Allegato del Capitolato Tecnico per la fornitura di nuovi Dispositivi Medici

Titolo allegato: “ISTRUZIONI e ATTO DI NOMINA per il Responsabile del Trattamento dei dati”

Sommario

Art 1 “Nomina del Responsabile del Trattamento”

AI sensi e per gli effetti dell’art. 28 del Regolamento GDPR, in occasione della stipula del Contratto di appalto (di seguito “Contratto”), con il presente Atto l’**Azienda Provinciale per i Servizi Sanitari** (di seguito “APSS”), in qualità di Titolare del Trattamento dei dati (di seguito “Titolare”), nomina la Ditta / Società ……. (*) quale Responsabile del trattamento dei dati (di seguito “Responsabile”) e l’autorizza al solo trattamento necessario alla corretta esecuzione della fornitura del Dispositivo Medico (di seguito DM) secondo quanto stabilito nell’art. 3 e dal Contratto. Ovvero il Responsabile si impegna a trattare i dati ai soli fini dell’esecuzione dei servizi oggetto del Contratto, secondo l’ambito di trattamento definito nell’art. 3 del presente Atto e nel rispetto della normativa vigente in materia di protezione dei dati personali, nonché delle istruzioni impartite dal Titolare nel presente Atto o in atti successivi.

Il Titolare quindi riconosce che la suddetta ditta (*, di seguito anche “Fornitore”) risulta esser idonea ad assumere tale ruolo ed impartisce di seguito le istruzioni e gli obblighi disciplinari che il Responsabile deve osservare durante il trattamento dei dati per conto di APSS 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 “Autorizzazione del Titolare per la nomina di sub-Responsabili”

Il Responsabile non ricorre ad altro ulteriore Responsabile del trattamento (di seguito “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 del trattamento, dando così al Titolare l’opportunità di opporsi a tali modifiche. Il Responsabile non può ricorrere a Sub-Responsabili nei cui confronti il Titolare abbia manifestato la sua opposizione.

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 che il trattamento soddisfi i requisiti del Regolamento, nonché della relativa disciplina nazionale.

In particolare, nel caso in cui il Responsabile ricorra ad un sub-Responsabile stabilito in un Paese extra-UE, sarà suo onere adottare adeguati strumenti per legittimare il trasferimento ai sensi dell’art. 44 e ss. del Regolamento.

Il Titolare ha diritto di chiedere al Responsabile del trattamento il rilascio della copia degli accordi stipulati tra Responsabile e sub-Responsabile (omettendo le sole informazioni strettamente confidenziali e gli accordi economici, se del caso).

Qualora il sub-Responsabile ometta di adempiere ai propri obblighi, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'inadempimento degli obblighi del sub-Responsabile. In tutti i casi, il Fornitore si assume la responsabilità nei confronti di APSS per qualsiasi omissione o violazione realizzati da un sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il Fornitore abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

*** 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 dei dati personali e, se è così, a tal fine, deve esser autorizzato dal Titolare quale Sub-Responsabile del trattamento.*

Art 3 "Ambito del trattamento"

Il Responsabile è obbligato a trattare i dati personali soltanto su istruzione documentata del Titolare: in particolare, in relazione al Contratto, il Responsabile può trattare i dati esclusivamente nell'ambito stabilito dal Titolare del trattamento.

Nella seguente tabella viene definito l'ambito di trattamento stabilito da APSS, in qualità di Titolare del Trattamento dei dati, per la fornitura in oggetto del presente Contratto.

AMBITO DI TRATTAMENTO AUTORIZZATO DA APSS
Dati personali presumibilmente trattati dal DM:
X dati sensibili (dati relativi alla salute, dati genetici, dati biometrici,..) □ dati anagrafici del paziente (nome, cognome, CF,..), residenza e/o domicilio del paziente □ dati anonimi (dati clinici senza alcun riferimento a dati anagrafici o identificativi che possono far risalire al paziente o cittadino a cui si riferiscono)
Categorie di interessati coinvolti nel trattamento dei dati:
X pazienti □ soggetti sani □ altri.....
Finalità del trattamento:
X Limitato alle attività di assistenza tecnica e istruzione all'uso □ Limitato alle attività di sola assistenza tecnica nel periodo di garanzia □ Limitato alle attività di sola istruzione all'uso (collaudo)
Operazioni di Trattamento approvate da APSS

TIPOLOGIA TRATTAMENTO	**PERIODICITA' del TRATTAMENTO**		
	OCCASIONALE	**CONTINUATIVO**	**MAI**
Raccolta			X
Registrazione			X
Organizzazione			X
Strutturazione			X
Conservazione			X
Consultazione	X, limitatamente alla finalità sopra indicata		

Uso			X
Modifica			X
Estrazione			X
Elaborazione/analisi			X
Copia di backup di sicurezza	X, limitatamente a quanto stabilito art 9		
Comunicazione			X
Diffusione			X
Cancellazione o distruzione	X, limitatamente a quanto stabilito art 9		X
Raffronto o interconnessione			X
Limitazione			X
Profilazione			X

Tabella 1: Ambito del trattamento definito dal Titolare del trattamento dei dati (APSS) e per cui l'eventuale Responsabile del trattamento dei dati viene autorizzato.

