SCHEMA DI CONVENZIONE TRA REGIONE DEL VENETO E AZIENDA ZERO PER LA NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

(ex art. 28 del Regolamento Europeo sulla protezione dei dati n° 679 del 27 aprile 2016 del Parlamento e del Consiglio Europeo)

Il giorno... il mese e l'anno.....

TRA

Regione del Veneto-Giunta Regionale, Titolare del trattamento ai sensi del Regolamento (UE) 2016/679, (di seguito "Regione" o "Titolare"), con sede legale in Venezia, Dorsoduro 3901, codice fiscale 80007580279, che interviene al presente atto in persona……

E

l'Azienda per il Governo della Sanità della Regione del Veneto - Azienda Zero in persona del legale rappresentante pro tempore, con sede in Padova, Passaggio Gaudenzio 1, C.F. e P. IVA: 05018720283, in qualità di Responsabile del trattamento ai sensi del Regolamento (UE) 2016/679 (di seguito "Azienda" o "Responsabile")

PREMESSO CHE

- Il decreto legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221, recante "Ulteriori misure urgenti per la crescita del Paese", così come modificato dall'articolo 17, comma 1, del decreto legge 21 giugno 2013, n. 69 convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98 recante "Disposizioni urgenti per il rilancio dell'economia", disciplina, all'articolo 12, il "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario" quale insieme di dati e di documenti digitali di tipo sanitario e socio- sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, istituito dalle regioni e province autonome a fini di: a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifica delle qualità' delle cure e valutazione dell'assistenza sanitaria ;
- il D.P.C.M. 29 settembre 2015, n. 178, recante "Regolamento in materia di fascicolo sanitario elettronico", individua, tra l'altro, i titolari del trattamento dei dati del Fascicolo sanitario elettronico in ragione delle finalità perseguite stabilendo: all'articolo 10 che per finalità di cura sono titolari del trattamento *"i soggetti del SSN e dei Servizi socio sanitari regionali che prendono in cura l'assisti*to, *presso cui sono redatti I dati e I documenti sanitari che alimentano il FSE",* all'articolo 15 che per le finalità di ricerca sono titolari del trattamento "le regioni e le province autonome e il Ministero della salute" e all'articolo 18 che per le finalità di governo i titolari sono "le regioni e province autonome, il Ministero della salute e il Ministero del lavoro e delle politiche sociali";
- la legge regionale 25 ottobre 2016, n. 19 "Istituzione dell'ente di governance della sanità regionale veneta denominato "Azienda per il governo della sanità della Regione del Veneto - Azienda Zero". Disposizioni per la individuazione dei nuovi ambiti territoriali delle aziende ulss", all'articolo 2, comma 1, lett. g), punto 11, pone in capo ad Azienda Zero la gestione di attività tecnico-specialistiche per il sistema e per gli enti del servizio sanitario regionale. In particolare è posta in capo ad Azienda Zero, "la attivazione entro un anno dall'entrata in vigore della presente legge del fascicolo sanitario elettronico e la conseguente tessera sanitaria elettronica per tutta la popolazione veneta". Viene inoltre previsto che "entro novanta giorni dall'entrata in vigore della presente legge, l'Azienda Zero sentita la commissione consiliare competente, approva i decreti attuativi del fascicolo sanitario elettronico con particolare riferimento alla realizzazione di un'unica rete regionale per interconnettere tutte le aziende

sanitarie e gli enti socio-sanitari; gli enti privati convenzionati del sistema socio-sanitario avranno l'obbligo di partecipare al fascicolo sanitario elettronico anche ai fini dell'accreditamento".

Tenuto conto dei compiti e responsabilità specifici del Responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'Interessato;

Visto l'art. 4, paragrafo 1, n. 7 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)» (di seguito "GDPR"), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, che individua il Titolare del trattamento ne «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 …»* e visto altresì l'art. 4, paragrafo 1, n. 8) del Regolamento, che identifica il Responsabile del trattamento ne «la *persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dat*i personali per conto del titolare del trattamento»;

