

**AZIENDA U.S.L.
PESCARA**

Il giorno 10 4 APR. 2019 nella sede dell'Unità Sanitaria Locale di Pescara.

IL DIRETTORE GENERALE

Dr. Armando Mancini, nominato dalla Giunta Regionale con deliberazione n. 119 del 29/02/2016 acquisiti i pareri allegati del Direttore Amministrativo e del Direttore Sanitario, ha adottato il seguente provvedimento su proposta del Direttore della U.O.C. Affari Generali e Legali, Dott.ssa Francesca Rancitelli

N. 427

OGGETTO: Procedura per la Gestione di Accordi, Nomine e Designazioni e relativa attribuzione di responsabilità della Asl 03 Abruzzo in base a quanto previsto dal Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) – artt. 26, 28 e 29 e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali (Art. 2-quaterdecies)

IL DIRETTORE GENERALE

- Vista la relazione di cui all'Allegato A, parte integrante e sostanziale della presente deliberazione;
- Giudicata corretta e regolare l'istruttoria condotta dalla UOC AA.GG.LL. e dal Responsabile per la Protezione dei Dati Personali (D.P.O.);
- Acquisiti i pareri espressi nell'Allegato B, parte integrante e sostanziale della presente deliberazione;

DELIBERA

- 1. DI ADOTTARE ED APPROVARE** la "Procedura per la Gestione di Accordi, Nomine e Designazioni e relativa attribuzione di responsabilità della Asl 03 Abruzzo in base a quanto previsto dal Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) – artt. 26, 28 e 29 e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali (Art. 2-quaterdecies)", che si allega;
- 2. DI RASSEGNARE** copia del presente Regolamento a tutte le Unità Operative e agli Uffici della Asl di Pescara;

Il Direttore della U.O.C. Affari Generali e Legali, Dott.ssa Francesca Rancitelli, letta e condivisa la relazione del Responsabile per la Protezione dei Dati Personali;

Visti il

- REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto Legislativo n. 196/2003 come modificato dal Decreto Legislativo n. 101/2018;
- Regolamento aziendale in materia di protezione dei dati personali attuativo del Regolamento (UE) 2016/679 e del Decreto Legislativo n. 101/2018, adottato con atto deliberativo n. 1061 dell'otto ottobre 2018;

Rilevato che

Ai sensi di quanto disposto dagli artt. 26, 28 e 29 del Regolamento (UE) 2016/679 e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali (Art. 2-quaterdecies), la Asl di Pescara con la presente Procedura si pone l'obiettivo di fornire una descrizione generale del processo di gestione degli Accordi, Nomine e Designazioni e delle relative indicazioni operative al fine di poter consentire alla Direzione Generale ed alle Unità Operative di poter procedere con le azioni di propria competenza.

Vista

La proposta di procedura relativa alla gestione degli Accordi, Nomine e Designazioni, allegata al presente provvedimento di cui ne costituisce parte integrante e sostanziale, redatta dal Responsabile per la Protezione dei dati (D.P.O.), in cui sono previste le modalità operative;

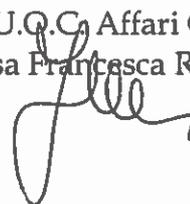
propone

1. **DI ADOTTARE ED APPROVARE** la "Procedura per la Gestione di Accordi, Nomine e Designazioni e relativa attribuzione di responsabilità della Asl 03 Abruzzo in base a quanto previsto dal Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) - artt. 26, 28 e 29 e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali (Art. 2-quaterdecies)", che si allega;
2. **DI RASSEGNARE** copia del presente Regolamento a tutte le Unità Operative e agli Uffici della Asl di Pescara;

Pescara, 02/04/2019

Il Responsabile per la Protezione
dei dati Personali
Dott. Giovanni Modesti

Il Direttore U.O.C. Affari Generali e Legali
Dott.ssa Francesca Rancitelli



Procedura per la Gestione di Accordi, Nomine e Designazioni

e relativa attribuzione di responsabilità

della Asl 03 Abruzzo

in base a quanto previsto dal

**Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) – artt. 26, 28 e 29 e
dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali (Art. 2-
quaterdecies)**

