Accordo Data Protection fra Titolare e Responsabile
(Data Protection Agreement)

OGGETTO: Nomina ex articolo 28 del Regolamento UE 2016/679 relativamente alle attività di conduzione studi epidemiologici sull'epidemia di CoViD-19

TRA

Regione Toscana, con sede legale in piazza Duomo 10, in persona del suo legale rappresentante- codice fiscale 01386030488, rappresentata in questo atto dal direttore della Direzione Diritti di Cittadinanza e Coesione Sociale, Dott. Carlo Rinaldo Tomassini, nato a _____- il _____-, domiciliato per la carica presso la sede dell'Ente, il quale interviene esclusivamente in nome, per conto e nell'interesse del medesimo Ente - Titolare

E

Agenzia regionale di sanità della Toscana con sede legale in Firenze – Via Pietro Dazzi, n. 1 - codice fiscale 04992010480, rappresentata in questo atto dal direttore, Dott. Mario Braga, nato a _____ il _____, domiciliato per la carica presso la sede dell'Ente, il quale interviene esclusivamente in nome, per conto e nell'interesse del medesimo Ente - Responsabile

Titolare e Responsabile verranno in seguito entrambi indicati congiuntamente "le Parti".

ART. 1 TRATTAMENTO DEI DATI PERSONALI

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali (Reg. UE n. 2016/679, di seguito "GDPR", nonché D. Lgs. 196/2003 da ultimo novellato dal D. Lgs. 101/2018, di seguito "Codice Privacy") ed in relazione alle operazioni che vengono eseguite per lo svolgimento delle attività previste dall'articolo art. 82-bis "Compiti e attribuzioni." della legge regionale n. 40/2005 e ss.mm. e l'adempimento di quanto previsto nel Titolo III, Capo I, della medesima legge citata, la Regione Toscana, in qualità di Titolare, nomina l'Agenzia regionale di sanità, Responsabile del trattamento, ai sensi dell'articolo 28 GDPR.

I dati affidati dal Titolare al Responsabile sono:

banca dati SISPC per la parte relativa ai pazienti COVID prevede le seguenti variabili di estremo interesse storicizzate nel tempo: Comune sorveglianza, Esito (RSA; Ric. Ospedaliero, Isolamento domiciliare, guarigione, decesso), Data del contagio, Medico Curante, Data contagio, Comune nascita, Comune residenza, Indirizzo residenza, Data inizio Data fine presa in carico , Ufficio di Igiene preposto alla sorveglianza. Possiede inoltre l'informazione del codice fiscale che può essere pseudonimizzata dagli uffici regionali preposti e linkata all'identificativo universale del soggetto (IDUNI)

Tutti i suddetti dati, infatti, saranno trasmessi in formato elettronico dagli Uffici Competenti della Direzione Diritti di cittadinanza e coesione sociale, in forma pseudonimizzata previa sostituzione di tutti gli identificativi in chiaro con il Codice Unico Regionale

Le operazioni di trattamento effettuate da ARS riguardano l'analisi epidemiologica dei suddetti dati anche attraverso il linkage con Anagrafe Sanitaria e dati sanitari correnti trasmessi ad ARS con i seguenti flussi:

1. Schede di dimissione Ospedaliera (SDO)
2. Emergenza-Urgenza 118 (RFC 134)
3. Pronto soccorso (RFC 106)
4. Prestazioni ambulatoriali (SPA)
5. Prestazioni farmaceutiche (SPF)
6. Farmaci erogati direttamente (FED)
7. Esenzioni per patologia o invalidità (RFC 192)
8. Prestazioni riabilitazione ex art. 26 L.833/78 (SPR)
9. Flusso Assistenza Domiciilare \ Residenze Sanitarie Assistite AD/RSA
10. Scheda di morte (RFC 148)

La trasmissione ai server ARS avverrà attraverso un canale sicuro protetto da crittografia. Nello specifico sarà utilizzato il protocollo https che garantisce la comunicazione all'interno di una connessione criptata, con chiave asimmetrica, dal Trasport Layer Security, previa autenticazione.

La finalità perseguita è:

a. progettare e relizzare un sistema di sorveglianza a partire dai dati della Banca Dati SISPC, che è stata indicata come la banca dati più completa tra quelle a dispozione di Regione Toscana per la sorveglianza saniataria dei pazienti COVID 19, integrandoli con i dati dei flussi correnti, che consenta di identificare precocemente nuovi focolai epidemici e le catene di trasmissione che li hanno generati attraverso la georeferenziazione degli indirizzi di residenza e\o luogo di contagio;
b. Studiare e proporre possibili integrazione degli attuali flussi, anche con l'utilizzo di sistemi innovativi basasti sulla connettività wireless e bluetooth;
c. Valutare l'impatto e l'efficacia degli strumenti di sanità pubblica adottati nella prima fase dell'epidemia;
d. Analizzare i fattori che aumentano il rischio di contrarre l'infezione e le condizioni che ne favoriscono la progressione e la morte.

I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno al completamento della presente convenzione ovvero in caso di sua risoluzione, per qualsiasi altro motivo.
Se una disposizione del presente articolo è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni del medesimo rimangono inalterate. In questo caso, Titolare e Responsabile concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi comuni.

L'Agenzia regionale di sanità, in quanto Responsabile, fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti normativi sanciti dal GDPR, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per garantire la riservatezza e la protezione dei diritti degli interessati.
L'Agenzia regionale di sanità, in quanto Responsabile, è tenuto ad assicurare e far assicurare ai propri dipendenti, collaboratori e responsabili ulteriori, la riservatezza ed il corretto trattamento delle

informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione.
In tal senso il responsabile, si impegna a consegnare, alla firma del presente accordo, al Titolare e al DPO di Regione Toscana "il disciplinare di comportamento degli autorizzati e degli altri dipendenti" coinvolti in modo e diretto o indiretto nella esecuzione dei trattamenti svolti per conto del Titolare e delle istruzioni impartite agli autorizzati nei loro relativi ruoli.