Visto l'articolo 28, paragrafo 3, del GDPR che dispone che *" i trattamenti da parte di un responsabile* del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto del*l'Unione europea o degli stati membri, che vincoli il responsabile del trattamento al titolare del* trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Dato atto che Azienda Zero risulta soddisfare la previsione di cui all'art. 28, comma 1, del Regolamento Europeo 2016/679, in base al quale "qualora un trattamento debba essere effettuato per *conto del Titolare del Trattamento, quest'ultimo ricorre unicamente a Responsabili del trattamento* che presentino 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*". Invero, Azienda Zero risulta soddisfare quanto richiesto dalla norma citata, tra l'altro, alla luce:

- delle previsioni di cui all'art. 2 della L.R. 19 del 2016;
- delle risorse e delle competenze possedute;
- dell'incarico già attribuito ad Azienda Zero , con DGR 1894/2019 di svolgimento delle attività e delle funzioni di Autorità Nis (Network and Information Security) in ambito sanitario, come previsto dall'art. 7 del D.Lgs. 65/2018, nonché delle attività correlate al ruolo regionale di coordinatore per le Regioni e Province Autonome delle iniziative e degli adempimenti previsti in attuazione del D.Lgs. 65/2018 per il perimetro sanità, (ossia a diffondere e sensibilizzare l'adozione delle linee guida, predisposte dalle Autorità competenti NIS in materia di cybersecurity, con particolare attenzione alle metodiche analisi del rischio cyber, alle misure di sicurezza e alle procedure di notifica degli incidenti);
- della esperienza già maturata con particolare riferimento al Fascicolo Sanitario Elettronico regionale;
- del Piano Sistema Informativo Socio Sanitario Regionale 2019-2023, approvato da Azienda Zero e recepito con DGR 252 del 2 marzo 2020 e della individuazione dei seguenti obiettivi strategici:
-
    - Fascicolo Sanitario Elettronico regionale: mantenere ed evolvere il Fascicolo Sanitario Elettronico regionale e garantire la sua alimentazione continuativa con dati e documenti digitali permettendo agli assistiti l'accesso, la consultazione e la gestione di essi.
    - Convergenza sistemi informativi: perseguire la razionalizzazione degli strumenti informativi e dei modelli organizzativi, potenziando la cooperazione tra le strutture socio-sanitarie regionali.
    - Infrastruttura tecnologica: perseguire l'evoluzione, il potenziamento e la razionalizzazione delle infrastrutture di data center, delle reti e dei componenti trasversali a tutti i servizi ICT del Sistema Socio Sanitario Regionale.

- Cittadini e operatori: perseguire il disegno partecipato e lo sviluppo di nuovi servizi, secondo un approccio centrato sull'utente (operatori e cittadini).
- Sviluppo e innovazione: perseguire le finalità di governo e ricerca del Sistema Socio Sanitario Regionale attraverso l'utilizzo dei big data, sistemi avanzati di data warehouse, applicazioni avanzate di intelligenza artificiale.
- Sicurezza e protezione dei dati: garantire la protezione e la sicurezza dei dati attraverso un approccio di data protection fondato sui principi di privacy by default e privacy by design.

- della previsione, all'interno del Piano del Sistema Informativo Socio Sanitario 2019/2023 di una apposita Cabina di Regia il cui coordinamento è stato posto in capo alla UOC Sistemi Informativi di Azienda Zero, che risulta avere assorbito, in ordine al Fascicolo Sanitario Elettronico, ruolo e funzioni in precedenza svolte dall'organismo regionale "Unità di Regia del progetto FSEr".

Ritenuto pertanto, in forza di quanto sopra, di individuare da parte di Regione del Veneto, quale Titolare del trattamento dei dati, Azienda Zero quale Responsabile del Trattamento dei dati in argomento;

Considerato che con la presente convenzione la Giunta regionale e Azienda Zero intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali relativi al FESr, accettando tutti i termini in essa indicati

SI CONVIENE E STIPULA QUANTO SEGUE

Articolo 1 - Oggetto e definizioni

1. Con la sottoscrizione della presente Convenzione Azienda Zero, nella persona del proprio legale rappresentante pro tempore, nominata con Deliberazione della Giunta regionale nr. del quale Responsabile del trattamento dei dati con l'incarico di effettuare le operazioni di trattamento sui dati personali contenuti nel FSE per conto della Regione, titolare del trattamento, esclusivamente per finalità di governo e ricerca, conferma di essere a conoscenza degli obblighi che si assume e si impegna a trattare i dati attenendosi a quanto previsto nella presente Convenzione ed a tutte le ulteriori istruzioni impartite dal Titolare, nel rispetto delle regole GDPR e della normativa nazionale e regionale. Tali dati saranno trattati sia su supporto cartaceo che con strumenti elettronici, in conformità ai principi di proporzionalità, necessità e indispensabilità del trattamento.