Sommario

1	Introduzione.....	4
2	Scopo.....	4
3	Campo di Applicazione.....	4
4	Definizioni.....	5
5	Normativa di Riferimento.....	7
5.1	Normativa di riferimento per la designazione di Responsabili del Trattamento.....	7
5.1.1	Articolo 28 Responsabile del trattamento.....	7
5.2	Normativa di riferimento per i Trattamenti sotto l'autorità del Titolare o del Responsabile del Trattamento.....	9
5.2.1	Articolo 29 – Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento.....	9
5.2.2	Art. 2-quaterdecies – Attribuzione di funzioni e compiti a soggetti designati.....	9
5.3	Normativa di riferimento per gli Accordi di Contitolarità.....	9
5.3.1	Articolo 26 Contitolari del trattamento.....	9
6	Premesse.....	10
6.1	Generalità.....	10
6.2	Struttura organizzativa dell'Azienda Sanitaria.....	10
6.3	Approccio metodologico agli accordi, nomine e designazioni.....	10
7	Descrizione del Processo.....	12
7.1	Soggetti Autorizzati al Trattamento con Delega.....	12
7.1.1	Identificazione.....	12
7.1.2	Designazione.....	12
7.1.3	Revoca.....	12
7.1.4	Archiviazione degli atti.....	13
7.2	Soggetti Autorizzati al Trattamento.....	13
7.2.1	Identificazione.....	13
7.2.2	Designazione.....	13
7.2.3	Revoca.....	13
7.2.4	Archiviazione degli atti.....	14
7.2.5	Gestione operativa.....	14
7.3	Responsabili del Trattamento.....	14
7.3.1	Identificazione e Classificazione.....	14
7.3.2	Designazione.....	15

7.3.3	Impegno da parte del Responsabile.....	16
7.3.4	Monitoraggio del Responsabile.....	16
7.3.5	Conclusione del rapporto e revoca.....	16
7.3.6	Archiviazione dei documenti degli atti di designazione.....	16
7.3.7	Unità Operative abilitate alla designazione.....	16
7.3.8	Processo di designazione e ratifica.....	17
7.4	Sub-Responsabili del Trattamento.....	17
7.5	Contitolari del Trattamento.....	17
7.5.1	Identificazione e Classificazione.....	17
7.5.2	Stipula dell'Accordo.....	17
7.5.3	Conclusione del rapporto e revoca.....	17
7.5.4	Archiviazione dei documenti degli atti di designazione.....	18
7.6	Conclusioni.....	18
8	Allegati.....	18

1 Introduzione

La normativa vigente in termini di Protezione dei Dati Personali, costituita dal Regolamento UE 679/2016 – 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.

La ASL n.03 di Pescara (di seguito anche la “ASL”) predispone il presente documento nell’ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati.

2 Scopo

Il presente documento descrive le modalità operative adottate dalla ASL n.03 di Pescara, per il rispetto di quanto previsto dagli artt. 26, 28 e 29 del Regolamento e dall’art. 2-quaterdecies del D.Lgs. 196/03 – Codice in materia di Protezione dei Dati Personali – come modificato dal D. Lgs. 101/2018 riguardanti le modalità di definizione delle nomine e designazioni, nonché delle modalità di gestione degli accordi contitolarità.

L’obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle Nomine e Designazioni e delle relative indicazioni operative al fine di poter consentire alla Direzione Generale ed alle Unità Operative di poter procedere con le azioni di propria competenza.

3 Campo di Applicazione

Il presente documento regola il processo di gestione delle nomine e designazioni nelle varie casistiche che possano presentarsi nelle strutture amministrative, ospedaliere e territoriali della ASL di Pescara.

4 Definizioni

Le seguenti definizioni sono di utilità per poter dare le risposte opportune nell'ambito del questionario in base all'art. 4 del Regolamento:

«**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;

«**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;

«**SAT**»: Soggetto Autorizzato al Trattamento dei dati personali

«SATD»: Soggetto Autorizzato al Trattamento dei dati personali con Delega

«RT»: Responsabile del Trattamento dei dati personali

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

«UOC»: Unità Operativa Complessa

«UOSD»: Unità Operativa Semplice Dipartimentale

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 gestione delle nomine per gli autorizzati interni alla struttura del titolare;
- normativa di riferimento per la gestione delle designazioni ed accordi per gli autorizzati esterni alla struttura del titolare.

Alla normativa principale (Regolamento UE 679/2016) sono aggiunti i riferimenti relativi alla normativa nazionale in materia di protezione dei dati personali applicabile al contesto della presente procedura (D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018) al fine di poter rendere il presente documento comprensivo delle normative menzionate.

5.1 Normativa di riferimento per la designazione di Responsabili 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.

5.1.1 Articolo 28 - Responsabile del trattamento

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; e
- 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. La Commissione 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 sotto l'autorità del Titolare o del Responsabile del Trattamento

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

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

5.2.1 Articolo 29 – Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, 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.

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

1. Il titolare o il responsabile 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. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

5.3 Normativa di riferimento per gli Accordi di Contitolarità

5.3.1 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 Premesse

6.1 Generalità

Il vigente Regolamento UE n. 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, "Regolamento"), stabilisce che la designazione dei Responsabili, da parte del titolare del trattamento, attiene a soggetti esterni all'organizzazione dello stesso titolare.

