

Accordo Data Protection fra Titolare, Responsabile

(Data Protection Agreement)

TRA

..... [specificare il nome del Titolare], con sede legale in [specificare l'indirizzo della sede legale],
in persona del suo legale rappresentante[specificare il nome completo del legale rappresentante]

E

Agenzia regionale di sanità della Toscana con sede legale in Firenze – Via Pietro Dazzi, n. 1 - codice fiscale 04992010480, rappresentata in questo atto dalla direttrice, Dott.ssa Lucia Turco, domiciliata per la carica presso la sede dell'Ente, la quale interviene esclusivamente in nome, per conto e nell'interesse del medesimo Ente

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

Premesse

(A) Il trattamento affidato al Responsabile è relativo ai dati necessari all'attività di analisi e monitoraggio dell'antibiotico-resistenza, in riferimento al mandato istituzionale dell'Agenzia di cui agli artt. 82 e ss della legge regionale n. 40/2005 e a quanto previsto dall'Allegato C) del DPCM 3 marzo 2017.

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

(C) 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

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

(E) 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.

(F) 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.

Le Parti convengono quanto segue:

Art. 1

Descrizione del trattamento

1.1 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'accordo di collaborazione tra l'Azienda e l'Agenzia regionale di sanità nell'ambito delle attività di monitoraggio e controllo della diffusione di microrganismi multiresistenti agli antibiotici.

L'Azienda, in qualità di Titolare, nomina l'Agenzia regionale di sanità, Responsabile del trattamento, ai sensi dell'articolo 28 GDPR.

I trattamenti affidati dal Titolare al Responsabile riguardano le prestazioni eseguite in regime di ricovero o in pronto soccorso e a livello ambulatoriale presso la propria struttura. Le prestazioni oggetto della sorveglianza includono: i referti di esami microbiologici colturali, i relativi profili di resistenza e ricerca di attività tossinogeniche (*Clostridioides difficile*). I dati raccolti comprendono le seguenti categorie di informazioni:

1. Identificativo individuale univoco;
2. Identificativi della prestazione (laboratorio, identificativo prestazione e data di prelievo);
3. Identificativo del luogo di prelievo, in particolare ospedale, reparto, data del ricovero;
4. Dati relativi al paziente (sesso ed età);
5. Dati relativi all'esame (tipo di prestazione, materiale analizzato);
6. Dati relativi al referto dell'esame (isolato, profilo di resistenza).

ARS si impegna a includere i dati nel database della rete SMART (Delibera n. 1138 del 9/12/2014) finalizzata alla **sorveglianza** microbiologica e dell'antibiotico-resistenza in Toscana.

La finalità è pubblicare analisi di questi dati a livello aggregato e anonimo sul portale di ARS. Inoltre, come previsto dal Piano Nazionale della Prevenzione (PNP) 2020-2025 (https://www.salute.gov.it/imgs/C_17_notizie_5029_0_file.pdf) verranno utilizzati per contribuire al sistema di sorveglianza AR-ISS.

Art. 2

Obblighi del Responsabile del trattamento

2.1 Ai sensi dell'art. 28 GDPR, [riferimento al soggetto individuato come Responsabile] si impegna a:

2.2 adottare e mantenere aggiornato un proprio registro dei trattamenti, qualora il Responsabile ricada nelle fattispecie previste dal GDPR, anche concordando la struttura e le modalità di aggiornamento, con il DPO della Agenzia regionale di sanità;

2.3 non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto del presente accordo. A tale scopo il Responsabile renderà accessibile al Titolare il registro dei trattamenti, consentendo operazioni di consultazione, approvazione e diniego in relazione ai trattamenti censiti;

2.4 fornire per iscritto agli autorizzati al trattamento le necessarie istruzioni in tema;

2.5 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;

2.6 collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare;

2.7 predisporre e trasmettere, con cadenza annuale e comunque ogni qualvolta ciò appaia necessario, al Titolare Agenzia regionale di sanità - 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;

2.8 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;

2.9 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;

2.10 assistere ed assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento, ed in particolare al CISO 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;

2.11 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;

2.12 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 DPO del Responsabile collabora e si tiene in costante contatto con il DPO del Titolare;

2.13 comunicare al Titolare, al DPO e al CISO (se nominato) il nome e i riferimenti di contatto del proprio Responsabile della sicurezza IT;

2.14 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 CISO (se nominato), 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;

2.15 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.

Art. 3

Misure di sicurezza

3.1 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.

3.2 Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati. Le parti stabiliscono che le misure tecniche e organizzative adeguate con cui il Responsabile del trattamento è tenuto ad assistere il Titolare del trattamento nell'applicazione del presente punto, nonché l'ambito di applicazione e la portata dell'assistenza richiesta, sono le seguenti:

- misure di pseudonimizzazione e cifratura dei dati personali
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- misure di identificazione e autorizzazione dell'utente;
- misure di protezione dei dati durante la trasmissione;

- misure di protezione dei dati durante la conservazione;
- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati;
- misure per garantire la registrazione degli eventi;
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita;
- misure di informatica interna e di gestione e governance della sicurezza informatica;
- misure di certificazione/garanzia di processi e prodotti (in corso di realizzazione);
- misure per garantire la minimizzazione dei dati;
- misure per garantire la qualità dei dati;
- misure per garantire la conservazione limitata dei dati;
- misure per garantire la responsabilità;
- misure per consentire la portabilità dei dati e garantire la cancellazione.

A tal fine si impegna ad assistere ed assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento e al CISO del Titolare.