2. Fatta eccezione per i termini e le espressioni altrimenti definiti nella presente convenzione, i termini e le espressioni contrassegnate da iniziali maiuscole avranno il significato di seguito specificato:

"GDPR"	indica il 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).
"Autorità di Controllo"	indica il Garante per la protezione dei Dati Personali.
"Autorizzati"	le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile ai sensi dell'art. 29 del GDPR.

Categorie Particolari di Dati”	indica ogni Dato Personale idoneo a rivelare l’origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, 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.
“Codice”	il D.Lgs. n. 196/2003 “Codice in materia dei dati personali” così come successivamente integrato e modificato (da ultimo del D.Lgs. n. 101/2018).
“Comitato Europeo per la protezione dei dati”	indica l’organismo dell’Unione Europea dotato di personalità giuridica istituito ai sensi degli artt. 68 e ss. del GDPR.
“Comunicazione”	dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, dal rappresentante del titolare nel territorio dell’Unione europea, del responsabile o dal suo rappresentante nel territorio dell’Unione europea, dalle persone autorizzate, ai sensi dell’art. 2-quaterdecies, al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.
“Convenzione”	l’accordo tra le Parti.
“Data Breach”	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
“Dato/i Personale/i”	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.
“Diffusione”	Indica il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

"DPIA"	valutazione di impatto sulla protezione dei dati personali, necessaria per il trattamento dei dati che presentano un rischio elevato per i diritti e le libertà delle persone.
"Gruppo di Lavoro Articolo 29"	indica il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE. ora sostituito dall'European Data Protection Board, o Comitato europeo per la protezione dei dati.
"Interessato"	la persona fisica identificata o identificabile cui si riferiscono i Dati Personali.
"Responsabile del trattamento"	Indica chi effettua un trattamento dati per conto del titolare del trattamento.
"Sub-Responsabile/Sub-responsabile	indica qualsiasi soggetto, persona fisica o giuridica, a cui il Responsabile ricorra per l'esecuzione di specifiche attività di Trattamento per conto del Titolare a cui sono imposti gli stessi obblighi del Responsabile.
"Terze Parti o Terzi"	indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non siano l'interessato, il Titolare, il Responsabile e gli incaricati autorizzati al trattamento dei Dati Personali sotto l'autorità diretta del titolare o del responsabile.
"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.
"Trattamento"	Indica 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.

Articolo 2 - Finalità del trattamento e tipologia dei dati trattati

1. Il Responsabile è autorizzato a trattare per conto del Titolare i dati sanitari e socio sanitari contenuti nel Fascicolo Sanitario Elettronico esclusivamente per finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nonché per finalità di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria. Le categorie di dati trattati e le categorie degli interessati sono così individuate:

a) categoria dei dati trattati: sono trattati i dati sanitari e socio sanitari contenuti nel Fascicolo Sanitario Elettronico purché privati dei dati identificativi diretti dell'assistito ai sensi degli articoli 16 e 19 del citato DPCM 178/2015;

b) categoria degli interessati: sono individuati come interessati gli assistiti appartenenti al servizio sanitario regionale e nazionale.

2. Resta inteso che il trattamento dei dati di cui al comma 1 è autorizzato nei soli limiti di esenzione dal divieto generale di cui all'articolo 9 del GDPR, secondo le misure ivi stabilite, nonché agli articoli 2 ter e seguenti del Codice, ivi comprese le regole deontologiche e le misure di garanzia che saranno volta per volta emesse. In nessun caso il Responsabile del trattamento acquisisce la proprietà intellettuale di dati e informazioni trattati nell'ambito di svolgimento della convenzione.

3. Il trattamento dei dati è autorizzato fino alla scadenza della presente convenzione.

Articolo 3 - Compiti del Titolare

1. Il Titolare impartisce al Responsabile istruzioni documentate per il trattamento dei dati personali e ha diritto di ottenere dal Responsabile tutte le informazioni necessarie per verificare il rispetto delle istruzioni impartite, l'adempimento degli obblighi della presente convenzione nonché della normativa in materia di protezione dei dati personali; il Titolare ha in particolare il diritto di ottenere le informazioni relative alle misure tecniche e organizzative adottate.

