Servizio di assistenza, custodia e supporto agli ospiti della Casa San Patrignano – San Vito (Pergine Valsugana)

ISTRUZIONI AL RESPONSABILE DEL TRATTAMENTO DEI DATI

(articoli 28 e 29 del Regolamento UE 2016/679)

L'Azienda Provinciale per i Servizi Sanitari, con sede legale in 38123 Trento, Via Alcide Degasperi, n. 79, partita IVA e C.F. 01429410226, nella persona del …, dott …, autorizzato giusta delega dalla deliberazione del Direttore generale n. 487 del 1.10.2018 (di seguito "**APSS**" o anche "**Titolare**"),

premesso che:

- tra APSS e la/il [●] intercorre un rapporto di [●], in forza del contratto sottoscritto tra le Parti in data [●];

- tale rapporto contrattuale implica, necessariamente, il trattamento, da parte della/del [●], di dati personali di cui APSS è Titolare del trattamento;

- il Regolamento UE 2016/679 (di seguito, il "Regolamento") "*si applica al trattamento dei dati personali effettuato nell'ambito delle attività* […] *di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*";

- ai sensi dell'art. 28, paragrafo 1, del Regolamento, "*Qualora un trattamento debba essere effettuato per conto del Titolare, 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 Regolamento e garantisca la tutela dei diritti dell'interessato*";

- ai sensi dell'art. 29 del Regolamento, "*Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare* […]";

- ai sensi dell'art. 28, paragrafo 3, del Regolamento, inoltre, "*I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico, che vincoli il Responsabile del trattamento al Titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento*";

- ai sensi dell'art. 31 del Regolamento, "[…] *il Responsabile del trattamento*[...] *coopera* […] *su richiesta, con l'Autorità di controllo*[…]";

- ai sensi dell'art. 82, paragrafo 2, del Regolamento, il *"Responsabile del trattamento risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme, o contrario, rispetto alle istruzioni impartite dal Titolare del trattamento*";

- a seguito delle garanzie offerte e delle dichiarazioni rilasciate dalla/dal [●], in forza di quanto previsto al considerando n. 81 del Regolamento, tale soggetto è stato ritenuto idoneo ad assumere la qualifica di Responsabile del trattamento;

tutto ciò premesso e ritenuto, nomina [●] "*Responsabile del trattamento*".

Il "*Responsabile del trattamento*" è tenuto ad ottemperare alle disposizioni di seguito indicate:

Art. 1 - Ai sensi e per gli effetti dell'art. 28 del Regolamento, con il presente documento, l'**Azienda provinciale per i servizi sanitari**, in qualità di "*Titolare del trattamento*" fornisce le istruzioni al "*Responsabile del trattamento*", riconoscendolo idoneo ad assumere tale ruolo, impartendogli, di seguito, le obbligazioni che lo stesso è tenuto a osservare con riferimento ai trattamenti effettuati per conto del Titolare. Il Responsabile, pertanto, si impegna al rigoroso rispetto – con la diligenza di cui all'art. 1176, comma 2, del Codice Civile – della predetta normativa comunitaria, della relativa disciplina nazionale, nonché delle prescrizioni del Garante per la protezione dei dati personali (di seguito, il "Garante"), del Gruppo di Lavoro Articolo 29 e del Comitato europeo per la protezione dei dati. Ferma ogni ulteriore responsabilità nei confronti del Titolare, resta inteso che ogni forma di determinazione delle finalità e/o dei mezzi del trattamento da parte del Responsabile comporta l'assunzione, da parte dello stesso, della qualifica di Titolare del trattamento, con ogni ulteriore conseguenza.

Art. 2 - I dati personali trattati dal Responsabile concernono sia i dati c.d. "comuni" che *i c.d. dati particolari;* le categorie di interessati coinvolti nel trattamento riguardano: gli utenti di APSS.