Nel caso in cui l'Aggiudicatario abbia incluso nell'offerta tecnica ulteriori ambiti di trattamento come riportato nel documento "Offerta tecnica: Allegato Privacy rev2.0" ed approvati, quali elementi migliorativi, da APSS nella Verifica di Conformità dell'offerta tecnica, la presente Nomina a Responsabile del Trattamento dei dati viene estesa (con il presente Atto) all'ambito di applicazione offerto dall'Aggiudicatario.

Come sancito dal GDPR, qualora il Responsabile determini autonomamente le finalità ed i mezzi di trattamento in violazione al Regolamento stesso, sarà considerato Titolare del trattamento assumendone i conseguenti oneri, rischi e responsabilità.

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.

Il Responsabile è consapevole ed accetta che i propri dati personali possano esser pubblicati sul sito istituzionale o sulla bacheca del Titolare per finalità di trasparenza nei confronti degli interessati.

Art 4 "Rispetto dei principi comunitari e nazionali"

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 art. 5 e 25 del Regolamento.

Il Responsabile riconosce espressamente che i dati personali trattati ai fini dell'esecuzione del Contratto hanno natura riservata e confidenziale. Pertanto il Responsabile si impegna ad utilizzare i dati personali esclusivamente ai fini dell'esecuzione del Contratto e nei limiti del presente Atto di nomina (art 3 "Ambito di trattamento"), nonché a mantenere i dati personali strettamente confidenziali e a non divulgarli o trasferirli, tutti o in parte, in qualsiasi modo, salvo autorizzazione scritta del Titolare e secondo le disposizioni del presente allegato al capitolato tecnico di gara o salvo sia obbligato in forza delle leggi a cui il Responsabile è soggetto.

Il Responsabile del trattamento, operando all'ambito dei suddetti principi, deve attenersi quindi ai compiti descritti dal titolare nei seguenti articoli.

Art 5 "Registro delle attività di trattamento"

In qualità di Responsabile del trattamento, il fornitore deve provvedere alla predisposizione del Registro delle attività di trattamento nei termini di cui art. 30 del Regolamento, mettendolo tempestivamente a disposizione del Titolare, o alle Autorità di controllo in caso di relativa richiesta.

Nel registro devono esser identificati e censiti i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività oggetto del Contratto (vedere art 3 "Ambito di trattamento") al fine di predisporre il registro delle attività di trattamento svolte per conto dell'Azienda Provinciale per i Servizi Sanitari della Provincia Autonoma di Trento (Titolare del trattamento). Tale registro deve esser esibito in caso di ispezione del'Autorità Garante e deve contenere almeno le seguenti informazioni:

a) il nome e i dati di contatto del Responsabile o dei responsabili del trattamento, del Titolare del trattamento per conto del quale agisce il Responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati (DPO);

b) le categorie dei trattamenti effettuati per conto del Titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la relativa documentazione di garanzia;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative applicate a protezione dei dati (di cui all'articolo 32, paragrafo 1).

Art 6 "Nomina del DPO del Responsabile del Trattamento"

Nei casi prescritti dall'art. 37 del Regolamento, oltre che nella fattispecie in cui tale adempimento sia raccomandato nelle specifiche Linee Guida del Gruppo di Lavoro art. 29, il Responsabile deve 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 dall'Autorità di controllo, garantendo il rispetto delle prescrizioni di cui all'art. 38 del Regolamento, anche allo scopo di consentire al medesimo DPO l'effettivo adempimento dei compiti di cui art. 39 del Regolamento.

In caso di nomina del DPO, il Responsabile deve comunicare al Titolare: il nome, i dati di contatto (indirizzo email e recapito telefonico) del proprio responsabile della protezione dei dati (DPO) nonché la durata della nomina.