2. Qualora venga rilevato che un'istruzione impartita dal Titolare violi le disposizioni normative in materia di protezione dei dati personali, il Responsabile si obbliga ad informare immediatamente il Titolare.

3. Sono considerate istruzioni documentate le prescrizioni previste nella presente convenzione, nei suoi eventuali allegati e nell'atto di nomina e ogni altra eventuale comunicazione scritta del Titolare concernente le modalità di trattamento dei dati da parte del Responsabile.

4. Il Titolare esercita i poteri di verifica e controllo secondo le modalità stabilite all'articolo 11.

Articolo 4 - Obblighi del Responsabile

1. Con la sottoscrizione della presente convenzione il Responsabile si impegna a garantire la correttezza del trattamento e ad adottare adeguate misure tecniche e organizzative in modo tale che il trattamento soddisfi i requisiti del GDPR ed ogni altra istruzione impartita dalla Regione, nonché a tener conto dei provvedimenti tempo per tempo emanati dall'Autorità di Controllo, dal Gruppo di Lavoro Articolo 29 e dal Comitato Europeo per la protezione dei dati, inerenti al trattamento svolto, garantendo la tutela dei diritti degli Interessati. A tal fine, il Responsabile opera secondo il principio di responsabilizzazione, fin dall'inizio del trattamento e per progettazione predefinita, per ridurre al minimo i rischi connessi al trattamento e per garantire il pieno rispetto delle disposizioni vigenti in materia di trattamento dei dati personali.
2. In particolare, il Responsabile è tenuto ad adempiere, secondo i principi di correttezza e buona fede, ai seguenti obblighi:
    a. rispettare i principi di liceità, correttezza, trasparenza, pertinenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione, tutela fin dall'inizio del trattamento e per progettazione definita, di cui al GDPR;
    b. assicurare il rispetto dei principi contenuti nel GDPR nelle attività di raccolta, archiviazione, conservazione, collocazione ed accesso agli archivi e nel compimento delle operazioni di trattamento sui dati personali, custodendo gli stessi in maniera che ad essi non accedano persone non autorizzate;
    c. assicurarsi che il modulo di informativa e consenso adeguato agli scopi sia reso agli interessati, in una versione concordata con il Titolare, ad eccezione dei casi in cui competa

direttamente al Titolare medesimo predisporre e controllare l'adempimento alle prescrizioni di legge in tema di informativa e consenso;

