Autorizzati al trattamento circa gli obblighi previsti dalle vigenti disposizioni in materia di privacy;
- adoperarsi al fine di rendere effettive le suddette istruzioni, curando in particolare il profilo della riservatezza, della sicurezza di accesso e dell'integrità dei dati;
- 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 persona fisiche.

Diritti dell'interessato

Ciascun Contitolare adotta misure tecniche e organizzative adeguate atte a dare seguito alle richieste di esercizio dei diritti da parte degli interessati/utenti di cui al capo III del Regolamento UE 679/2016 tra le altre:

- Diritti di accesso, rettifica, cancellazione e opposizione;
- Diritto alla limitazione del trattamento;
- Diritto alla portabilità dei dati;
- Diritto di opposizione ad un processo decisionale automatizzato relativo alle persone fisiche;
- Violazione dei dati personali.

Ciascun Contitolare si impegna ad informare l'interessato/utente sulle modalità utilizzate per conservare i dati in modo da consentire la sua identificazione per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e/o successivamente trattati, avendo cura di applicare, in caso di conservazione digitalizzata, le norme vigenti in materia.

L'interessato/utente può esercitare i propri diritti nei confronti di e contro ciascuno dei Contitolari.

Ciascun comunque ***si impegna a garantire e garantisce:***

- di comunicare, a richiesta dell'altro Contitolare, in caso di esercizio dei diritti di cui e agli artt. da 15 a 21 e 23 del Regolamento UE n. 679/2016, i dati inerenti i file di log di accesso in formato intellegibile al fine di consentire la loro esibizione, come previsto all'interno del sopracitato Regolamento UE.

Su richiesta di un Contitolare o di un interessato/utente, l'altro Contitolare dà seguito direttamente e tempestivamente a dette richieste di esercizio dei diritti, dandone contestualmente comunicazione al Contitolare.

In caso di violazione, fuga o perdita di dati personali, Ciascun Contitolare del trattamento, contestualmente agli adempimenti previsti dal regolamento UE 679/2016 e norme di armonizzazione, informa l'altro Contitolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Nell'informare il Contitolare comunica le seguenti informazioni:

- Descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di dati personali oggetto della violazione;
- il nome ed i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere ulteriori informazioni;
- descrizione delle misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi sui diritti e libertà delle persone fisiche;
- descrizione delle probabili conseguenze della violazione dei dati personali.

Valutazione d'impatto

Se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto del presente Accordo, i Contitolari si impegnano a collaborare nella redazione

della Valutazione d'impatto sulla protezione dei dati e negli adempimenti conseguenti previsti dalla vigente normativa.

Consultazione preventiva

Se si rende necessaria la Consultazione preventiva dell'Autorità di Controllo, in merito alle attività di trattamento oggetto del presente Accordo, i Contitolari collaborano per la raccolta di tutte le informazioni necessarie e per la Redazione della Consultazione preventiva.

Responsabile della Protezione dei Dati

Ciascun Contitolare designa ai sensi dell'art. 37.1, un Responsabile della Protezione dei Dati (RPD) di cui al capo IV, Sezione 4, qualora rientrante nei casi previsti dall'art. 37.1 e, comunque, un referente Privacy e ne comunica i dati di contatto all'altro Contitolare.

Misure di sicurezza

Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, ma anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, Ciascun Contitolare mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Ciascun Contitolare deve implementare misure che garantiscano:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi in uso ai fini dello svolgimento delle Attività di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico;
- la verifica e valutazione periodica dell'efficacia delle misure tecniche e organizzative.

Nello specifico Ciascun Contitolare deve garantire comunque l'implementazione delle misure di sicurezza di carattere generale indicate nell'**Allegato B** "Misure di sicurezza".

Ciascun Contitolare comunque ***si impegna a garantire e garantisce:***

1. di osservare e applicare, anche per conto di eventuali terzi affidatari, le misure idonee alla sicurezza dei dati a norma del Regolamento UE n.679/2016 e relative norme di armonizzazione, con particolare riferimento all'applicazione del criterio di indispensabilità del dato nella cernita degli stessi;
2. di applicare, anche in caso di trattamento digitale dei dati, misure di sicurezza, volte ad eliminare o, comunque, a ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati personali e delle categorie particolari di dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle disposizioni contenute nel Regolamento U.E. 679/2016 e relative norme di armonizzazione;
3. di adottare le cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo

sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);