Il Responsabile si obbliga a trattare i dati personali soltanto su istruzione documentata del Titolare; in particolare, in relazione al rapporto contrattuale di cui in premessa, il Responsabile può trattare i dati esclusivamente per finalità di organizzazione del servizio e può effettuare, con o senza strumenti automatizzati, soltanto le seguenti operazioni di trattamento: raccolta, registrazione, organizzazione, strutturazione, conservazione, estrazione e consultazione.

Qualora la normativa, comunitaria o nazionale, imponesse al Responsabile il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, lo stesso Responsabile informa il Titolare di tale obbligo giuridico prima del relativo trasferimento, salvo che la normativa in questione vieti tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile informa immediatamente il Titolare qualora, a suo parere, un'istruzione violasse il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Art. 3 – In ogni fase e per ogni operazione di trattamento, il Responsabile deve garantire il rispetto dei principi comunitari (ad esempio, di *privacy by design e by default*) e nazionali in ambito di protezione dei dati personali e, in particolare, quelli di cui agli artt. 5 e 25 del Regolamento. Inoltre, il Responsabile deve:

a) garantire che le persone che trattano dati personali siano state specificamente autorizzate, adeguatamente istruite e si siano impegnate alla riservatezza, o abbiano un adeguato obbligo legale di riservatezza.

Di seguito sono riportate le istruzioni minime che il Responsabile del trattamento deve fornire alle persone autorizzate al trattamento dei dati (di seguito "Persone Autorizzate"):

- non compiere alcuna operazione su dati personali che non sia autorizzata da precise disposizioni di legge o da altre basi giuridiche ove applicabili ai sensi dalla normativa, quali per esempio il consenso dell'interessato. Qualora non sia certa di tale circostanza, la Persona Autorizzata si deve rivolgere al Responsabile del trattamento per ottenere le conferme del caso; le operazioni di trattamento eseguite

devono essere inoltre pertinenti e non eccedenti le finalità per le quali i dati sono stati raccolti;

- trattare le informazioni ed i dati personali con cui la Persona Autorizzata entra in contatto per ragioni di lavoro esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza sia nei confronti del mondo esterno che interno. In nessun caso tali dati vanno diffusi o comunicati a terzi senza la preventiva autorizzazione del Titolare del trattamento.

- adottare tutte le misure di sicurezza, di cui l'art. 32 Regolamento, con riferimento ai trattamenti effettuati sia con strumenti elettronici che senza, e di volta in volta indicate dal Responsabile del trattamento, segnalando a quest'ultimo eventuali rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta;

- adottare le necessarie cautele per assicurare la segretezza delle credenziali affidate, nonché la diligente custodia dei dispositivi in proprio esclusivo uso e possesso;

- verificare l'esattezza e la completezza dei dati raccolti e trattati e, se del caso, provvedere alla relativa correzione e aggiornamento;

- partecipare ai corsi di formazione organizzati dal Responsabile o dal Titolare del trattamento in merito alla protezione dei dati personali;

- comunicare al Responsabile del trattamento qualsivoglia notizia reputi rilevante con riferimento al trattamento dei dati personali.

Ulteriori e specifiche istruzioni, anche in ragione della tipologia di trattamento, andranno di volta in volta fornite alle Persone Autorizzate dal Responsabile del trattamento. Il Responsabile dovrà comunicare alle Persone Autorizzate al trattamento che in qualunque circostanza le stesse non abbiano la certezza in merito alla correttezza di una operazione di trattamento, dovranno rivolgersi senza indugio al Responsabile del trattamento che provvederà, se necessario, ad interessare il Titolare.