Il Titolare comunica con la presente i riferimenti del proprio DPO:

Studio legale PwC Tax and Legal Services
referente: avv. Andrea Cardini Orlandi Lensi
contatto email: ResponsabileProtezioneDati@apss.tn.it

Art 7 “Personale preposto alle attività che prevedono un trattamento”

Il Responsabile deve garantire che le persone (sia dipendenti che collaboratori) preposte al trattamento dei dati personali per conto del Titolare APSS siano state specificatamente autorizzate, adeguatamente istruite e si siano impegnate alla riservatezza, o abbiano un adeguato obbligo legale di riservatezza.
Al fine di garantire un trattamento corretto, lecito e sicuro il Responsabile deve vigilare sull’operato delle persone durante il trattamento dei dati personali dei pazienti per conto di APSS. In particolare il Responsabile deve limitare l’accesso ai suddetti dati al solo personale che esegue le attività necessarie ai fini dell’esecuzione del Contratto.
Tutte le informazioni acquisite durante lo svolgimento delle attività autorizzate da APSS (vedere art 3 “Ambito del trattamento”) devono rimanere riservate anche dopo la cessazione del rapporto di lavoro con al Ditta stessa. In ogni caso il Fornitore è direttamente ritenuto responsabile per qualsiasi divulgazione o comunicazione di dati personali dei pazienti ad opera del suddetto personale.

Art 8 “Amministratori di sistema”

Nel caso in cui il dispositivo medico venga fornito completo di un applicativo software, un portale web-based per il trattamento dei dati e/o un database per la raccolta dei dati registrati dal DM, ed i suddetti sistemi software prevedono almeno un utente con il ruolo di Amministratore di sistema (ad esempio: per la configurazione del software o per la manutenzione), in conformità al Provvedimento delle Autorità Garante del 27 novembre 2008 e s.m.i., il Responsabile deve:

- provvedere alla designazione per iscritto del/degli Amministratore/i di Sistema secondo i criteri di individuazione e selezione previsti dal suddetto provvedimento,
- conservare l’elenco degli stessi Amministratori,
- verificare annualmente l’operato adottando sistemi idonei alla registrazione dei relativi accessi logici (da conservare con caratteristiche di inalterabilità e integrità per almeno 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, il Responsabile deve comunicare a quest’ultimo l’identità degli Amministratori di Sistema (provvedendo a dare idonea informativa, ex art. 13 del Regolamento, agli stessi Amministratori di sistema).

Nel caso di sistemi software che prevedono almeno un utente con il ruolo di Amministratore di sistema al termine del Contratto il Responsabile del trattamento dei dati deve procedere alla modifica della password dell’account con il suddetto ruolo di Amministratore di sistema onde evitare accessi non autorizzati da parte del proprio personale dopo il termine del contratto. Nel caso di mancato rinnovo del contratto, al fine di garantire il servizio di assistenza tecnica nel periodo post-garanzia del DM, il Responsabile deve comunque collaborare con il Titolare nel fornire al nuovo Responsabile (ditta aggiudicataria per il nuovo contratto di fornitura del servizio di manutenzione del DM e relativo sistema sw) le credenziali di accesso dell’utente con ruolo di Amministratore di Sistema.

Nel caso di assistenza da remoto al termine del contratto verrà inibito l’accesso all’IP del suddetto sistema software dai Sistemi Informatici di APSS onde evitare accessi non autorizzati. Nel caso invece di assistenza in loco il personale clinico del reparto (in cui è in uso il DM e il relativo sistema software) verrà avvisato del termine contrattuale e che quindi il personale tecnico dell’Aggiudicatario non è più autorizzato ad accedere al DM e relativo software.

Art 9 “Obblighi di sicurezza”

Il Responsabile adotta e mantiene le misure tecniche e organizzative adeguate per proteggere la sicurezza, la riservatezza e l’integrità dei dati personali tenendo conto: dei pericoli di varia probabilità e gravità (di distribuzione o perdita, di modifica, di divulgazione non autorizzata o di accesso accidentale o illegale a dati trasmessi, conservati o comunque trattati), dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento (art 32 del Regolamento). Laddove il trattamento comporti trasmissioni di dati su una rete, il Responsabile deve proteggere i dati da qualsiasi altra forma illegittima di trattamento.

In caso di trattamento con strumenti automatizzati, il Responsabile garantisce di aver adottato misure di sicurezza analoghe e non inferiori al livello ……* [“minimo”, “standard“ o “altro”] di cui alla circolare Agid nr. 2/2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni) e s.m.i. Nel caso in cui l’offerta tecnica preveda anche la gestione di un database per la raccolta dei dati sensibili registrati da/dal dispositivo/i medico/i, il Responsabile deve assicurare la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico, testare e verificare periodicamente l’efficacia delle misure tecniche ed organizzative applicate (es: backup periodici di sicurezza,..).

