Regione Abruzzo

Procedura per la

Designazione del Responsabile del Trattamento e per la gestione di accordi di Contitolarità

della ASL Teramo

in base a quanto previsto dal

Regolamento UE 2016/679 sulla Protezione dei Dati (GDPR) – artt. 26 e 28

e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali

(Art. 2-quaterdecies)

Redazione	Verifica	Parere favorevole	Approvazione
R.T.I.	UOSD Segreteria di Direzione	D.P.O.	Titolare

Sommario

1 Introduzione

La normativa vigente in termini di Protezione dei Dati Personali, costituita dal Regolamento UE 2016/679 – Regolamento sulla Protezione dei Dati (di seguito anche il "Regolamento") e dal D. Lgs. 196/2003 – Codice in materia di Protezione dei Dati Personali (di seguito anche il "Codice") come modificato dal D. Lgs. 101/2018, ha l'obiettivo di proteggere i dati personali degli interessati al fine di evitare che un uso non corretto delle informazioni possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati. Considerato il contesto operativo dell'Azienda Sanitaria, tali problematiche sono di notevole rilevanza.

Le tipologie di dati personali trattati dall'Azienda Sanitaria sono costituiti principalmente sia da dati personali (ad esempio dati anagrafici, recapiti, identificativi di tessera sanitaria, codici fiscali, ecc...) che da "particolari categorie di dati personali" quali i dati relativi alla salute.

2 Scopo

L'obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle Nomine e Designazioni a Responsabile del Trattamento (RT) dei Dati Personali e degli Accordi tra contitolari del trattamento dei dati e delle relative indicazioni operative al fine di poter consentire alla Direzione Generale ed ai Soggetti Autorizzati alle Unità Operative di poter procedere con le azioni di propria competenza.

La ASL Teramo (di seguito anche la "ASL") ha predisposto il presente documento nell'ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati che descrive le modalità operative adottate dalla ASL, per il rispetto di quanto previsto dall' Art. 28 del Reg. UE 2016/679 (GDPR – General Data Protection Regulation) e della vigente normativa di settore.

3 Destinatari

Il presente documento regolamenta il processo di gestione degli accordi tra Contitolari e delle nomine e designazioni dei Responsabili del trattamento (RT) nelle varie casistiche che possano presentarsi nelle strutture amministrative, ospedaliere e territoriali della ASL di Teramo.

4 Definizioni

Le seguenti definizioni sono di utilità per comprendere i termini esposti nella procedura e nei documenti allegati, secondo l'art. 4 del Regolamento e secondo l'organigramma interno aziendale:

«dato personale»: 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;

«trattamento»: 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;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«contitolarità»: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento, sono contitolari del trattamento;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«violazione dei dati personali»: 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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«banca di dati»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«evento sulla sicurezza delle informazioni»: occorrenza identificata di uno stato di un sistema, servizio o della rete che indichi una possibile violazione di una policy sulla sicurezza delle informazioni (Information Security Policy) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza;

«incidente sulla sicurezza delle informazioni»: evento singolo o serie di eventi sulla sicurezza delle informazioni indesiderati o imprevisti che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni;

«DPO - RPD»: Data Protection Officer o Responsabile della Protezione Dati;

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento;

«trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

«UOC»: Unità Operativa Complessa;

«UOSD»: Unità Operativa Semplice Dipartimentale;

«AUT I»: Soggetto Autorizzato al Trattamento dei dati personali di I livello;

«AUT II»: Soggetto Autorizzato al Trattamento dei dati personali di II livello;

«RT»: Responsabile del Trattamento dei dati personali;

«SRT»: Sub-Responsabile del Trattamento dei dati personali.

5 Normativa di Riferimento

La normativa di riferimento per la gestione delle nomine, designazioni ed accordi si compone di vari riferimenti, tra cui:

- normativa di riferimento per la designazione di Responsabili del trattamento,

- normativa di riferimento per i Trattamenti effettuati sotto l'autorità del Titolare o del Responsabile del Trattamento,

- normativa di riferimento per gli Accordi di Contitolarità.