Di fatto, a decorrere dal 25 maggio 2018 le figure relative ai responsabili interni del trattamento e agli incaricati del trattamento, anch'essi interni alla organizzazione del titolare, hanno cessato di esistere in quanto non più previste dal vigente Regolamento.

Questa situazione rappresentava un vulnus, soprattutto, per le organizzazioni più complesse ed articolate (quali le Asl) in quanto privava il titolare del trattamento della possibilità di designare soggetti preposti a tutelare specifici ambiti del trattamento.

Per tale ragione, al fine di consentire la definizione di un organigramma aziendale privacy all'interno delle organizzazioni più complesse, il Decreto Legislativo n. 101/2018 - che ha adeguato il Codice in materia di protezione dei dati personali (decreto legislativo n. 196/2003) alle disposizioni contenute nel Regolamento - ha previsto che il Titolare del trattamento può ricorrere alla attribuzione di funzioni e compiti a soggetti designati.

Nello specifico, l'*art. 2 - quaterdecies* stabilisce che il titolare o il responsabile del trattamento possono prevedere che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

Per questa ragione il Titolare del trattamento (id est, la Asl) ha deciso di provvedere alla designazione dei Soggetti Autorizzati al Trattamento dei Dati personali con Delega (SATD), la cui figura sostanzialmente coincide - almeno in parte - con quella del responsabile interno del trattamento (ex d.lgs. n. 196/2003, pre-Regolamento UE). Nell'ambito dell'organizzazione identificata, tali Soggetti delegati, in base a quanto specificato nei modelli di designazione in allegato al presente documento, hanno il compito di nominare i Soggetti Autorizzati al Trattamento (SAT) sotto la propria responsabilità.

6.2 Struttura organizzativa dell'Azienda Sanitaria

Su tale argomento si richiama quanto delineato attraverso l'Atto Aziendale recepito con Delibera n. 220 del 02.03.2018

6.3 Approccio metodologico agli accordi, nomine e designazioni

Per dare una visione generale dell'organizzazione aziendale per il Trattamento dei Dati Personali, di seguito viene proposta una versione grafica Organigramma Aziendale Privacy:

7 Descrizione del Processo

Di seguito verranno indicate le modalità di gestione delle designazioni e delle revoche per le seguenti tipologie di figure privacy:

- Soggetti Autorizzati al Trattamento con Delega (SATD)
- Soggetti Autorizzati al Trattamento (SAT)
- Responsabili del Trattamento (RT)
- Sub-Responsabili del Trattamento (SRT)
- Contitolari e Titolari autonomi del trattamento

7.1 Soggetti Autorizzati al Trattamento con Delega

7.1.1 Identificazione

Mutuando quanto previsto dal Regolamento UE in merito all'identificazione dei responsabili del trattamento, il titolare ricorre unicamente a soggetti 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 delle normativa vigente in materia e garantisca la tutela dei diritti dell'interessato.

Il ruolo di Soggetto Autorizzato al Trattamento con Delega (SATD) viene identificato nel ruolo di Direttore di UOC (Unità Operativa Complessa) e di UOSD (Unità Operativa Semplice Dipartimentale), considerando il ruolo di Direttore di tali strutture una condizione preliminare ed essenziale per la designazione a SATD. La delega non potrà quindi essere assegnata a figure che ricoprano un ruolo diverso salvo che in alcuni specifici casi da determinare da parte dell'Ufficio Privacy con il supporto del Responsabile della Protezione dei Dati.

7.1.2 Designazione

Per la designazione a Soggetto Autorizzato al Trattamento con Delega deve essere utilizzato l'apposito modello allegato alla presente procedura (all. n. 01), e sottoscritto dal Direttore Generale.

Le modalità di designazione sono le seguenti:

- Il modello viene predisposto dall'Ufficio Privacy ed è trasmesso all'attenzione del Direttore Generale per la firma;
- Firmato il documento, l'Ufficio Privacy si occupa di attribuire un numero di registrazione interno di identificazione della pratica, acquisire il numero di protocollo generale, trasmettere il documento al destinatario e curare la successiva firma per accettazione dell'atto di designazione;
- L'originale dell'atto viene conservato dal Soggetto Autorizzato al Trattamento con Delega che si impegnerà a trasmetterne copia all'Ufficio Privacy.
- Ricevuta la copia, l'Ufficio Privacy provvede ad archiviare il documento in opportuno archivio dedicato.