** Tale livello di sicurezza deve esser concordato con il Titolare sulla base di un’adeguata analisi del rischio.*

Il Responsabile deve inoltre:

- definire una politica di sicurezza per assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- 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 eventuali ispezioni, realizzate dal Titolare, dal suo Data Privacy Officer (DPO) o da un altro soggetto a ciò deputato;
- assistere il Titolare nel garantire il rispetto degli obblighi di cui da art. 32 a 36 del Regolamento. In particolare, relativamente alla predisposizione della “valutazione di impatto” (alias “Data privacy impact assessment” di cui agli art. 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;
- mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente Atto di designazione;
- collaborare, su richiesta del Titolare, con gli altri Responsabili esterni del trattamento al fine di armonizzare e coordinare l’intero processo di trattamento dei dati personali;
- realizzare quant’altro sia ragionevolmente utile e/o necessario al fine di garantire l’adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati personali, nei limiti dei compiti affidati con il presente Atto di designazione;
- informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia che il trattamento dei dati violi la normativa in materia dei dati personali o presenti comunque rischi specifici per i diritti degli interessati o qualora, a suo parere, un’istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che

gli rendono illeciti o impossibile agire secondo le istruzioni ricevute dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Art 9 – bis "Obblighi di sicurezza durante interventi di collaudo e formazione"

In occasione del collaudo o di demo dimostrative ai fini della formazione degli operatori sanitari e/o tecnici al corretto e sicuro utilizzo del Dispositivo Medico, il/i Responsabile/i deve seguire le seguenti istruzioni operative (obblighi e compiti):

- limitare l'accesso ai dati del/i paziente/i al solo personale che esegue le attività necessarie ai fini della formazione del personale APSS sul corretto utilizzo e sulle funzionalità del D.M. (durante il collaudo o demo dimostrative);
- Non utilizzare o accedere a dati personali, sensibili e/o genetici se non per ragioni connesse al servizio richiesto, per cui la visualizzazione dei dati sia indispensabile per l'espletamento della formazione. La consultazione quindi deve limitarsi esclusivamente ai dati necessari per un efficace formazione sul corretto e sicuro utilizzo del D.M. e per il tempo strettamente necessario all'effettuazione dell'intervento (inclusi i test dimostrativi sulle funzionalità del dispositivo medico);
- Adottare misure minime di sicurezza al fine di impedire accessi non autorizzati all'apparecchiatura (HW e SW) e/o al relativo archivio (es: archivio nel PC ambulatoriale a cui viene collegato il DM) o ai servizi di rete accessibili dal dispositivo medico (o dal relativo applicativo software);
- Durante l'intervento il personale non può:
    - Accedere ad altri servizi di rete accessibili dal D.M. o dal relativo PC ambulatoriale a cui viene collegato il DM;
- Dopo l'intervento deve:
    - provvedere alla cancellazione irreversibile dei dati dei pazienti generati ed utilizzati ai fini dimostrativi delle funzionalità del DM
    - nel verbale d'intervento riportare il riferimento del tecnico e la tipologia di azioni effettuate

Art 9 – ter "Obblighi di sicurezza durante interventi di assistenza"

Durante gli interventi di assistenza tecnica (manutenzione preventiva o correttiva) in loco o da remoto il/i Responsabile/i deve seguire le seguenti istruzioni operative (obblighi e compiti):

- limitare l'accesso ai dati del/i paziente/i al solo personale che esegue le attività necessarie ai fini della risoluzione del guasto/malfunzionamento del D.M.;
- Non utilizzare o accedere a dati personali, sensibili e/o genetici se non per ragioni connesse al servizio richiesto, per cui la visualizzazione dei dati sia indispensabile per l'espletamento dell'intervento di manutenzione. La consultazione quindi deve limitarsi esclusivamente ai dati necessari per un efficace risoluzione del guasto o malfunzionamento del D.M. e per il tempo strettamente necessario all'effettuazione dell'intervento (inclusi i test di verifica della risoluzione della problematica);
- Adottare misure minime di sicurezza al fine di impedire accessi non autorizzati all'apparecchiatura (HW e SW) e/o al relativo archivio (es: archivio nel PC ambulatoriale a cui viene collegato il DM) o ai servizi di rete accessibili dal dispositivo medico (o dal relativo applicativo software);
- Prima dell'intervento deve:
    - verificare la disponibilità di una copia di backup ed in caso effettuare un backup di sicurezza dei dati al fine di salvaguardare i dati sensibili memorizzati nell'apparecchiatura;
- Durante l'intervento il personale non può:

- Accedere ad altri servizi di rete accessibili dal D.M. o dal relativo PC connesso;
- Trasferire, in tutto o in parte, in nessun modo i dati senza previa autorizzazione scritta del Titolare (es: backup autorizzati di sicurezza prima di iniziare l'intervento al fine di salvaguardare i dati sensibili memorizzati sull'apparecchiatura);
- Lasciare incustoditi eventuali supporti di memoria rimossi durante l'intervento. Tali supporti di memoria non possono essere duplicati se non assolutamente necessario all'effettuazione dell'intervento stesso;

- Dopo l'intervento deve:
  - ripristinare tempestivamente la disponibilità e l'accesso dei dati dei pazienti al termine dell'intervento di manutenzione correttiva e/o preventiva, cancellando il backup di sicurezza solo dopo aver verificato l'integrità dei dati ripristinati nel DM;
  - provvedere alla cancellazione irreversibile o alla distruzione dei supporti di memoria utilizzati durante l'intervento o duplicati o presenti sulle apparecchiature sostituite o temporaneamente utilizzate come muletto;
  - nel verbale d'intervento riportare il riferimento del tecnico e la tipologia di azioni effettuate.
- Ove applicabile fornire, su richiesta di APSS, i log degli accessi tramite servizi di rete offerti dall'Aggiudicatario assieme al D.M..

Art 9 – quater "Obblighi di sicurezza durante interventi di assistenza da remoto"

Nel caso in cui l'offerta tecnica dell'Aggiudicatario include anche il servizio di assistenza da remoto, la ditta che effettua tale attività di trattamento deve esser nominata Responsabile del trattamento dal titolare APSS con il presente Atto (se l'Aggiudicatario non si avvale di sub-fornitori per la suddetta attività) oppure nominata sub-Responsabile da parte dell'Aggiudicatario (nel caso in cui l'Aggiudicatario si avvale di un sub-fornitore, quale ad esempio la casa madre del DM, per svolgere la suddetta attività) previa autorizzazione da parte del Titolare del trattamento dei dati.

Il Responsabile deve garantire una connessione sicura e solo il personale autorizzato può acceder da remoto al dispositivo medico. Il Responsabile deve consegnare, su richiesta del Titolare in caso di accertamenti/audit:

- dati identificativi della ditta che effettua la suddetta attività (in caso di Sub-Responsabile);
- le modalità di connessione da remoto e le politiche di accesso;
- i protocolli di trasmissione (se in chiaro o crittografato);
- i riferimenti degli Amministratori di Sistema che possono accedere da remoto al device e/o applicativo sw e/o database;
- gli accessi eseguiti e il relativo elenco delle operazioni effettuate.

Le stesse indicazioni valgono nel caso in cui l'Appalto preveda la gestione da parte del Responsabile di uno o più database (di seguito "DB") per la raccolta dei dati sensibili registrati dal/i dispositivo/i medico/i installato/i presso una o più sedi APSS. In tal caso il Responsabile deve indicare al Titolare la localizzazione geografica dei suddetti database su server fisico o virtuale (es: in cloud) e i relativi dati identificativi (nome del server, indirizzo IP,..). Nonché le politiche di accesso al DB, i nominatori degli Amministratori di sistema, la gestione dei log di accesso al DB, le politiche di backup, le politiche di sicurezza (es: i piani di continuità operativa,..) e i protocolli di trasmissione dei dati tra DB e dispositivi medici.

Art 10 "Trasferimento e trattamento dei dati personali fuori dall'UE"

Qualora i dati personali oggetto del trattamento fossero trasferiti verso Paesi Terzi ovvero organizzazioni internazionali, il Responsabile deve 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.

Il Responsabile del Trattamento …… (indicare nominativo o ragione sociale) con la presente dichiara che:

□ non trasferisce e tratta dati personali fuori dall'area economica europea;

□ trasferisce e tratta dati personali fuori dall'area economica europea. In tale fattispecie il trasferimento dei dati avviene nel rispetto dell'art 44 del Regolamento e delle condizioni riportate in Tabella nr. 2.