5.1 Normativa di riferimento per la designazione di Responsabili del Trattamento - Articolo 28 Responsabile del trattamento

In base alla definizione data dall'art. 4.8 del Regolamento il "Responsabile del Trattamento" è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il riferimento normativo principale per la gestione del rapporto con in Responsabili del Trattamento è costituito dall'Art. 28 del Regolamento di seguito riportato.

1. 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.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione 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 la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 del Regolamento;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 del Regolamento può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43 del Regolamento.

7. Il Titolare può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93 del Regolamento, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63 del Regolamento.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 82, 83 e 84 del Regolamento, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

5.2 Normativa di riferimento per i Trattamenti effettuati sotto l'autorità del Responsabile del Trattamento - Articolo 29 Trattamento sotto l'autorità [...] del responsabile del trattamento

La normativa applicabile per la nomina di soggetti che trattano dati personali sotto l'autorità del Responsabile del Trattamento è costituita dai seguenti punti:

- Art. 29 del Regolamento - Trattamento sotto l'autorità [...] del responsabile del trattamento
- Art. 2-quaterdecies – Attribuzione di funzioni e compiti a soggetti designati

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 del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

5.2.1 Art. 2-quaterdecies – Attribuzione di funzioni e compiti a soggetti designati

1. I responsabili del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2. I responsabili del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

I fornitori che trattano dati per conto del titolare del trattamento e sono, pertanto, designati al trattamento ex art. 28 GDPR, devono istruire ed autorizzare al trattamento tutti i soggetti che trattano dati sotto la propria responsabilità ex art. 29 GDPR ed ex art. 2.14 del Codice Privacy.

5.3 Normativa di riferimento per gli Accordi di Contitolarità - Articolo 26 Contitolari del trattamento

1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un

accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

6 Descrizione del Processo

6.1 Responsabili del Trattamento

6.1.1 Identificazione e Classificazione

Come indicato dall'art. 28 del Regolamento, qualora un'attività che preveda il trattamento di dati personali di persone fisiche, debba essere effettuato per conto della ASL, quest'ultima 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.

Per quanto concerne la designazione dei Responsabili del trattamento, la ASL, ha previsto di lasciare in capo al Titolare del trattamento la gestione della nomina; tuttavia, il Titolare, si avvale della collaborazione della UOC ABS/UTE/UO procedenti e del Responsabile Unico del Procedimento (RUP), secondo la procedura che in seguito si esplica.

Con riferimento a quanto disciplinato nella presente procedura, il censimento dei fornitori risulta essere la condizione necessaria per avere la piena consapevolezza delle attività di trattamento di dati personali che vengono svolte per suo conto.

Inoltre, al fine di individuare – tra tutti i soggetti fornitori di prodotti e servizi per l'ASL– coloro i quali trattano dati per conto del titolare, è senz'altro indispensabile tenere traccia dell'oggetto della fornitura e degli altri elementi caratterizzanti del prodotto/servizio: così facendo, il titolare si assicura la possibilità di individuare eventuali trattamenti di dati personali effettuati dai fornitori, al fine di poter agevolmente identificare i soggetti che operano in qualità di responsabili del trattamento, ai sensi dell'articolo 28 del Regolamento UE 2016/679.

A titolo esemplificativo e non esaustivo, si riporta qui di seguito una rappresentazione di alcuni ambiti in cui il trattamento di dati personali è di norma previsto (a sinistra), distinguendoli da altri che invece normalmente non prevedono la necessità di sottoscrivere l'accordo per il trattamento:

Accordo con il responsabile del trattamento GENERALMENTE RICHIESTO per:	Accordo con il responsabile del trattamento GENERALMENTE NON RICHIESTO per:
Fornitori di servizi informatici	Pubbliche amministrazioni e Professionisti esterni
Fornitori di servizi di manutenzione e/o assistenza su apparati contenenti dati personali (di pazienti o altri), come: stent, protesi, pacemakers, dialisi peritoneale, noleggio ausili assistenza respiratoria, noleggio sistemi per la terapia pressione negativa, prodotti che prevedono la consegna a domicilio diretta, servizio mensa per i dipendenti, servizi di archiviazione documentale)	Istituti di credito o Compagnie assicurative
Fornitori di servizi consistenti nella messa a disposizione di personale che svolge attività di trattamento di dati (mera somministrazione esclusa)	Fornitori di beni generici (cibi, bevande, ecc.), o di altri strumenti di lavoro che non prevedono alcun trattamento di dati personali
Fornitori di servizi di ristorazione (se trattano i dati dei dipendenti, ad es. per allergie o intolleranze)	Fornitori di servizi di facchinaggio o pulizie dei locali
Fornitura di servizi personalizzati per pazienti (es. materassi antidecubito, protesi, ecc.)	Fornitori di servizi di spedizione e trasporto (che non implichino l'imbustamento dei documenti)