d. istituire un Registro dei Trattamenti di tutte le categorie di attività relative al trattamento, svolte in esecuzione della presente convenzione, secondo quanto prescritto dall'articolo 30, paragrafo 2, del GDP e, su richiesta, mettere tale registro a disposizione del Titolare e/o dell'Autorità di Controllo;
e. istituire un Registro delle violazioni dei dati personali (Data Breach) ai sensi dell'articolo 33 del GDPR e dell'articolo 12 della presente convenzione, e, su richiesta, mettere tale registro a disposizione del Titolare e/o dell'Autorità di Controllo;
f. gestire le richieste che gli interessati avanzino nell'esercizio dei diritti conferiti dal GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione ;
g. individuare e autorizzare per iscritto le persone autorizzate al trattamento e fornire loro adeguata formazione e le istruzioni relative alle operazioni da compiere, vigilando sulle stesse e supervisionando il loro operato affinché il trattamento avvenga in conformità alla legge, per le finalità previste dalla convenzione e nel rispetto delle misure di sicurezza previste dalla presente convenzione;
h. mantenere la riservatezza delle informazioni, dei documenti e degli atti amministrativi dei quali venga a conoscenza in relazione al trattamento svolto per le funzioni affidategli, garantendo altresì che i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e, in ogni caso, che abbiano ricevuto la formazione necessaria;
i. effettuare la valutazione di impatto (DPIA) ai sensi dell'articolo 5 della presente convenzione;
j. adottare le misure di notifica e di comunicazione nel caso di violazione di dati personali (data breach), ai sensi degli artt. 33 e 34 GDPR, secondo le regole di cui all'articolo 12 della presente convenzione;
k. effettuare la comunicazione dei dati personali, laddove prevista, solo nei limiti consentiti dalle finalità del trattamento, dal contenuto del consenso prestato dall'Interessato, da disposizioni di legge o regolamenti, e in particolare dall'articolo 2 ter del Codice, nonchè dai provvedimenti dell'Autorità di controllo;
l. adoperarsi in ogni altro modo ed adottare ogni altra misura idonea per garantire il massimo rispetto dei diritti degli Interessati;
m. non diffondere dati, se non nei casi previsti da leggi e regolamenti, e in particolare dall'articolo 2 ter del Codice, nonché dai provvedimenti dell'Autorità di Controllo;
n. al fine di evitare e/o ridurre il rischio di distruzione o perdita anche accidentale dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, adottare le preventive ed adeguate misure tecniche e organizzative al fine di garantire un livello di sicurezza adeguato al rischio nel rispetto delle disposizioni contenute nel GDPR e, in particolare, dall'articolo 32, nonché di quanto previsto dall'articolo 8 della presente convenzione;
o. coadiuvare il Titolare del trattamento nella difesa in caso di procedimenti (relativi a trattamenti di dati connessi allo svolgimento dell'attività oggetto della convenzione) dinanzi all'Autorità di controllo o all'autorità giudiziaria, fornendo al Titolare del trattamento tutte le informazioni e/o i documenti necessari che potranno essere richiesti da quest'ultima;
p. cooperare con il Titolare del trattamento e con il Responsabile della Protezione dei Dati (Data Protection Officer) regionale, anche mediante il proprio Responsabile della Protezione dei Dati, in particolare gestendo le richieste che gli interessati avanzino direttamente al Titolare nell'esercizio dei diritti conferiti dal GDPR;
q. nominare gli amministratori di sistema, il cui operato deve essere oggetto, con cadenza almeno annuale, di verifica da parte del Responsabile al fine di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

3. Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle circostanze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

Articolo 5 - Valutazione di impatto sulla protezione dei dati personali (DPIA)

1. Il Responsabile effettua la valutazione di impatto (DPIA) ai sensi dell'articolo 35 del GDPR ogniqualvolta si renda necessario nonché avvia la consultazione preventiva all'Autorità di Controllo nei casi previsti dall'articolo 36 del GDPR, fornendo documentata informazione al Titolare di tale valutazione e delle ulteriori misure di sicurezza eventualmente approntate.

Articolo 6 - Obblighi informativi

1. Per quanto concerne gli obblighi informativi, il Responsabile:

a) agisce tempestivamente e in autonomia informando il Titolare in caso di ispezioni dell'Autorità di controllo e/o organi istituzionali (es. Guardia di Finanza, NAS, etc…), nonchè di azioni giudiziarie intraprese nei suoi confronti per violazione della normativa in materia di tutela dei dati personali;

b) informa tempestivamente il Titolare di ogni violazione dei dati personali e di ogni attività di notifica e di comunicazione effettuate a suo nome e per suo conto ai sensi dell'articolo 12 della presente convenzione;

c) comunica le risultanze della valutazione di impatto svolta ai sensi dell'articolo 5 della presente convenzione e le ulteriori misure di sicurezza approntate qualora tale valutazione ne evidenzi la necessità;

d) presenta al Titolare i rapporti periodici delle attività di audit interni ai sensi dell'articolo 8, comma 3, della presente convenzione;

e) informa il Titolare dell'effettuazione di test periodici per attestare la validità della procedura di Data Breach adottata ai sensi dell'articolo 12;

f) informa il Titolare di ogni questione rilevante che dovesse presentarsi nel corso del trattamento dei dati e segnala, altresì, le azioni o eventi che possano costituire o causare un rischio per la conservazione dei dati o la loro integrità, adottando nel contempo tutte le misure idonee ad evitare conseguenze pregiudizievoli al trattamento dei dati.

Articolo 7 - Sub-responsabili

1. Il Responsabile non ricorre ad un altro responsabile (sub responsabile) senza previa autorizzazione scritta, specifica o generale, del Titolare ai sensi dell'articolo 28 del GDPR.

2. Qualora sia individuato un sub responsabile per l'esecuzione di specifiche attività di trattamento, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub responsabile.