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI
Trasferimento in base ad una Decisione di Adeguatezza (art 45 del Regolamento)
□ Si, indicare la decisione di adeguatezza……..
Trasferimento in base a garanzie adeguate senza autorizzazione dell'autorità competente (art 46 del Regolamento)
□ norme vincolanti d'impresa in conformità appositamente approvate (indicare l'autorità ……)
□ clausole tipo di protezione dei dati adottate dalla Commissione
□ clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione
□ un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del Responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
□ un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del Responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.
□ le clausole contrattuali tra il titolare del trattamento o il Responsabile del trattamento e il titolare del trattamento, il Responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale che siano state appositamente autorizzate dall'Autorità di controllo competente
□ altre modalità ……

Tabella 2: Modalità di trasferimento di dati personali verso paesi terzi o organizzazioni internazionali (Regolamento art. 45 e 46).

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.

Art 11 "Data breach"

Qualsiasi evento che possa comportare una violazione, anche accidentale, dei dati personali oggetto del trattamento, deve esser immediatamente comunicato dal Responsabile al DPO del Titolare, fornendo tutte le informazioni disponibili sull'evento e prestando la necessaria collaborazione con il Titolare in relazione all'adempimento degli obblighi previsti dal Regolamento. In particolare il Responsabile, in tal caso, deve compilare la "Scheda Segnalazione" definita nella procedura APSS per la gestione dei Data Breach e riportata in calce al presente documento.

Con riferimento ai casi di *data breach* (di cui art. 33 e 34 del Regolamento), nel caso in cui gli strumenti/applicativi informatici del Titolare fossero forniti o gestiti dal Responsabile, quest'ultimo è comunque tenuto a comunicare immediatamente al Titolare (struttura competente in materia di protezione dei dati personali) tutte le informazioni necessarie a consentirgli di effettuare i conseguenti adempimenti in materia di violazione di dati personali previsti dal Regolamento.

Art 12 "Valutazioni d'impatto ed analisi del rischio"

Il Responsabile deve assistere il Titolare nell'effettuare la valutazione di impatto sulla protezione dei dati nonché dell'eventuale consultazione preventiva alla Autorità Garante (art. 35 e 36 del Regolamento), fornendo tutte le informazioni e gli elementi utili a tal fine.

Il Responsabile è tenuto a predisporre ed aggiornare l'analisi del rischi (probabilità di violazione della sicurezza dei dati) del dispositivo medico/applicativo informatico, comunicandola al Titolare ed adottando i criteri di valutazione forniti da quest'ultimo (nel modulo Privacy richiesto in gara nella documentazione tecnica).

Con riferimento inoltre all'esito dell'analisi dei rischi condotta dal Titolare sul trattamento dei dati personali cui concorre il Responsabile (assieme ad eventuali sub-Responsabili), quest'ultimo assicura massima collaborazione e assistenza al fine di dare effettività alle azioni di mitigazione eventualmente previste dal Titolare per ridurre possibili rischi identificati.

Art 13 "Audit"

Con riferimento inoltre all'esito dell'analisi dei rischi condotta dal Titolare sul trattamento dei dati personali cui concorre Il Responsabile si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte del Titolare, consentendo pertanto all'APSS l'accesso ai proprio locali e ai locali di qualsiasi Sub-Responsabile eventualmente nominato, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il fornitore e/o sub-fornitore rispettino gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, dal presente accordo.

La conduzione di tali audit da parte del Titolare o suo delegato non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

Il rifiuto del Responsabile di consentire al Titolare di effettuare l'audit comporta la risoluzione del contratto.

Art 14 "Istanze degli interessati"

Il Responsabile deve 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). In particolare deve:

- informare tempestivamente il Titolare dei reclami eventualmente presentati dagli interessati;
- fornire tempestivamente tutte le informazioni necessarie e/o i documenti utili ai fini di soddisfare le richieste degli interessati (ad esempio: richieste di accesso, rettifica, limitazione, opposizione al trattamento dei dati, oscuramento,..);
- collaborare con il DPO del Titolare fornendo ogni informazione e/o documento richiesto;
- qualora il trattamento dei dati personali oggetto del Contratto comporti la raccolta di dati personali da parte del Responsabile del trattamento, questi provvede al rilascio della relativa informativa ai soggetti interessati.

Art 15 “Durata”

Il presente atto è parte integrante e sostanziale del Capitolato tecnico 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.

La durata del periodo di garanzia del Dispositivo Medico è conforme a quanto offerto dall’Aggiudicatario in sede di gara, quindi al termine del suddetto periodo il Titolare può decidere se rinnovare la nomina del Responsabile mediante un Contratto di rinnovo della manutenzione oppure affidare tale incarico ad un ente terzo. In tal caso il Responsabile deve fornire tutte le informazioni necessarie affinché la protezione dei dati sia garantita e conforme al Regolamento anche nel periodo di post garanzia del Dispositivo Medico oggetto della presente fornitura.