7.1.3 Revoca

La revoca della designazione deve essere effettuata mediante atto formale sottoscritto da parte del Direttore Generale. L'atto deve specificare se la responsabilità dei trattamenti attribuiti al SATD di cui si sta procedendo alla revoca venga contestualmente attribuita ad altro SATD o se il Titolare intenda avocare a sé tale delega.

Le modalità di revoca della designazione sono le seguenti:

- Sono predisposte due copie originali dell'atto da parte dell'Ufficio Privacy che vengono successivamente trasmesse all'attenzione del Direttore Generale per la firma;
- Firmati i documenti, l'Ufficio Privacy si occupa di attribuire ad essi un numero di registrazione interno di identificazione della pratica, acquisire il numero di protocollo generale, trasmettere i documenti al destinatario e curare la successiva firma per ricezione;
- Una copia originale dell'atto viene conservata dal revocando Soggetto Autorizzato al Trattamento con Delega che si impegnerà a trasmettere l'altro originale, debitamente sottoscritto, all'Ufficio Privacy.
- Ricevuta la propria copia originale dell'atto, l'Ufficio Privacy provvede ad archiviare il documento in opportuno archivio dedicato.

7.1.4 Archiviazione degli atti

L'archiviazione di copia degli Atti di Designazione dei Soggetti Autorizzati al Trattamento con Delega e delle eventuali revoche viene effettuata da parte dell'Ufficio Privacy.

Ogni Soggetto Autorizzato al Trattamento con Delega si impegna a conservare in opportuno archivio riservato le proprie copie originali degli atti.

7.2 Soggetti Autorizzati al Trattamento

Con la seguente Procedura si intende fornire ai SATD le istruzioni necessarie al fine di consentir loro di ricorrere alla designazione dei Soggetti Autorizzati al Trattamento (di seguito, "SAT").

7.2.1 Identificazione

Premesso che la designazione può avere ad oggetto solo persone fisiche, nello specifico trattasi di tutti i collaboratori del SATD che compiono attività di trattamento, l'elenco dei soggetti designati comprenderà, letteralmente, tutti i dipendenti assegnati alla UOC diretta dal SATD.

7.2.2 Designazione

La designazione, nominativa e personale, dovrà essere predisposta in due copie originali e recare la firma del SATD e del SAT (per ricezione); l'atto dovrà essere redatto utilizzando il Modello che si allega alla presente procedura (all. n. 02), debitamente protocollato.

A valle della designazione del Soggetto Autorizzato al Trattamento, il SATD deve predisporre ed aggiornare l'elenco dei SAT sotto la propria responsabilità; l'aggiornamento va compiuto ogni qual volta si proceda ad una nuova designazione.

7.2.3 Revoca

La revoca, nominativa e personale, dovrà essere predisposta in due copie originali e recare la firma del SATD e del SAT (per ricezione); l'atto dovrà essere debitamente protocollato.

A valle della revoca della designazione del Soggetto Autorizzato al Trattamento, il SATD deve aggiornare l'elenco dei SAT sotto la propria responsabilità; l'aggiornamento va compiuto ogni qual volta si proceda ad una cessazione di un SAT (a seguito di quiescenza, trasferimento, altro).

In caso di cessazione del rapporto di lavoro del SAT, a qualunque titolo, l'evento dovrà essere annotato sull'elenco dei SAT al fine di indicare la revoca della designazione.

7.2.4 Archiviazione degli atti

L'originale degli atti, una volta firmati da entrambi i soggetti (SATD e SAT) dovranno essere conservati a cura del SATD designante in un proprio archivio opportunamente protetto.

7.2.5 Gestione operativa

I Soggetti Autorizzati al Trattamento con Delega (SATD), una volta designati i Soggetti Autorizzati, dovranno assicurarsi che gli stessi siano:

1. inseriti in un percorso di formazione aziendale in materia di protezione dei dati personali;
2. forniti di credenziali di autenticazione, ed al contempo, in caso di revoca della designazione, tali credenziali siano ritirate; questo adempimento va espletato servendosi del supporto tecnico dell'UOSD Sistemi Informativi.

7.2.5.1 Elenco dei SAT

Una volta designato il SAT, il Soggetto Autorizzato al Trattamento con Delega dovrà registrare gli estremi dei Soggetti Autorizzati su un "Elenco dei SAT" contenente i seguenti campi:

- a) nome e cognome del SAT;
- b) numero di matricola;
- c) gestionale/i a cui è autorizzato l'accesso;
- d) partecipazione a corsi di formazione sulla Privacy (con indicazione della data e dell'oggetto);
- e) data di decorrenza della nomina (coincidente con la data apposta dal SAT a fianco alla propria firma);
- f) data di cessazione della nomina.