3. Il Responsabile si obbliga, in caso di autorizzazione scritta generale, ad informare il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sub-Responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche.

4. Il Responsabile può comunicare o rendere disponibili i dati personali trattati per conto del Titolare esclusivamente ai fornitori autorizzati.

5. Il Responsabile si obbliga a designare detti eventuali fornitori quali sub-responsabili, previa acquisizione della necessaria preventiva autorizzazione da parte del Titolare ai sensi del comma 1, e a far assumere agli stessi i medesimi obblighi in materia di protezione dei dati personali cui si è

impegnato quale Responsabile del trattamento dati con il presente atto, mediante sottoscrizione di appositi atti giuridici o contratti.

6. Il Responsabile è tenuto ad impartire ai sub-responsabili precise istruzioni relativamente al Trattamento in oggetto e ad assicurarsi che gli stessi offrano le medesime garanzie in materia di misure tecniche e organizzative previste dal GDPR.

7. I sub-responsabili potranno trattare i dati personali nella misura in cui tale trattamento sia strettamente necessario per l'esecuzione delle funzioni delegate al Responsabile.

8. Qualora il sub responsabile del trattamento designato dall'odierno Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'odierno Responsabile conserva, nei confronti del Titolare l'intera responsabilità dell'adempimento di tali obblighi.

Articolo 8 - Sicurezza del trattamento

1. Ferma restando l'applicazione delle misure tecniche e organizzative ai sensi dell'articolo 32 del GDPR, al fine di garantire un livello di sicurezza sempre adeguato al rischio, il Responsabile, anche nella sua qualità di Fornitore di Servizi Digitali (FSD) erogati quotidianamente ai cittadini, ai sensi della Direttiva NIS 2016/1148 (Network and Information Security), ha l'obbligo di assicurare la continuità operativa delle reti e dei sistemi informativi volta a garantire la fruibilità dei servizi ai cittadini e a prevenire o ridurre al minimo l'impatto che eventuali incidenti potrebbero causare ai suddetti sistemi, informando tempestivamente il Titolare degli eventuali incidenti di sicurezza occorsi ai sensi dell'articolo 33, comma 2, del GDPR e dell'articolo 12, comma 7, della presente convenzione.
2. In particolare il Responsabile, per le misure tecniche ed organizzative atte a gestire i rischi è chiamato a conformarsi alla norma ISO 27799:2016 quale linea guida per la sicurezza delle informazioni prevedendo la selezione, l'implementazione e la gestione dei controlli di sicurezza, in relazione al rischio valutato, nonché alla norma ISO 27701: 2019 quale linea guida per gestire adeguatamente i rischi per la privacy relativi alle informazioni personali e per dare dimostrazione che il trattamento dei dati personali avviene nel rispetto delle prescrizioni del GDPR. L'osservanza delle suddette linee guida consente al Responsabile di mantenere nel contesto sanitario un livello di sicurezza e di privacy adeguato, in grado di garantire la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie personali dei cittadini/pazienti e la continuità operativa e la fruibilità dei servizi.
3. Il Responsabile è tenuto a presentare al Titolare i rapporti periodici delle attività di audit interni secondo il programma concordato e definito preventivamente volte a verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative implementate al fine di assicurare la loro adeguatezza in relazione al trattamento dei dati effettuato. E' comunque facoltà del Titolare condurre, con la collaborazione del Responsabile, degli audit di seconda e/o di terza parte sulle misure di sicurezza dalla stessa adottate.
4. Il Responsabile è inoltre tenuto ad adeguare i controlli e le misure di sicurezza adottate all'evoluzione tecnologica al fine di garantire costantemente la loro efficacia.
5. Il Responsabile è tenuto ad operare secondo il principio di responsabilizzazione, fin dall'inizio del trattamento e per progettazione predefinita, per ridurre al minimo i rischi connessi al trattamento e per garantire il pieno rispetto delle disposizioni vigenti in materia di trattamento dei dati personali.

Art. 9 - Documentazione Privacy

1. Il Responsabile si impegna ad adottare la documentazione in materia di protezione dei dati personali prevista dalla normativa italiana ed europea tenendo traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare le scelte in ambito di privacy e le relative procedure concernenti le adeguate misure tecniche e organizzative.

