"Istruzioni al Responsabile del Trattamento dei dati"

ISTRUZIONI CONFERITE DAL TITOLARE DEL TRATTAMENTO (AZIENDA PROVINCIALE PER I SERVIZI SANITARI)

AL RESPONSABILE DEL TRATTAMENTO (Appaltatore)

PER DISCIPLINARE I TRATTAMENTI SVOLTI DAL RESPONSABILE

Premesso che:

- 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*";

- l'Appaltatore con la stipula del contratto di appalto si obbliga a garantire misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento, in forza di quanto previsto al considerando n. 81 del Regolamento;

Tutto ciò premesso si disciplina che:

Art. 1 - Dando atto che, ai sensi e per gli effetti dell'art. 28 del Regolamento, con la stipula del contratto di appalto (di seguito, il "Contratto") l'**Azienda provinciale per i servizi sanitari**, in qualità di "*Titolare del trattamento*" (di seguito, il "Titolare"), nomina **l'Appaltatore** "*Responsabile del trattamento*" (di seguito, il "Responsabile"), riconoscendolo idoneo ad assumere tale ruolo, il Titolare impartisce, di seguito, le istruzioni e gli obblighi disciplinari che il Responsabile deve osservare a riguardo dei trattamenti effettuati per conto del Titolare in ragione dell'appalto. 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 dell'Autorità di

controllo. 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 sensibili"; 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 Contratto, 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 del 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. In particolare, 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;

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 Contratto, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare, dal suo *Data Privacy 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 privacy 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. Con riferimento ai casi di *data breach* (di cui agli artt. 33 e 34 del Regolamento), nel caso in cui gli strumenti/applicativi informatici del Titolare fossero forniti o gestiti dal Responsabile, quest'ultimo è sin d'ora delegato dal Titolare, accettando tale delega senza costi aggiuntivi, ad effettuare la relativa notifica all'Autorità di controllo e la comunicazione ai relativi interessati qualora la violazione riguardasse gli strumenti/applicativi informatici stessi; tali adempimenti dovranno essere effettuati previa valutazione, con la struttura dell'APSS direttamente coinvolta, degli elementi della violazione e delle necessarie conseguenti azioni da intraprendere. Il Responsabile, inoltre, è tenuto a comunicare immediatamente al Titolare (struttura competente in materia di protezione dei dati personali), non appena venuto a conoscenza dell'evento, ogni *data breach* che potrebbe ragionevolmente riguardare i dati personali che tratta per conto del Titolare;

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, provvedere alla nomina del Data Privacy 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 dalla Autorità di controllo, 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 dall'Autorità di controllo con provvedimento dd. 27/11/2008 e s.m.i., conservando l'elenco degli stessi Amministratori, 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 nei termini di cui all'art. 30 del Regolamento, mettendolo tempestivamente a disposizione del Titolare, o dell'Autorità di controllo, 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 del Contratto (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 (ivi comprese ogni eventuale copia esistente) dei dati personali in oggetto (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 soggetto, 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 altro ulteriore Responsabile del trattamento (di seguito il "*sub-Responsabile*" [1]) 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, deve sottoscrivere, con tale sub-Responsabile, un contratto (o altro atto giuridico vincolante) analogo, nel contenuto, al presente atto – stipulato in forma scritta, anche in formato elettronico – imponendo a quest'ultimo gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto (e in ogni altro atto giuridico o *addendum* intervenuto tra le Parti) e prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento, nonché della relativa disciplina nazionale.

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 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 dell'Autorità di controllo per inadempienze normative o contrattuali commesse dallo stesso Responsabile.

Art. 6 – Il presente atto è parte integrante e sostanziale del Capitolato speciale d'appalto allegato al Contratto in oggetto; pertanto, ha termine lo stesso giorno in cui si ha la conclusione dell'appalto stesso, o per intervenuta scadenza naturale o per risoluzione anticipata o per recesso.

Art. 7 – E' 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.

[1] **Attenzione:** ai fini dell'**autorizzazione al subappalto** si deve **verificare se** anche il **subappaltatore** (o altro **sub-fornitore,** anche se questi non è rilevante ai fini della tracciabilità dei flussi finanziari ex art. 3 della L. n. 136/2010) **è tenuto, in ragione del Contratto d'appalto, al trattamento di dati personali** e, **se è così**, a tal fine, **deve essere autorizzato** dal Titolare quale Sub-Responsabile del trattamento.