Può verificarsi il caso che lo stesso dipendente venga nominato in qualità di SAT da più SATD (cioè da più Direttori di UOC/UOSD); tale fattispecie si verifica quando un dipendente risulta assegnato contemporaneamente a più Unità Operative; in questo caso ciascun SATD che procederà alla nomina avrà un ambito di responsabilità in merito agli obblighi del SAT limitato al trattamento – da parte di questi – dei dati personali afferenti alla propria UO.

7.3 Responsabili del Trattamento

7.3.1 Identificazione e Classificazione

Come indicato 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 Regolamento e garantisca la tutela dei diritti dell'interessato.

7.3.1.1 Classificazione dei Responsabili del Trattamento

Sono identificati tre 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:

1. Designazione di Responsabile del Trattamento per Professionisti che erogano servizi presso le strutture dell'Azienda e che non utilizzano infrastrutture proprie

2. Designazione di Responsabile del Trattamento per Società/Organizzazioni che erogano servizi presso le strutture o per conto dell'Azienda e che utilizzano infrastrutture proprie di bassa o media complessità
3. Designazione di Responsabile del Trattamento per Società/Organizzazioni che erogano servizi presso le strutture o per conto dell'Azienda e che utilizzano infrastrutture ad alta complessità

7.3.2 Designazione

In funzione del profilo di designazione, individuato secondo i criteri di classificazione indicati nel paragrafo precedente, tenendo in considerazione che la normativa prevede una previa 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, è necessario sottoporre al fornitore, in via preliminare, gli allegati al modulo di designazione in qualità di Responsabile del Trattamento in maniera da poter raccogliere le necessarie informazioni per l'effettuazione della valutazione richiesta.

Tale operazione, unitamente alla formalizzazione della designazione, deve essere effettuata preliminarmente alla sottoscrizione del contratto di fornitura al fine di poter garantire un corretto trattamento di dati personali da parte del fornitore.

Per la gestione della designazione del Responsabile del Trattamento devono essere osservati i seguenti punti:

- Per la designazione dei Responsabili del Trattamento (ex. Art. 28 del Regolamento) devono essere utilizzati esclusivamente i moduli predisposti e messi a disposizione dall'Ufficio Privacy;
- Non devono essere accettate eventuali proposte di designazione fatte dai fornitori su propri modelli; tali proposte dovranno però essere tenute in considerazione nel caso in cui contengano alcune specificità da prevedere all'interno dei moduli di designazione predisposti dall'Ufficio Privacy.
- La designazione può, su segnalazione del soggetto designante (SATD o Direttore Generale), essere corredata da ulteriori aspetti specifici riguardanti l'oggetto della fornitura (servizi o altro)
- 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, nel caso sia richiesta, deve essere svolta preliminarmente alla designazione ed il cui positivo esito è propedeutico alla valutazione del fornitore da parte dell'Amministrazione. I criteri di determinazione della necessità di una Valutazione di Impatto DPIA sono determinati dalle seguenti indicazioni normative:
 - 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 regolamento 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 Regolamento (UE) n. 2016/679 - 11 ottobre 2018;
- Per l'effettuazione della Valutazione di Impatto DPIA, il fornitore deve fornire tutti gli elementi necessari alla valutazione da parte dell'Azienda; tale valutazione dovrà essere fatta dall'Ufficio Privacy con il supporto delle UO competenti e la validazione da parte del Responsabile della Protezione dei Dati aziendale (Data Protection Officer – DPO);
- La designazione deve avvenire contestualmente alla sottoscrizione del contratto di fornitura dei servizi al fine di poter garantire la protezione dei dati personali fin dall'attivazione del contratto stesso.

7.3.3 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 opportunamente Delegati
- Impegno alla Riservatezza
- Impegno alla Sicurezza del trattamento
- Assistenza al Titolare del Trattamento e di suoi soggetti opportunamente Delegati (SATD)
- 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 (SAT)
- Designazione di Sub-responsabili del Trattamento
- Nomina e comunicazione di Amministratori di Sistema
- Eventuali ulteriori indicazioni previste dallo specifico trattamento

7.3.4 Monitoraggio del Responsabile

Il soggetto designante ha l'obbligo, in base 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.

7.3.5 Conclusione del rapporto e revoca

La designazione è automaticamente revocata alla conclusione del contratto di erogazione del servizio/fornitura.

7.3.6 Archiviazione dei documenti degli atti di designazione

Il soggetto designante ha l'obbligo di conservazione del modulo di designazione originale che dovrà essere allegato al contratto di fornitura e la cui copia dovrà essere inviata, per opportuna archiviazione, all'Ufficio Privacy.