Anche successivamente alla cessazione o alla revoca del Contratto, il Responsabile ed eventuali sub-Responsabili dovranno mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell’adempimento dei suoi obblighi.

Art 16 “Restituzione e cancellazione dei dati”

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 compresa ogni eventuale copia esistente) dei dati personali in oggetto (dandone conferma scritta la 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.

Il Responsabile deve rilasciare un’attestazione scritta che presso la propria struttura o presso eventuali sub-Responsabili non esiste più alcuna copia dei dati trattati per conto di APSS nei seguenti casi:

- restituzione dei dati al Titolare (incluse tutte le eventuali copie di backup e/o tutta la documentazione cartacea) oppure
- cancellazione dei dati presso il Responsabile ed eventuali Sub-Responsabili.

In caso di richiesta scritta del Titolare, il Responsabile è tenuto ad indicare le modalità tecniche e le procedure utilizzate per la cancellazione o distruzione.

La restituzione e cancellazione dei dati deve esser attuata anche nel caso di sostituzione di un dispositivo medico guasto.

Art 17 “Rapporti con le Autorità”

Il Responsabile provvede ad informare tempestivamente il Titolare del trattamento di ogni richiesta, ordine o attività di controllo da parte dell’Autorità Garante per la protezione dei dati personali o dell’Autorità Giudiziaria e coadiuva il Titolare stesso nella difesa in caso di procedimenti dinanzi dalle suddette Autorità che riguardano il trattamento dei dati oggetto del Contratto. A tal fine il Responsabile fornisce, in esecuzione del Contratto, e quindi, gratuitamente, tutta la dovuta assistenza ad APSS per garantire che la

stessa possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

Art 18 "Risarcimento civile o responsabilità amministrative"

In caso di 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 e contrattuali commesse dallo stesso Responsabile.

Art 19 "Modifiche al presente Atto"

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 al 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.

Per quanto non espressamente previsto nel presente Atto di designazione, si rinvia alle disposizione generali vigenti in materia di protezione dei dati personali, nonché alle disposizioni di cui al Contratto stipulato tra le parti sopra individuato. Si precisa altresì che qualora l'adozione del D.Lgs 101 del 10 agosto 2018 o successive disposizioni normative in materia di adeguamento del DGPR incidano sulla figura del Responsabile del trattamento, la presente nomina sarà integrata a cura del Titolare.

Il presente atto di nomina è regolato dalla legge italiana. Per tutte le controversie derivanti da o in connessione con il presente Atto di nomina il Foro Competente esclusivo sarà il Tribunale della sede legale del Titolare.

Art 20 "Accettazione della Nomina"

Il legale rappresentante della Ditta/ Società …….. nella sua qualità di Responsabile del trattamento dei dati stabilito nel presente Atto:

- Accetta la nomina;
- Si impegna a procedere al trattamento dei dati personali attenendosi alle disposizioni di cui alla normativa in materia di protezione dei dati personali ed alle istruzioni impartite dal Titolare APSS nel presente Atto o in atti successivi;
- Dichiara di aver ricevuto ed esaminato i compiti e le istruzioni sopra indicate

Il Responsabile del trattamento dei dati

Dott. _____ Luogo e data _____

Azienda Provinciale per i Servizi Sanitari
Provincia Autonoma di Trento

Scheda Segnalazione

Il/La sottoscritto/a [Nome e Cognome] _____,

nato/a il ____ / ____ / _____, nel Comune: _____, Provincia: _____,

Stato: _____, codice fiscale: ☐☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐,

quale:

- persona direttamente interessata;
- per conto della persona interessata [Nome e Cognome] _____,
  nato/a il ____ / ____ / _____, nel Comune: _____, Provincia: _____,
  Stato: _____, codice fiscale: ☐☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐,
  residente all'indirizzo: _____,
  nel Comune: _____, Provincia: ____, Stato_____, dichiarando di essere, consapevole di quanto prescritto dagli art. 76 e 73 del D.P.R. n. 445 del 28 dicembre 2000 sulle sanzioni penali per le ipotesi di falsità in atti e dichiarazioni mendaci:
  ☐ Tutore ☐ Legale rappresentante ☐ Amministratore di sostegno ☐ Esercente la responsabilità genitoriale
- preposto al trattamento, responsabile del trattamento, operatore autorizzato al trattamento;
- amministratore di sistema (interno o esterno) e tecnico di Dipartimento Tecnologie o Servizio Ingegneria Clinica;
- tecnico manutentore esterno che gestisce e/o manutiene apparecchiature elettromedicali o software medicali;
- altro soggetto esterno all'Azienda diverso dall'Interessato.

segnala un evento legato alla privacy, indicando le seguenti informazioni:

- data e ora dell'evento: ____ / ____ / _____, luogo dell'evento: _____,
- breve descrizione dell'evento: _____
  _____,
- unità organizzative coinvolte: _____,
- note o altre informazioni utili: _____
  _____,

Nell'evento sono coinvolti dati personali ?