In particolare, ai sensi dell'art. 28 GDPR, l'Agenzia regionale di sanità si impegna a:

1. adottare e mantenere aggiornato un proprio registro dei trattamenti, concordandone la struttura e le modalità di aggiornamento, con il DPO di Regione Toscana entro 30 giorni dalla firma del presente accordo;
2. non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto del presente accordo e presenti, se sia adottato, nel registro dei trattamenti. In tal senso renderà accessibile al Titolare il registro dei trattamenti, attivati per effetto dell'accordo, consentendo operazioni di consultazione, approvazione e diniego in relazione a singoli o gruppi di trattamenti.
3. fornire per iscritto agli autorizzati al trattamento le necessarie istruzioni in tema;
4. nominare gli autorizzati che svolgono le funzioni di "amministratore di sistema", ai sensi dei provvedimenti del Garante italiano per la protezione dei dati personali del 27/11/2008 e del 25/6/2009, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e comunicandone al titolare l'elenco nominativo con i relativi ambiti di operatività;
5. di collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare;
6. predisporre e trasmettere, con cadenza annuale e comunque ogni qualvolta ciò appaia necessario, al Titolare una relazione in merito agli adempimenti eseguiti e alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate ed aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi;
7. assistere e garantire il titolare del trattamento nell'evasione delle richieste e del rispetto dei tempi previsti, nei rapporti con l'Autorità Garante per la protezione dei dati personali,
8. assistere il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto verso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei tempi prescritti,
9. assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento, ed in particolare al Security IT Manager del Titolare se nominato, nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento, della tipologia di dati trattati, delle categorie e numerosità degli interessati,
10. garantire al Titolare, su richiesta, l'accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del titolare, consentendo in tal modo la piena continuità dei servizi oggetto del presente appalto e in modo che mai si configuri una situazione di lock in. Il Titolare deve essere sempre messo in condizione di poter garantire la continuità del servizio.
11. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso

    a. la pseudonimizzazione e la cifratura dei dati personali (ARS tratterà dati pseudonimizzati

attraverso l'attribuzione da parte di Regione Toscana di un codice identificativo universale -IDUNI- in luogo degli elementi identificativi diretti);

b. la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;

c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati 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.

A tal fine si impegna: ad assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento, ed in particolare al Security IT Manager del Titolare.

1. Il Responsabile si impegna a restituire tutti i dati personali di pertinenza del Titolare, dopo che è terminata la prestazione dei servizi relativi al trattamento, cancellando le copie esistenti in proprio possesso, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati. In tal senso entro 120 giorni dalla firma del presente accordo l'Agenzia regionale di sanità e il responsabile dell'accordo per la Regione Toscana, concordano modalità, tempi e forme idonee a garantire il non precostituirsi di situazioni di lock in, inteso come la diminuzione o perdita della possibilità da parte del Titolare di garantire i servizi, senza ricorrere forzatamente al soggetto Responsabile, e di gestire agevolmente, in modo sicuro e con tempi ragionevoli, la chiusura della convenzione e l'eventuale subentro di un nuovo contraente o la gestione in autonomia in toto o in parte dei servizi. Tale accordo documentato viene messo a disposizione del Titolare e del DPO della Regione Toscana. Resta salva la possibilità di ri-uso di dati resi anonimi per finalità di ricerca scientifica.
2. il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili;
3. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione, su richiesta del titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal regolamento UE, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato, ivi compresa, se necessario, l'attività di monitoraggio e controllo da parte del DPO e del Security IT Manager, sulle misure di sicurezza attuate e sulla loro efficacia fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura.
4. Comunicare al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati" (DPO), qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali (DPO) del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati (DPO) del Titolare.
5. Comunicare al Titolare, al DPO e al Security Manager il nome e i riferimenti di contatto del proprio Responsabile della sicurezza IT.

6. Mettere in atto gli interventi necessari qualora l'attività di monitoraggio e controllo mettesse in evidenza punti di debolezza nelle misure e nelle tecniche adottate o qualora durante l'esecuzione del Contratto, la normativa in materia di Trattamento dei Dati Personali generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti;
7. Fornire e a mantenere aggiornato il catalogo degli asset (comprese le applicazioni utente e quelle di gestione dei sistemi e degli apparati), delle minacce e delle misure di sicurezza adottate e delle loro correlazioni al fine di una agevole valutazione dei rischi in fase di DPIA. A tal fine Titolare concorda entro 30 giorni dalla firma dell'accordo, con il responsabile di contratto e il Security IT Manager oppure con il responsabile della sicurezza del committente, i contenuti e i formati dei cataloghi al fine della condivisione e l'aggiornamento di tali informazioni.
8. Fornire al Titolare e al DPO la propria policy, contenente le misure tecniche, organizzative e di processo al fine di fare fronte ai principi del GDPR con riferimento particolare all'accountability, alla Data Protection by Design e by Default, alla tenuta del registro dei trattamenti, alla garanzia del rispetto dei diritti degli interessati di cui al Capo III del regolamento e alla consapevole responsabilizzazione del proprio personale coinvolto nel trattamento dei dati, che avviene per conto del Titolare.

ART 2 - Penali

Nel caso in cui il Responsabile agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, il Titolare potrà risolvere la presente convenzione, salvo il risarcimento del maggior danno.

Data --/--/----

per la
Regione Toscana

per la
Agenzia regionale di sanità