Il soggetto designante dovrà inserire il Responsabile designato all'interno del Registro dei Responsabili del Trattamento, con relativi estremi della designazione e delle scadenze previste dal registro stesso.

7.3.7 Unità Operative abilitate alla designazione

La designazione dei Responsabili del Trattamento può essere effettuata direttamente dal Titolare del Trattamento (nella persona del Direttore Generale) o dai Direttori delle seguenti Unità Operative (in base alle rispettive competenze)

7.3.8 Processo di designazione e ratifica

Il processo di designazione, viene effettuato a valle del processo di selezione del fornitore o della terza parte che erogherà servizi/effettuerà trattamenti per conto dell'Azienda; in fase di sottoscrizione del contratto/convenzione, in allegato dovrà essere apposto il modello di designazione.

La validità della designazione sarà subordinata alla sottoscrizione del contratto/convenzione da parte della Direzione Generale (in qualità di Titolare del Trattamento).

7.4 Sub-Responsabili del Trattamento

Il soggetto designante il Responsabile del Trattamento (RT), in virtù di quanto disposto dall'art. 28.2 del Regolamento, si occupa di raccogliere e valutare, con il supporto dell'Ufficio Privacy e del Responsabile della Protezione dei Dati, le designazioni dei Sub-Responsabili del Trattamento da parte dell'RT designato. Potranno essere valutabili anche atti di designazione già effettuati dal Responsabile (in qualità di Titolare) verso i propri Responsabili.

Qualora tali atti vengano giudicati positivamente, si potrà procedere con la validazione dei Sub-Responsabili; in alternativa, le designazioni effettuate dovranno essere integrate con le dovute osservazioni pervenute dai valutatori.

7.5 Contitolari del Trattamento e Titolari autonomi

7.5.1 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) che determini 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)

7.5.2 Stipula dell'Accordo

Prima dell'avvio del rapporto contrattuale/convenzionale è necessario stabilire un accordo che tuteli i diritti degli interessati e garantisca ambo le parti del rispetto dei principi di trattamento.

Le modalità di stipula dell'accordo ed i relativi contenuti sono da valutare di volta in volta in base alla specifica situazione: tale valutazione deve essere effettuata con il supporto dell'Ufficio Privacy e del Responsabile della Protezione dei Dati.

7.5.3 Conclusione del rapporto e revoca

L'accordo è automaticamente revocato decorsi i termini di scadenza dello stesso. Eventuali proroghe devono essere esplicitamente sottoscritte dalle parti.

7.5.4 Archiviazione dei documenti degli atti istituenti il rapporto

L'Ufficio Privacy riceverà copia dell'accordo firmato dalle parti ed opportunamente protocollato per propria archiviazione e registrazione.

7.6 Conclusioni

Per tutto quanto non contemplato in questa Procedura si rinvia alla vigente normativa di settore in materia di protezione dei dati personali.

In caso di dubbi contattare il responsabile per la Protezione dei dati Personali, per il tramite dell'Ufficio Privacy (ai seguenti recapiti: tel.; email – Ufficio Privacy:)

8 Allegati

Alla presente procedura sono allegati i seguenti documenti:

- Allegato 1 – Modulo di nomina per Soggetto Autorizzato al Trattamento dei dati con Delega (SATD)
- Allegato 2 – Modulo di nomina per Soggetto Autorizzato al Trattamento dei dati (SAT)
- Allegato 3 – Modulo di designazione per Responsabile del Trattamento (Caso 1 – Professionisti)
- Allegato 4 – Modulo di designazione per Responsabile del Trattamento (Caso 2 – Servizi Non Tecnologici/Complessi)
- Allegato 5 – Modulo di designazione per Responsabile del Trattamento (Caso 3 – Servizi Tecnologici/Complessi)



www.ausl.pe.it

Regione Abruzzo

ASL 03 Pescara

Regolamento Aziendale
Privacy – Allegato 5

**LETTERA DI NOMINA AL SOGGETTO AUTORIZZATO
CON DELEGA AL TRATTAMENTO DEI DATI
PERSONALI**

Artt. 28 e 29 Regolamento UE 679/2016,

Art. 2-quaterdecies D. Lgs. 196/2003 (come modificato dal D.
Lgs. 101/2018)

Rev. 02/2018

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530982

IL TITOLARE

Prot. n. _____/

Pescara, li _____

Preg.mo Dr./Dr.ssa _____

Ruolo: _____

UO _____

Posta Elettronica _____

Oggetto: Lettera di Nomina a Soggetto Autorizzato al Trattamento dei dati personali con Delega (SATD) ai sensi degli Artt. 28 e 29 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation), dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore.