Articolo 10 - Condizioni particolari per il riscontro alle istanze degli Interessati

1. Tenendo conto della natura del trattamento, il Responsabile si obbliga di dare riscontro alle richieste, che pervengano allo stesso direttamente o che gli siano trasmesse dal Titolare, per l'esercizio dei diritti dell'interessato di cui alla Sezione 3 del GDPR nel rispetto dei termini previsti dall'articolo 12 del GDPR.

Articolo 11 - Verifiche e controlli

1. Al fine di verificare il rispetto delle istruzioni impartite, l'adempimento degli obblighi della presente convenzione nonché della normativa in materia di protezione dei dati personali, Il Titolare ha diritto di disporre verifiche e controlli e di svolgere specifiche attività di audit, avvalendosi anche di personale espressamente incaricato a tale scopo, nonché di svolgere ispezioni anche presso le sedi del Responsabile.
2. Il Responsabile si impegna a prestare ogni necessaria collaborazione alle attività di verifica, controllo, ispezione e alle attività di audit svolte dal Titolare o da altro soggetto da questi incaricato.

3. Le attività di verifica e controllo di cui al presente articolo saranno eseguite in maniera tale da non interferire con il normale corso delle attività del Responsabile del trattamento e fornendo a quest'ultimo un ragionevole preavviso.

Articolo 12 Procedura per il caso di violazioni dei dati personali (Data Breach)

1. Il Responsabile è tenuto ad effettuare le notifiche di violazione dei dati personali all'Autorità di Controllo ai sensi dell'articolo 33 del GDPR e le comunicazioni di violazione dei dati personali all'interessato ai sensi dell'articolo 34 del GDPR in nome e per conto del Titolare, e con la presente convenzione è a ciò specificatamente autorizzato.
2. Il Responsabile adotta un Protocollo di risposta disciplinante il processo di Data Breach, da attivare nelle ipotesi di violazione dei dati personali, comunicandolo al Titolare.
3. Il Protocollo di cui al comma 2 deve prevedere:
   a) la nomina di un referente per la gestione del processo di Data Breach adeguatamente supportato anche con l'eventuale costituzione di un apposito gruppo di lavoro interdisciplinare;
   b) l'effettuazione, secondo le tempistiche indicate dal Protocollo, di test periodici per attestare la validità della procedura adottata, fornendo adeguata informazione al Titolare.
4. Il Responsabile è tenuto a:
   a) istituire un Registro di Data Breach, ove, secondo le indicazioni del Protocollo di risposta adottato, devono essere registrati anche i fatti che non configurano episodi di violazione dei dati personali, in quanto necessari ai fini dell'aggiornamento della procedura, in osservanza della lettera b);
   b) procedere all'aggiornamento della procedura, qualora ritenuto indispensabile a seguito dello sviluppo tecnologico, delle risultanze dei test periodici effettuati, nonché in forza di sopravvenute modifiche normative;
   c) stipulare con una compagnia assicurativa adeguata polizza per la copertura di eventuali danni diretti o indiretti, conseguenti dalla violazione dei dati personali.
5. Qualora si verifichi un episodio che possa configurare una violazione dei dati personali, il referente per la gestione del processo di Data Breach è tenuto ad effettuare una valutazione dell'evento e delle probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, avvalendosi del supporto di cui alla lettera a) del comma 3, al fine di redigere una corretta classificazione, necessaria per la notifica all'Autorità di Controllo.
6. Qualora a seguito dell'attività di valutazione di cui al comma 5, emerga la probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Responsabile, su istruttoria del proprio referente, effettua la notifica all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, corredando la notifica dei motivi del ritardo qualora non sia effettuata entro le 72 ore, in conformità all'articolo 33 del GDPR.

7. Il Responsabile è tenuto ad informare il Titolare tempestivamente di ogni violazione dei dati personali e di ogni attività di notifica e di comunicazione effettuata a suo nome e per suo conto ai sensi del presente articolo.

Articolo 13- Condizioni particolari per il trasferimento dei dati all'estero

1. Il Responsabile si impegna a limitare gli ambiti di circolazione e trattamento dei Dati Personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server o in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE.