Inoltre dovrà comunicargli che l'adempimento dell'obbligo di diligente e corretta esecuzione delle istruzioni ricevute in ordine alle istruzioni potrà costituire elemento di valutazione dell'attività svolta nell'ambito del proprio rapporto contrattuale con il Responsabile.

b) adottare tutte le misure richieste ai sensi dell'articolo 32 del Regolamento. In caso di trattamento con strumenti automatizzati, il Responsabile garantisce di aver adottato misure di sicurezza analoghe e non inferiori al livello minimo di cui alla circolare Agid n. 2/2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni) e successive modifiche e integrazioni;

c) assistere il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (Capo III del Regolamento), nonché informare tempestivamente il Titolare dei reclami eventualmente presentati dagli interessati;

d) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente documento, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare, dal suo *Data Protection Officer*, o da un altro soggetto a ciò deputato;

e) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento. In particolare, relativamente alla predisposizione della "valutazione di impatto" ("*Data Protection impact assessment*", di cui agli artt. 35 e 36 del Regolamento), nel caso in cui il Responsabile fornisse al Titolare gli strumenti/applicativi informatici e/o gestisse gli stessi strumenti/applicativi informatici del Titolare, lo stesso è tenuto a predisporre ed aggiornare l'analisi dei rischi (probabilità di violazione della sicurezza) degli strumenti/applicativi informatici, comunicandola al Titolare, adottando i criteri di valutazione forniti da quest'ultimo. Il Responsabile, inoltre, è tenuto a comunicare immediatamente al Titolare (struttura competente in materia di protezione dei dati personali), non appena venuto a conoscenza di un eventuale *data breach*, tutte le informazioni necessarie a consentirgli di effettuare i conseguenti adempimenti in materia di violazione di dati personali previsti dal Regolamento.

f) nei casi prescritti dall'art. 37 del Regolamento, oltre che nelle fattispecie in cui tale adempimento sia raccomandato nelle specifiche Linee Guida del Gruppo di Lavoro Art. 29, nonché dalle indicazioni fornite dal Garante, provvedere alla nomina del *Data Protection Officer* (di seguito, "DPO"), nel rispetto dei criteri di selezione stabiliti dallo stesso Regolamento, dalle relative Linee Guida del Gruppo di Lavoro Art. 29, nonché dalle indicazioni fornite dal Garante, garantendo il rispetto delle prescrizioni di cui all'art. 38, anche allo scopo di consentire al medesimo DPO l'effettivo adempimento dei compiti di cui art. 39 del Regolamento;

g) provvedere alla designazione per iscritto del/degli Amministratore/i di Sistema secondo i criteri di individuazione e selezione previsti dal Garante con provvedimento dd. 27/11/2008 e s.m.i., conservando l'elenco degli stessi Amministratori di Sistema, verificandone annualmente l'operato ed adottando sistemi idonei alla registrazione dei relativi accessi logici (da conservare con caratteristiche di inalterabilità e integrità per almeno per 6 mesi). Qualora l'attività degli stessi Amministratori di Sistema riguardasse, anche indirettamente, servizi o sistemi che trattano, o che permettono il trattamento, di informazioni di carattere personale dei dipendenti del Titolare, comunicare a quest'ultimo l'identità degli Amministratori di Sistema (provvedendo a dare idonea informativa, ex art. 13 del Regolamento, agli stessi Amministratori);

h) nel caso in cui non sia stato attivato prima della stipula del contratto, provvedere alla predisposizione del Registro delle attività del trattamento nelle ipotesi e nei termini di cui all'art. 30 del Regolamento, mettendolo tempestivamente a disposizione del Titolare, o del Garante, in caso di relativa richiesta;

i) nel caso in cui non si sia provveduto prima della stipula del contratto, comunicare, al Titolare, i nominativi di riferimento per l'esecuzione del Contratto, nonché il nominativo dell'eventuale DPO;

j) alla scadenza rapporto contrattuale di cui in premessa (ivi compresi i casi di risoluzione o recesso), o al più al termine dell'esecuzione delle relative attività/prestazioni e, quindi, delle conseguenti operazioni di trattamento, fatta salva una diversa determinazione del Titolare, il Responsabile deve provvedere alla cancellazione dei dati personali in oggetto (ivi comprese ogni eventuale copia esistente), dandone conferma scritta al Titolare, a meno che la normativa comunitaria o nazionale ne preveda la conservazione ed escluda ogni altra forma di conservazione anche per finalità compatibili. In caso di trattamento con modalità automatizzate, il Responsabile garantisce che, su richiesta del Titolare e senza costi aggiuntivi, prima di effettuare la cancellazione predetta può effettuare la trasmissione sicura dei dati personali ad altro titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, beninteso qualora il destinatario sia attrezzato a riceverli.