Il sottoscritto Dott. Armando Mancini in qualità di rappresentante legale della ASL di Pescara – Titolare del trattamento dei dati personali - considerato che:

- a) La ASL di Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;
- b) La nomina a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;

- c) L'equivalente funzione, per soggetti alle dipendenze della struttura del Titolare, viene assegnata a Soggetti Autorizzati al Trattamento di dati personali con Delega (SATD), ai sensi degli artt. 28 e 29 del Regolamento UE 679/2016 e dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018);
- d) La presente nomina integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di Pescara e sul Soggetto Autorizzato al Trattamento di dati personali con Delega (di seguito "SATD" o "Delegato") derivanti dall'esecuzione degli incarichi organizzativi tra la ASL di Pescara (di seguito "ASL") e il Delegato;

con il presente atto nomina

ai sensi degli artt. 28 e 29 del Reg. UE 679/2016 e

dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018)

Soggetto Autorizzato al Trattamento di dati personali con Delega (SATD)

Il/la Dr./Dr.ssa _____

per i dati trattati dall'Unità Operativa _____

La presente nomina si applica a tutte le attività svolte dal Delegato nell'ambito del trattamento dei dati personali ai sensi del Regolamento UE 679/2016 (di seguito "Regolamento" o "GDPR"), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito "Codice" – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore, ivi comprese le attività svolte dai soggetti autorizzati al trattamento o terze parti (es.: fornitori), nominate dal Delegato, che trattino dati di Terzi Interessati.

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

- 1) Il presente Atto si applica al trattamento dei dati personali svolto dal Delegato in qualità di Soggetto Autorizzato al Trattamento di dati personali con Delega per conto della ASL, quale titolare del trattamento ("Titolare del Trattamento"), ai sensi della presente nomina e definisce gli obblighi del Delegato in materia di tutela dei dati personali.
- 2) L'ambito del trattamento è definito da tutti i trattamenti di dati personali effettuati dall'UO da Lei diretta e riportati nell'Allegato al presente Atto di Nomina; qualora dovessero risultare ulteriori trattamenti attribuiti all'UO da Lei diretta, verrà prontamente aggiornato l'allegato alla presente nomina;
- 3) Natura e finalità del trattamento: il Delegato tratta i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte dall'Unità Operativa da Lui diretta. Le attività di trattamento sono correlate allo svolgimento delle Sue funzioni (Contratto di Lavoro).
- 4) Il Delegato è responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali e delle istruzioni impartite dal Titolare.
- 5) Nel presente documento, ove venga richiesta la comunicazione al Titolare del Trattamento, detta comunicazione si intende da effettuarsi all'Ufficio Privacy del Titolare (ufficio.privacy@ausl.pe.it).
- 6) Nell'Ambito di Trattamento definito, sarà compito del Delegato fare in modo che i dati personali, trattati dalla propria UO, siano:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Articolo 2 – Tipologie di dati personali e categorie di interessati

- 1) I soggetti i cui dati personali sono oggetto del trattamento da parte del Delegato ai sensi del presente Atto possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL, terzi incaricati, a qualunque titolo, dalla ASL, pazienti, controparti contrattuali della ASL e, in generale, terze parti rispetto alle quali la ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore. I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

Articolo 3 – Istruzioni

- 1) Il Delegato effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta. Il presente Atto e la Sua designazione costituiscono parte delle istruzioni della ASL per il trattamento dei dati personali da parte del Delegato che potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.
- 2) Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto dal presente Atto deve essere fornita dalla ASL al Delegato per iscritto (es. Procedure operative, ecc...) per mezzo dei canali di comunicazione istituzionali (ad es.: posta elettronica ordinaria).
- 3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Materiale didattico per la formazione e tutto quanto attinente alla materia pubblicato sul sito aziendale nella sezione Privacy.
- 4) È fatto obbligo al Delegato di:
 - a) nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 29 del Reg. UE 679/2016 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;

- b) redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e verificare annualmente l'ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell'assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);
- c) controllare le operazioni di trattamento svolte dagli autorizzati e la conformità all'ambito di trattamento consentito;
- d) attuare gli obblighi di informazione (Informativa ex Artt. 13-14 del Regolamento) ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- e) comunicare immediatamente al titolare non oltre le 12 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria
- f) ove competente (ved. Art. 6) nominare i Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 679/2016, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- g) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti.

Articolo 4 – Riservatezza

- 1) Il Delegato si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
- 2) Il Delegato garantisce che i soggetti, da lui nominati quali autorizzati al trattamento dei dati personali (Soggetti Autorizzati al Trattamento dei dati personali o SAT), si siano impegnati per iscritto a mantenere la riservatezza dei dati e sono soggetti a tale obbligo.