Articolo 14 - Responsabilità

1. Il Responsabile si impegna a manlevare e mantenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento o altro onere che possa derivare al Titolare dalla mancata osservanza degli obblighi di cui alla presente convenzione e più in generale dalla violazione della normativa sulla tutela dei dati personali da parte del Responsabile e dei suoi sub-responsabili. Nel caso in cui il Titolare sia assoggettato a sanzioni, il Responsabile solleva integralmente il Titolare qualora la sanzione sia applicata a seguito della mancata osservanza degli obblighi di cui alla presente convenzione e più in generale dalla violazione della applicabile normativa sulla tutela dei dati personali da parte del Responsabile e dei suoi sub-responsabili.

2. Il Responsabile dichiara di aver contratto specifica polizza con idonea e adeguata copertura assicurativa.

Articolo 15 - Ipotesi di recesso dalla convenzione e revoca della nomina

1. Il Titolare, previa contestazione scritta dei fatti e assegnando un congruo termine al Responsabile entro cui far pervenire le proprie controdeduzioni, può recedere dalla presente convenzione per effetto della revoca della nomina adottata con la deliberazione della Giunta regionale n. del nei seguenti casi:

   a) qualora riscontri, anche durante le attività di controllo, una riduzione o modifica peggiorativa delle garanzie di corretto trattamento da parte del Responsabile;

   b) qualora riscontri ritardi od omissioni nelle notifiche e comunicazioni che incombono sul Responsabile riferite alla procedura di Data Breach, in violazione della presente convenzione e del Protocollo di risposta;

   c) qualora riscontri un grave inadempimento degli obblighi imposti dalla presente convenzione concernenti la sicurezza del trattamento, tale da non permettere la prosecuzione del rapporto.

2. Il Responsabile può in qualsiasi momento recedere dalla presente convenzione e conseguentemente decadere dall'incarico ricevuto con il provvedimento di nomina di cui alla DGR n. del _____ , comunicando tale decisione, adeguatamente motivata, con un preavviso di almeno sei mesi, al fine di permettere al Titolare di individuare eventualmente un altro Responsabile del trattamento. In tali ipotesi il Titolare, a seguito della comunicazione del Responsabile, dovrà impartire al medesimo puntuali istruzioni per la comunicazione di tutte le informazioni ritenute necessarie che dovranno essere successivamente messe a disposizione del nuovo Responsabile del trattamento, ove nominato.
3. Il Responsabile, nei casi di cui ai commi 1 e 2, per effetto della cessazione del trattamento, è tenuto a rispettare quanto previsto dall'articolo 16, comma 2.

Articolo 16 - Durata e Cessazione del Trattamento

1. La presente convenzione è efficace tra le parti fino all'eventuale recesso e revoca della nomina. Il trattamento non potrà comunque avere una durata superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile per un periodo di tempo non superiore a quello indicato.

2. A seguito della cessazione del trattamento affidato al Responsabile o nei casi di cui al comma 1, il Responsabile sarà tenuto, a scelta del Titolare e sulla base delle istruzioni dallo stesso impartite, a restituire al Titolare i dati personali trattati, con impegno alla rimozione integrale dei dati dai propri sistemi informativi e dai propri archivi.

Articolo 17 - Disposizioni finali

1. Trovano applicazione, ove non diversamente previsto, le norme del GDPR, del Codice Civile ed delle disposizioni legislative e regolamentari, nazionali e comunitarie vigenti in materia.

2. La presente Convenzione potrà essere integrata a seguito di successive disposizioni normative intervenute o di disposizioni ulteriori del Titolare del Trattamento.

3. La sottoscrizione della presente Convenzione non comporta alcun diritto per il Responsabile del trattamento ad uno specifico compenso o indennità o rimborso per l'attività svolta.

Art. 18 - Foro competente

1. In caso di violazioni alla presente convenzione il Foro competente è quello di Venezia.

Articolo 19 - Approvazione specifica

1. Ai sensi e per gli effetti di cui all'art. 1341 e 1342 c.c., si approvano specificamente le seguenti clausole: articolo 4 "Obblighi del Responsabile", articolo 12 "Procedura per il caso di violazioni dei dati personali (data breach)", articolo 15 "Ipotesi di recesso dalla convenzione e revoca della nomina".

Data _____

Il Titolare del trattamento

Per la Giunta della Regione del Veneto

_____

Il Responsabile del trattamento

Azienda Zero

_____