3.3 Il Responsabile del trattamento si impegna a 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.

3.4 Nei casi in cui il Responsabile effettui trattamenti di conservazione dei dati personali del Titolare nel proprio sistema informativo, garantisce la separazione di tipo logico di tali dati da quelli trattati per conto di terze parti o per proprio conto. Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate a salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al Titolare, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.5 Conformemente alla disposizione di cui all'art. 28 comma 1 del Regolamento e alla valutazione delle garanzie che il Responsabile del trattamento deve presentare, lo stesso Responsabile attesta, a mezzo della sottoscrizione del presente accordo, la conformità della propria organizzazione almeno ai parametri di livello minimo di cui alle misure di sicurezza individuate da Agid la circolare n. 2/2017.

3.6 Il Responsabile si impegna a mettere a disposizione del Titolare la procedura adottata per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 4

Soggetti autorizzati ad effettuare i trattamenti - Designazione

4.1 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.

4.2 In tal senso, il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali effettuati per conto dell'Ente e che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando all'Ente le evidenze di tale formazione. Con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza. In ogni caso il Responsabile del trattamento è direttamente ritenuto Responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

Art. 5

Obblighi in materia di violazioni di dati personali (“data breach”)

5.1 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.

5.2 Il Responsabile si impegna a fornire al Titolare del trattamento specifico report relativo alla violazione di sicurezza occorso entro il termine sopra indicato; tale documento dovrà contenere quantomeno:

- a) una descrizione relativa alla natura della violazione dei dati personali compresi, ove possibile, dell'indicazione delle categorie e del numero approssimativo di interessati in questione nonché delle categorie e del numero approssimativo di registrazioni dei dati personali in questione;
- b) l'indicazione del nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) una descrizione delle probabili conseguenze della violazione dei dati personali;
- d) una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

5.3 Il Responsabile si impegna a supportare il Titolare nella gestione della violazione dei dati personali, anche nell'eventuale comunicazione agli interessati.

Art. 6

Trasferimenti di dati personali in paesi extra-UE

6.1 Il Responsabile del trattamento si impegna a non trasferire i dati personali di cui al presente accordo verso un paese terzo o un'organizzazione internazionale se non su istruzione documentata del Titolare o per adempiere a una norma del diritto dell'Unione o dello Stato membro cui è soggetto il Responsabile del trattamento.

Art. 7

Durata dell'accordo

7.1 I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno al completamento del contratto/convenzione ovvero in caso di conclusione dell'attività di trattamento o in caso di sua risoluzione, o 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.

7.2 Il Responsabile del trattamento 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. Il Titolare e il Responsabile concordano modalità, tempi e forme idonee a garantire il non precostituirsi di situazioni di lock in.

Art. 8

Ricorso a Sub-Responsabili del trattamento di dati personali

8.1 Nell'ambito dell'esecuzione del presente accordo, il Responsabile deve sottoporre a preventiva autorizzazione scritta e specifica del Titolare qualsiasi affidamento di trattamenti ad ulteriore Responsabile (cd. "sub-Responsabile") fornendo allo stesso le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

8.2 L'autorizzazione specifica di cui al punto che precede è subordinata al possesso da parte del "sub-Responsabile" dei seguenti requisiti:

- a) sede legale in uno degli Stati membri dell'UE
- b) non siano trasferiti i dati in Paesi extra UE
- c) il sub-Responsabile è subappaltatore o partner del Responsabile del trattamento sulla base di contratti continuativi di cooperazione, servizio e/o fornitura
- d) il sub-Responsabile sia in possesso della certificazione ISO/IEC 27001 o, parimenti, presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato dello stesso livello del Responsabile del trattamento
- e) i compiti e le responsabilità correlate al trattamento dei dati personali di titolarità dell'Ente siano disciplinate da atto scritto tra Responsabile e Sub-Responsabile

Art. 9

Risoluzione delle controversie e manleva

9.1 Eventuali controversie che dovessero insorgere legate alla possibilità che il Responsabile possa aver agito in modo difforme o contrario alle legittime istruzioni del Titolare oppure abbia adottato misure di sicurezza inadeguate rispetto al rischio del trattamento, saranno risolte, in prima istanza, secondo procedimento amichevole tra le Parti tramite richiesta da parte del Titolare di apertura di una procedura di conciliazione della controversia. Un referente del Titolare (il DPO, se nominato) e un referente del Responsabile (il DPO, se nominato) porteranno avanti la composizione della controversia in tempi ragionevoli.

9.2 Il Responsabile del trattamento tiene indenne e manleva il Titolare da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Responsabile del trattamento delle disposizioni contenute nel presente Accordo.

9.3 Le Parti riconoscono e convengono che il rispetto delle istruzioni di cui al presente accordo, nonché alle prescrizioni della normativa applicabile, non producono l'insorgere di un diritto in capo al Responsabile del trattamento al rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per conformarsi.

Art.10

Inosservanza delle clausole e risoluzione

10.1 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.

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

a) 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;

b) 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;

c) 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 o del regolamento (UE) 2016/679;

d) dopo aver esperito ogni tentativo di conciliazione, la controversia non venga risolta entro 30 giorni dall'avvio della procedura, e venga altresì comprovata la causa esclusiva di inadempienza da parte del Responsabile. Pertanto, questi risponderà del danno causato agli "interessati" e il Titolare potrà risolvere il contratto, salvo il risarcimento del maggior danno.

10.3 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, il Titolare del trattamento insista sul rispetto delle istruzioni.

10.4 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.

Firenze, _____

Il Titolare del trattamento*

Il Responsabile del trattamento*

* *Firmato digitalmente*