Art. 4 - Il Responsabile non ricorre ad un ulteriore Responsabile del trattamento (di seguito il "*sub-Responsabile*" senza previa autorizzazione scritta, specifica o generale, del Titolare. Nel caso di autorizzazione scritta generale, il Responsabile informa il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di ulteriori sub-Responsabili, dando così al Titolare l'opportunità di opporsi a tali modifiche. In ogni caso, qualora il Responsabile ricorresse ad un sub-Responsabile per l'esecuzione di specifiche attività di trattamento per conto del Titolare, si impegna a sottoscrivere – in forma scritta, anche in formato elettronico – con tale sub-Responsabile, un atto giuridico vincolante analogo, nel contenuto, al presente, imponendo al sub-Responsabile gli stessi obblighi in materia di protezione dei dati contenuti nel presente documento (e in ogni altro atto giuridico o *addendum* intervenuto tra le Parti). In particolare, la nomina del sub-Responsabile deve prevedere l'obbligo di quest'ultimo di mettere in atto misure tecniche e organizzative adeguate tali per cui i trattamenti effettuati soddisfino i requisiti del Regolamento, nonché la relativa disciplina nazionale in materia di protezione dei dati personali.

Qualora i dati personali fossero trasferiti verso Paesi terzi ovvero organizzazioni internazionali, il Responsabile deve informarne il Titolare e garantire il rispetto delle condizioni di cui agli art. 44 e ss. del Capo V del Regolamento. Resta inteso che, laddove il sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile è ritenuto integralmente responsabile nei confronti del Titolare dell'adempimento degli obblighi del sub-Responsabile.

Art. 5 – In caso azione di risarcimento civile, o responsabilità amministrativa, promossa nei confronti del Titolare per i danni provocati, o le violazioni commesse dal Responsabile e/o dal sub-Responsabile a seguito di inadempienze normative o contrattuali, il Responsabile stesso manleva integralmente il Titolare, ogni eccezione rimossa. Analogamente, il Responsabile manleva integralmente il Titolare, ogni eccezione rimossa, in caso di applicazione di sanzioni da parte del Garante o di ogni altra autorità che dovesse essere competente per inadempienze normative o contrattuali commesse dallo stesso Responsabile e/o dal sub-Responsabile.

Art. 6 – La nomina a Responsabile del trattamento avrà termine il [●]; in forza del collegamento con il contratto di cui in premessa, la risoluzione o il recesso dello stesso contratto produrrà medesimo effetto sul presente accordo.

Art. 7 – È possibile modificare il presente atto solo per giustificati motivi, da formalizzare con apposito provvedimento amministrativo adottato dal medesimo organo che ha assunto il provvedimento a contrarre, esclusivamente riguardante le modifiche del presente atto e non anche altri aspetti del contratto d'appalto.

Sono considerati giustificati motivi i soli eventi sopravvenuti e imprevedibili rispetto al momento dell'attivazione della procedura di affidamento dell'appalto, che incidono sulla materia di protezione delle persone fisiche nel trattamento dei dati personali, in particolare, sull'aggiornamento delle misure attuative di protezione adottate.

Per ogni modifica del presente atto, successiva alla stipula ed in corso di validità del Contratto a cui accede l'atto stesso, si procede mediante scambio di corrispondenza, secondo gli usi commerciali].

Con l'accettazione della nomina, il Responsabile del trattamento è assoggettato agli obblighi contenuti nelle disposizioni sopra indicate e dichiara di accettare espressamente, in particolare, ai sensi e per gli effetti dell'art. 1341 c.c., i seguenti articoli: art. 1 - Diligenza professionale; art. 4 - Restrizione alla libertà contrattuale nei rapporti coi terzi; art. 5 - Limitazione di responsabilità (manleva).

Per delega del Direttore generale

Dott……..