6.1.2 Requisiti di Responsabili del Trattamento

Il Titolare, al fine di definire i requisiti del Responsabile del Trattamento, considerato che :

- il titolare rientra fra i soggetti di cui all'art. 37, par. 1, lett. a) del GDPR e che nell'ambito delle proprie attività, assegna alcuni compiti a soggetti esterni, fornitori, che nell'ambito dell'incarico conferito tratterebbero dati degli interessati di cui l'ASL è titolare;

- il rischio alto per i diritti e le libertà dei soggetti interessati di cui l'ASL è titolare (es. pazienti, dipendenti);

- sono tenuti alla designazione del RPD il titolare o il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lettere b) e c), del RGPD. Si tratta di soggetti le cui principali attività (in primis, le

attività c.d. di core business) consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. Gruppo ex art. 29, "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243 rev. 01 , paragrafi 2.1.3 e 2.1.4). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del RPD (art. 37, par. 4 del RGPD; cfr., in tal senso, ad esempio, art. 2-sexiesdecies del D. lgs. 196/2003). Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: concessionari di servizi pubblici (trasporto pubblico locale, raccolta dei rifiuti, gestione dei servizi idrici ecc.), istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle utilities (telecomunicazioni, distribuzione di energia elettrica o gas, ecc.); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento;

ritiene necessario adottare idonee misure di sicurezza e mitigazione del rischio nell'ambito della selezione di fornitori che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento a loro affidato soddisfi i requisiti del Regolamento UE 2016/679 e garantisca la tutela dei diritti dell'interessato, di seguito indicate:

- Inserire fra i requisiti di esecuzione dei contratti che i fornitori rientranti nelle categorie riportate in premessa (espresse dall'Autorità Garante compente) debbano essere dotati di Responsabile della Protezione dei Dati

- Accettazione dell'accordo per il trattamento e relativi allegati (accordo ex art. 28, addendum ADS, Valutazione del fornitore) in fase di partecipazione alle gare (dichiarazione di accettazione, in caso di aggiudicazione, da rendere in fase di partecipazione alle gare).

- Accettazione da parte dei fornitori del regolamento per la sicurezza informatica/clinica dei fornitori (a cura dell'UO informatica reti e sistemi informativi aziendali e dell'UO ingegneria clinica), (dichiarazione di accettazione, in caso di aggiudicazione, da rendere in fase di partecipazione alle gare)

- Polizza assicurativa specifica cyber/violazione dei dati in caso di aggiudicazione della gara (da valutare caso per caso in relazione al rischio elevato conseguente al servizio/prodotto contrattualizzato)

- Dettagliata descrizione del flusso delle informazioni, delle modalità, degli strumenti adottati per il trattamento e dei soggetti a vario titolo coinvolti (da valutare caso per caso in relazione al rischio elevato conseguente al servizio/prodotto contrattualizzato);

- Valutazione dei rischi derivanti dal trattamento previsto dalla gara, sottoscritta dal titolare, unitamente a parere favorevole del DPO del fornitore, dallo stesso sottoscritto (da valutare caso per caso in relazione al rischio elevato conseguente al servizio/prodotto contrattualizzato);

- Valutazione d'impatto del trattamento previsto dalla gara, sottoscritta dal titolare, unitamente a parere favorevole del DPO del fornitore, dallo stesso sottoscritto (da valutare caso per caso in relazione al rischio elevato conseguente al servizio/prodotto contrattualizzato);

6.1.3 Classificazione dei Responsabili del Trattamento

Sono identificati 2 profili possibili di Responsabili del trattamento, a fronte dei quali verranno richiesti diversi livelli di approfondimento relativamente ai requisiti in materia di misure di sicurezza da applicare al servizio.