4. di comunicare per iscritto, in forma chiara, compiuta e specifica all'altro Contitolare entro e non oltre 60 giorni dal presente Accordo, le misure assunte a norma dello stesso, nonché, negli stessi termini e tempi, le modalità di conservazione dei dati, del loro ripristino, della gestione dei *data breach* e dei *file di log* relativi alla tracciabilità degli accessi;
5. di garantire il rispetto degli artt. da 32 a 36, con particolare riferimento all'art. 33 par. 2 del Regolamento UE n.679/2016 (*data breach*);
6. di comunicare per iscritto, in forma chiara, compiuta e specifica all'altro Contitolare le misure idonee alla sicurezza del dato, a norma del Regolamento UE n. 679/2016 e relative norme di armonizzazione;
7. di produrre acconcia documentazione scritta ovvero relazione circa il regolare adempimento di quanto sopra all'altro Contitolare e per esso al suo RPD.

Termine del rapporto

I termini di conservazione dei dati trattati sono definiti da ciascun Contitolare ai sensi della vigente normativa e ne viene data informativa all'interessato/utente nelle forme di legge in materia.

Ciò fatto salvo, la durata del presente Accordo segue il rapporto contrattuale/convenzionale sostanziale di cui in premessa a decorrere dall'effettiva attivazione dello stesso.

In caso di inadempimento di una delle parti agli obblighi derivanti dal presente Accordo, l'altra parte, previa formale diffida ad adempiere, in caso di persistente inadempienza nei termini assegnati, potrà procedere alla risoluzione-cessazione degli effetti del presente Accordo e del rapporto sostanziale sotteso, fatto salvo ed impregiudicato ogni diritto.

Obblighi del Titolare

Ciascun Contitolare fornisce ai propri autorizzati istruzioni precise sulle modalità di trattamento dei dati (come da presente Accordo e da **Allegato B**, sulle categorie di dati e sulla finalità per le quali vengono trattati.

Ciascun Contitolare garantisce che i dati siano stati raccolti in maniera lecita, per finalità determinate (indicate **nell'Allegato A**), e che i dati siano adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti.

Responsabilità

Ciascun Contitolare rimane responsabile delle attività di trattamento di cui al presente Accordo per le quali ha determinato finalità e mezzi del trattamento e manleva l'altro Contitolare da eventuali danni inerenti o derivanti dalla mancata osservanza delle presenti istruzioni e/o da comportamenti illeciti per fatto proprio o dei soggetti dei quali lo stesso si avvale.

Il presente Accordo potrà essere oggetto di revisione qualora successivamente alla sottoscrizione intervengano modifiche normative che comportino il suo adeguamento alla normativa nazionale e/o a quella europea.

Data e luogo _____

ASL 3

In persona del delegato del Legale Rappresentante

[*****]

In persona del Legale Rappresentante

.....

Allegati

Allegato A: "Attività di trattamento"

[*****]

Allegato B: "Misure di sicurezza" e "Istruzioni su mezzi e modalità trattamento" all'accordo relativo alle funzioni di Contitolare nel trattamento dei dati personali ai sensi del Regolamento Europeo n. 679/2016 e norme di armonizzazione:

INFORMAZIONI, MISURE DI SICUREZZA ED ISTRUZIONI OPERATIVE

Il Regolamento Europeo 679/2016 e norme di armonizzazione prevedono precisi obblighi per coloro che intendono procedere ad un trattamento di dati personali.

Tali obblighi si sostanziano in adempimenti dettagliati, omessi i quali scattano le sanzioni sia penali, sia amministrative, sia civili, poste a salvaguardia dei diritti tutelati.

La normativa in materia di protezione dei dati personali in oggetto individua tre figure fondamentali:

1. Il Titolare del trattamento;
2. Il Responsabile esterno del trattamento;
3. Gli autorizzati al trattamento
4. Il Responsabile per la Protezione dei Dati (R.P.D.).

Il Titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento od i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.. E' Responsabile dell'attuazione dei precetti normativi previsti dalla Legge.

Il titolare del trattamento è la A.S.L. 3.

Il Responsabile esterno del trattamento, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. E' nominato dal titolare, nella persona del legale rappresentante pro-tempore anche tramite delega alla sottoscrizione e deve provvedere all'applicazione di tutti i compiti impartiti dal Titolare, nonché fornire, agli autorizzati al trattamento istruzioni in merito alle operazioni di raccolta e trattamento dei dati, nonché vigilare sulla corretta applicazione delle medesime.

L'autorizzato al trattamento, nominato dal Titolare o dal Responsabile esterno, anche tramite delega alla sottoscrizione, deve elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni impartite.