○ No ○ Sì – informazioni correlate:

- tipologia dei dati personali coinvolti [identificativi, sanitari, economici/finanziari, giuridici, genetici, altri dati particolari]: _____,
- numero approssimativo dei dati personali coinvolti [0-10, 11-50, 51-100, 101-500, >500]: _____,
- categorie di interessati coinvolti: _____,
- numero approssimativo di persone coinvolte nell'evento [0-10, 11-50, 51-100, 101-500, >500]: _____,

- tipologia degli strumenti coinvolti [procedure organizzative / sistemi informatici / modulistica / documenti cartacei / apparecchiature medicali / rete dati / banca dati] _____.

Lo scrivente indica i seguenti riferimenti ai quali inviare ogni comunicazione relativa alla presente pratica:

tel. / cell.: _____ e/o email: _____.

Con la seguente firma dichiaro di aver preso visione della seguente informativa sul trattamento dei dati personali e di aver compreso quanto indicato nella stessa.

_____ _____

luogo e data firma del segnalante (estesa e leggibile)

INFORMATIVA TRATTAMENTO DEI DATI PERSONALI

Art. 13 Regolamento UE 2016/679

- I dati personali forniti nell'ambito della presente domanda verranno trattati esclusivamente per le seguenti finalità: esecuzione di un compito di interesse pubblico di cui è investita l'Azienda Provinciale per i Servizi Sanitari (APSS), in base agli artt. 6, par. 1, lett. e) e 9, par. 2, lett. g), Regolamento Ue 2016/679 ed, in particolare, per la gestione da parte di APSS della segnalazione.
- Il conferimento dei dati personali è obbligatorio per dar corso al procedimento di cui alla presente domanda e per tutte le attività connesse. Il rifiuto al conferimento dei dati comporterà l'impossibilità di dar corso alla presente domanda e di espletarne il relativo procedimento.
- Il trattamento sarà effettuato con modalità cartacee e con strumenti informatici/elettronici con logiche atte a garantire la riservatezza, l'integrità e la disponibilità dei dati stessi.
- I dati personali sono trattati, esclusivamente per le finalità di cui sopra, da personale autorizzato, in qualità di Preposti al trattamento/Addetti al trattamento dei dati/Responsabili del trattamento appositamente nominati ed istruiti.
- È esclusa l'esistenza di un processo decisionale automatizzato, compresa la profilazione.
- I dati personali forniti verranno conservati per i tempo previsto nel Piano di conservazione, allegato al manuale di gestione, disponibile nel sito internet APSS https://www.apss.tn.it/privacy.
- I dati personali non saranno trasferiti fuori dall'Unione Europea.
- Il titolare del trattamento dei dati personali è l'Azienda Provinciale per i Servizi Sanitari (APSS) con sede in via Degasperi n. 79 a Trento a cui l'interessato potrà rivolgersi per far valere, nei casi previsti, i diritti di cui al Capo III del Regolamento, tramite l'Ufficio rapporti con il pubblico (URP) sito a Palazzo Stella in Via Degasperi, n. 77 – 38123 Trento – tel. 0461/904172 urp@apss.tn.it.
- L'interessato per le questioni relative al trattamento dei propri dati personali può rivolgersi al Responsabile della protezione dei dati (RPD) i cui dati di contatto sono i seguenti: Via Degasperi, 79 – 38123 Trento, e-mail ResponsabileProtezioneDati@apss.tn.it
- L'interessato ha diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali in caso di illecito trattamento o di ritardo nella risposta del Titolare a una richiesta che rientri nei diritti dell'interessato.

SEZIONE DI COMPETENZA DEL D.P.O. DELL'APSS di TRENTO

rif. pratica: _____ data e ora della segnalazione: ___ / ___ / _____

La segnalazione è un evento che riguarda dati personali?

○ No ○ Sì – informazioni correlate:

- nominativo del Preposto individuato: _____,
- data invio Scheda al Preposto: ___ / ___ / _____, data riscontro dal Preposto: ___ / ___ / _____,

_____ _____

luogo e data firma del D.P.O.