La classificazione adottata è la seguente:

Cod.	Tipologia di RT	Utilizzo Infrastrutture
1	Fornitore Tipo 1	Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che **non utilizzano infrastrutture proprie**
2	Fornitore Tipo 2	Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che **utilizzano infrastrutture proprie**

6.1.4 Designazione

La designazione del Responsabile del Trattamento, in funzione del profilo di designazione individuato secondo i criteri di classificazione indicati nel paragrafo precedente, prevede che debba essere eseguita una valutazione delle garanzie sufficienti per la messa in atto di misure tecniche ed organizzative adeguate in maniera che il trattamento effettuato dalle terze parti soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato, come descritto in maniera analitica nella Procedura di valutazione delle misure di sicurezza del fornitore a cui si rinvia per approfondimenti.

Successivamente alla fase di valutazione, di norma in sede di sottoscrizione del contratto (protocollo di intesa, convenzione ecc...) la UOC ABS/UTE/UO procedenti, insieme al Responsabile Unico del Procedimento (RUP), predisporranno l'Accordo, per la designazione a responsabile del trattamento dei dati personali da far sottoscrivere al fornitore contestualmente alla firma del contratto, previo eventuale parere del DPO.

Per i contratti già sottoscritti, sarà premura della UOC ABS/UTE/UO procedenti, con il supporto di DPO, in collaborazione con il RUP della UOC interessata, predisporre l'Accordo sulla Protezione dei Dati, ossia l'Atto di designazione del Responsabile del Trattamento.

Per la gestione della designazione del Responsabile del Trattamento devono essere utilizzati esclusivamente i moduli predisposti e messi a disposizione, allegati alla presente procedura:

- Accordo per la designazione a responsabile del trattamento dei dati personali (fornitori che non utilizzano infrastrutture proprie) MRT1
- Accordo per la designazione a responsabile del trattamento dei dati personali (fornitori che utilizzano infrastrutture proprie) MRT2

Non devono essere accettate eventuali proposte di designazione fatte dai fornitori su propri modelli.

La designazione può, su segnalazione del soggetto designante Direttore Generale, sentiti le UO competenti e il DPO, essere corredata da ulteriori aspetti specifici riguardanti l'oggetto della fornitura (servizi o altro).

L'atto di designazione dei Responsabili del Trattamento è sottoscritto dal Direttore Generale, in qualità di titolare del trattamento, ove possibile contestualmente alla sottoscrizione del contratto con il fornitore, in ogni caso prima che il trattamento di dati personali abbia inizio.

6.1.5 Valutazione d'impatto sulla protezione dei dati

Il fornitore responsabile del trattamento deve dimostrare al titolare di aver rispettato e di rispettare le norme relative alla protezione dei dati nell'ambito delle proprie attività. Un documento di valutazione dei rischi e di valutazione d'impatto relativo a quanto previsto contrattualmente può essere ritenuto idoneo a soddisfare il requisito di affidabilità del fornitore.

La designazione, in base al trattamento di dati personali previsto dalla fornitura, può essere preceduta da una Valutazione di Impatto sulla Protezione dei Dati (c.d. DPIA o Data Protection Impact Assessment – ex art. 35-36 del Regolamento) che dovrà essere fornita dal fornitore all'Amministrazione preliminarmente alla designazione ed il cui positivo esito è propedeutico alla valutazione del fornitore da parte dell'Amministrazione.

Per i contratti in essere, o per i contratti in fase di stipula, l'esito della DPIA può contenere una gap analysis che impone al fornitore di adeguare le misure.

I criteri di determinazione della necessità di una Valutazione di Impatto DPIA sono determinati dalle seguenti indicazioni:

- linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Reg. UE 2016/679 - WP248rev.01, adottate il 4 aprile 2017 e modificate il 4 ottobre 2017;

- elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Reg. UE 2016/679 - 11 ottobre 2018.

Per l'effettuazione della DPIA, il fornitore dovrà realizzare la valutazione d'impatto del proprio servizio/prodotto secondo lo standard ISO 29134 o secondo lo standard Enisa.