All'autorizzato del trattamento sono devoluti compiti volti a garantire una puntuale applicazione della vigente normativa in materia di protezione dei dati.

Il Responsabile per la Protezione dei dati Personali R.P.D: è una figura, obbligatoria nei casi previsti dal Regolamento U.E. 679/2016 e norme di armonizzazione, che sovrintende a tutte le attività di protezione dei dati e che costituisce il soggetto di raccordo con l'autorità di controllo (Autorità garante per la Protezione dei dati) e con gli interessati/utenti.

Questa comunicazione è l'allegato dell'Accordo di Contitolarità nel trattamento dei dati personali nell'ambito dei rapporti che La legano all'A.S.L. 3 individuati nello stesso.

Si ricorda che per trattamento si intende " qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"

Si fa presente che, per quanto riguarda il trattamento dei dati personali, lo stesso si considera lecito se ricorre almeno una delle seguenti condizioni (art. 6 comma 1 Regolamento Europeo 679/2016 e norme di armonizzazione):

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, salvi i casi in cui non è richiesto ai sensi della medesima normativa (tra gli altri art.9.2 Regolamento Europeo 679/2016) e disposizioni di armonizzazione;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Il Regolamento Europeo 679/2016 e norme di armonizzazione che regolano il trattamento dei dati personali prevede il trattamento di dati personali *(qualsiasi informazione riguardante una persona fisica identificata o identificabile «interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale)* e di dati c.d. "particolari" (che il D. Lgs. 196/2003 e s.m.i. definiva quali "dati sensibili" e richiamati dall'art.9 del Regolamento Europeo 2016/679), *cioè i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

Il Contitolare è tenuto in relazione a detti trattamenti dati:

- a) Ad effettuarli in modo lecito, corretto e trasparente e nel rispetto dei principi sanciti dal Regolamento UE 679/2016 e norme di armonizzazione;
- b) a raccogliarli e registrarli per finalità determinate, esplicite e legittime, e successivamente a trattarli in modo che non siano incompatibili con tali finalità;
- c) a verificare, ove possibile, la loro esattezza e, se necessario, aggiornarli;
- d) a verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;
- e) a conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali sono stati raccolti o successivamente trattati, rispettando le misure di sicurezza predisposte. In ogni operazione di trattamento andrà garantita la massima riservatezza;
- a) a osservare scrupolosamente tutte le misure di sicurezza predisposte ed idonee ai sensi della vigente normativa in materia.

Nell'espletamento dell'Accordo di cui trattasi ciascun Contitolare e ciascun autorizzato dallo stesso, dovrà, inoltre:

1. adempiere agli obblighi di cui all'Accordo stesso;
2. collaborare con il R.P.D. Aziendale e con l'altro Contitolare per l'attuazione delle prescrizioni in materia di privacy;
3. attuare le misure di sicurezza informatiche e non informatiche idonee a rispettare le indicazioni del Regolamento Europeo 679/2016 e norme di armonizzazione ;
4. garantire il rispetto degli artt. da 32 a 36, con particolare riferimento all'art. 33 par. 2 del Regolamento UE n.679/2016 (*data breach*);
5. accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
6. attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto dalla normativa vigente, nei confronti dell'interessato;
7. conservare gli atti e documenti, contenenti dati personali utilizzati per lo svolgimento dei compiti propri, in contenitori muniti di serratura (cassetti, armadi, ecc.) e restituirli al termine delle operazioni di competenza. Sulla base di quanto sopra, in caso di allontanamento, anche temporaneo, dalla postazione di lavoro dei suoi autorizzati al trattamento, il Contitolare dovrà verificare che non vi sia la possibilità da parte di terzi,

anche dipendenti, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;

8. testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative volte a garantire la sicurezza dei trattamenti espletati;
9. in caso di utilizzo di strumento elettronico, lo stesso non dovrà mai essere lasciato incustodito e accessibile durante una sessione di trattamento. In particolare si ricorda che anche in caso di abbandono temporaneo della postazione di lavoro, il personal computer con il quale si sta operando un'operazione di trattamento dei dati dovrà essere spento, dopo aver effettuato il salvataggio dei dati oppure dovrà essere attivato lo screensaver con inserimento di password personale al fine di evitare la riapertura a terzi della sessione di trattamento in corso;
10. Sempre in caso di utilizzo di strumento elettronico, nel caso di informazioni memorizzate sulle memorie locali dei personal computer e affidate esclusivamente agli utenti, effettuare il tempestivo salvataggio dei dati;
11. Qualora il trattamento dei dati, la formazione e la comunicazione di documenti ed atti, avvenga con strumenti elettronici dovranno essere accuratamente applicate, tra le altre, le seguenti misure di sicurezza:
 - dovranno essere predisposte tutte le cautele necessarie per assicurare la segretezza della componente riservata della credenziale di autenticazione (codice associato a parola chiave o dispositivo di autenticazione conosciuto o in possesso e uso esclusivo del responsabile esterno e dei soggetti dallo stesso autorizzati);
 - la password personale dovrà essere modificata periodicamente e ogni qualvolta l'autorizzato al trattamento abbia motivo di ritenere che non sia di sua esclusiva conoscenza;
 - i supporti rimovibili (floppy disk, cd rom, chiavette USB, ecc.) su cui sono memorizzati copie di dati dovranno essere custoditi in appositi contenitori muniti di serratura (armadi, cassette, ecc.), al fine di evitare accessi non autorizzati e trattamenti non consentiti o comunque custoditi in locali ad accessi autorizzati e chiusi a chiave;
 - i supporti rimovibili contenenti dati sensibili, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri autorizzati solo se le informazioni precedentemente in essi contenute non sono intelligibili e in nessun modo tecnicamente ricostruibili.
12. mantenere aggiornate costantemente e conservare le informazioni contenute nel Registro dei Trattamenti di cui all'art.30.2 del Regolamento UE 679/2016 e norme di armonizzazione, qualora previsto per legge;
13. adottare le cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici

di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);

14. Collaborare con il Contitolare nella redazione della Valutazione d'impatto sulla protezione dei dati e negli adempimenti conseguenti, se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto dell'Accordo;
15. Collaborare con il Contitolare ed il R.P.D. per l'evasione di eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati ed ulteriori esercizi di diritti su istanza dall'interessato ai sensi del Regolamento UE 2016/679 e norme di armonizzazione.
16. comunicare, a richiesta del Contitolare, in caso di esercizio dei diritti di cui e agli artt. da 15 a 21 e 23 del Regolamento UE n. 679/2016, i dati inerenti i *file di log* di accesso in formato intellegibile al fine di consentire la loro esibizione, come previsto all'interno del sopracitato Regolamento UE;
17. inviare, con cadenza annuale, al Contitolare l'elenco aggiornato degli Amministratori di Sistema e degli eventuali terzi affidatari, designati Responsabili del trattamento dei dati afferenti l'Accordo;
18. comunicare al Contitolare il luogo fisico di archiviazione dei dati sottoposto ad allocazione vincolante all'interno del territorio italiano, nonché le modalità di loro conservazione (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 designato preventivamente a responsabile esterno;
19. Procedere all'individuazione di eventuali soggetti sotto propria responsabilità da autorizzarsi al trattamento dei dati personali o di categorie particolari di dati personali e procedere alla loro autorizzazione al trattamento, completa di specifiche istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun autorizzato, nonché ciascun Contitolare dovrà vigilare, che l'accesso ai dati da trattare da parte degli autorizzati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni ciascun Contitolare dovrà anche verificare la permanente sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto procedere alla revoca delle stesse. La nomina ad autorizzato dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti , che effettuano trattamento dei dati inerente l'Accordo di cui trattasi.

Per quanto concerne la gestione degli archivi cartacei dovranno essere adottate misure di sicurezza idonee e comunque:

1. Tutti i documenti dovranno essere accuratamente custoditi all'interno degli appositi locali o contenitori amovibili muniti di serratura;
2. L'accesso all'interno degli archivi dovrà essere rigorosamente limitato alle persone autorizzate dal Contitolare ed addette a tale attività;
3. Deve essere vietato allontanarsi dagli archivi, dalla segreteria e dagli uffici lasciando i locali incustoditi;

4. Gli atti ed i documenti contenenti dati personali, utilizzati per lo svolgimento dei compiti propri devono essere conservati accuratamente in contenitori e/o locali muniti di serratura e restituiti al termine delle operazioni affidate;
5. Nessun dato potrà essere comunicato a terzi o diffuso, al di fuori di quanto previsto nell'Accordo di cui trattasi;
6. E' comunque vietata la diffusione dei dati inerenti lo stato di salute e la vita sessuale degli interessati;
7. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica e/o cessazione del rapporto sotteso all'Accordo.

Data e luogo _____

ASL 3

In persona del delegato del Legale Rappresentante

[*****] In persona del Legale Rappresentante

.....