6.1.6 Impegno da parte del Responsabile

L'impegno da parte del Responsabile del Trattamento è descritto nei punti previsti dal modulo di designazione:

- Ricevere Istruzioni da parte del Titolare del Trattamento (ASL) o di suoi soggetti Delegati
- Impegno alla Riservatezza
- Impegno alla Sicurezza del trattamento
- Assistenza al Titolare del Trattamento e ai suoi soggetti opportunamente Delegati

- Modalità di Conservazione, Riconsegna e Cancellazione dei Dati personali oggetto di trattamento
- Modalità di gestione di eventuali Violazioni di Dati Personali (cd. "Data Breach")
- Supporto nella Valutazione D'impatto sulla Protezione dei Dati (DPIA – Data Protection Impact Assessment)
- Designazione di Soggetti Autorizzati al Trattamento
- Designazione di Sub-responsabili del Trattamento
- Nomina e comunicazione di Amministratori di Sistema
- Eventuali ulteriori indicazioni previste dallo specifico trattamento

6.1.7 Monitoraggio del Responsabile

Il Titolare ha l'obbligo di valutare caso per caso in relazione al rischio elevato conseguente al servizio/prodotto contrattualizzato, in base anche a quanto previsto dal modulo di designazione, di monitorare l'operato dei Responsabili con particolare riguardo ai seguenti punti:

- rispetto delle istruzioni impartite dal Titolare;
- verifica della conformità dell'esecuzione dei servizi erogati rispetto a quanto stabilito nella fase preliminare di attivazione degli stessi e validati in termini di Protezione dei Dati Personali;
- essere l'interfaccia per l'organizzazione di eventuali audit;
- specificare le funzioni aziendali coinvolte nell'audit.

Il titolare si riserva la facoltà di effettuare un controllo periodico, a campione, utilizzando il modulo MAF, dal quale si evincerà l'esito positivo/negativo del controllo periodico sul RT. Qualora il controllo fosse negativo il Titolare indicherà al fornitore le necessarie misure di mitigazione alle quali il Fornitore si obbliga ad aderire nei termini che indicherà il Titolare. In caso di mancato adeguamento, la designazione sarà revocata.

6.1.8 Conclusione del rapporto e decadenza

La designazione decade alla conclusione del contratto di erogazione del servizio/fornitura.

In caso di proroga del contratto, l'accordo e la relativa designazione s'intendono prorogati per pari periodo.

6.1.9 Archiviazione dei documenti degli atti di designazione

L'atto di designazione è conservato dall'ufficio procedente ed una copia viene consegnata alla UOSD Segreteria di direzione.

6.2 Sub-Responsabili del Trattamento

Il Responsabile del trattamento si impegna a comunicare al Titolare i propri sub-responsabili.

6.3 Contitolari del Trattamento e Titolari autonomi

6.3.1 Identificazione e Classificazione

Come previsto dall'art. 28 del Regolamento, 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.

L'indicazione fornita dalla normativa prevede quindi che sia il Titolare (ASL) a determinare le finalità ed i mezzi di trattamento; qualora questi vengano determinati in maniera congiunta o autonoma si profilano le conseguenti due modalità di gestione del rapporto, rispettivamente:

- Contitolarità del Trattamento (ex art. 26 del Regolamento)
- Titolarità Autonoma del Trattamento (due distinti titolari del trattamento)

6.4 Conclusioni

Per tutto quanto non contemplato nel presente documento, si rinvia alla vigente normativa in materia di protezione dei dati personali ed al DPO che definirà con il Titolare eventuali ulteriori modalità che si rendessero necessarie per espressa previsione legislativa.

7 Allegati

Alla presente procedura sono allegati i seguenti documenti:

- MEF Elenco dei Fornitori GDPR,

- MRT 1 Accordo per la designazione del Responsabile del trattamento di tipo 1 (Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che non utilizzano infrastrutture proprie),

- Accordo per la designazione del Responsabile del Trattamento di tipo 2 (Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che utilizzano infrastrutture proprie),

- Accordo di Contitolarità ex art. 26 del GDPR,

- Check list di valutazione del fornitore GDPR,

- MAF Audit controllo periodico del RT.