Articolo 5 – Sicurezza del trattamento

- 1) Il Delegato si impegna ad adottare le misure richieste dall'Art. 32 del GDPR e le procedure in materia stabilite dal Titolare.
- 2) In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati - il Delegato si impegna:
 - a) Nei contratti di fornitura di prodotti e servizi in corso di esecuzione, aventi ad oggetto il trattamento di dati personali, con il supporto - se del caso - della UOSD Sistemi Informativi e/o della UOC Ingegneria Clinica, a verificare l'attuazione delle misure tecniche e organizzative, da parte del fornitore, così come comunicate dallo stesso negli allegati al modello di nomina a Responsabile del Trattamento. Ove competente, il Delegato deve garantire l'adeguata compilazione da parte del fornitore del sopracitato allegato relativo alle modalità di implementazione delle misure richieste (ved. Art. 6);
 - b) Nei contratti di fornitura di prodotti e servizi da stipulare, aventi ad oggetto il trattamento di dati personali, con il supporto - se del caso - della UOSD Sistemi Informativi e/o della UOC Ingegneria Clinica, a garantire che nei requisiti richiesti al fornitore siano previste le misure tecniche e organizzative indicate negli allegati al modello di nomina a Responsabile del Trattamento e a verificarne l'effettiva attuazione. Ove competente, il Delegato deve garantire l'adeguata compilazione da parte del fornitore del sopracitato allegato relativo alle modalità di implementazione delle misure richieste (ved. Art. 6);

- 3) Qualora il Delegato intendesse apportare modifiche alle misure tecniche e organizzative adottate dal Titolare, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione al Titolare per la necessaria autorizzazione.

Articolo 6 – Responsabili del Trattamento

- 1) Per l'esecuzione di specifiche attività per conto del Titolare, il Delegato potrà avvalersi di Responsabili del trattamento esterni all'organizzazione del Titolare – ASL – (ciascuno un "Responsabile del Trattamento") ai sensi del GDPR. I Responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti dal Delegato ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Delegato nominerà Responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto tra il Titolare del trattamento e il Delegato, 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 e della normativa vigente in materia. **Qualora il Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Delegato è tenuto a rilevarne gli inadempimenti nell'ambito delle attività di controllo a lui affidate con obbligo di comunicazione tempestiva (entro 12 ore) al Titolare. Il Delegato conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'inadempimento degli obblighi del Responsabile nei seguenti due casi:**
- a) **Controllo inadeguato (es.: mancato controllo, controllo non sistematico o non esaustivo);**
- b) **Rilevazione di inadempimenti e loro mancata comunicazione tempestiva al Titolare.**
- 2) Il nominativo del singolo Responsabile del Trattamento che il Delegato intenda designare per l'esecuzione di attività di trattamento dei dati, riguardanti le attività istituzionali svolte dall'Unità Operativa dal lui diretta, dovrà essere previamente comunicato al Titolare per la necessaria autorizzazione.
- 3) Il Delegato, a valle dell'autorizzazione del Titolare di cui al punto precedente, si impegna a:
- a) Nel caso di fornitura di servizi che prevedano per la loro esecuzione in maniera totale o parziale il ricorso a sistemi informatici e/o tecnologici, assicurarsi che i dirigenti dell'UOSD Sistemi Informativi e/o della UOC Ingegneria Clinica (in base alle rispettive competenze) procedano alla nomina del fornitore quale Responsabile del Trattamento di dati personali, sulla base di quanto previsto dalla procedura di assegnazione del servizio, assolvendo (da parte dei sopraccitati dirigenti) a tutti gli obblighi previsti dalla lettera di Nomina del Responsabile. In questo caso il Delegato ha il compito di garantire in maniera continuativa il rispetto delle istruzioni impartite al Responsabile e relazionare periodicamente, in forma scritta, in merito alla corretta esecuzione del servizio, per la parte di propria competenza (operativa), al dirigente del servizio tecnologico che ha effettuato la nomina del fornitore (UOSD Sistemi Informativi o UOC Ingegneria Clinica). La periodicità di relazione da parte dei soggetti delegati è stabilita in un anno, con scadenza annuale fissata al 15 dicembre; in caso di variazioni nelle forniture di servizi (a titolo esemplificativo e non esaustivo, nei casi di rinnovo contrattuale, variazione del fornitore, variazione dei requisiti/modalità di esecuzione o strumenti per l'erogazione del servizio) dovranno essere effettuate relazioni specifiche entro 30 giorni dall'avvio dell'esecuzione operativa delle variazioni previste. L'individuazione dei compiti e responsabilità, relativi alla protezione dei dati personali, tra i servizi tecnologici e l'UO

richiedente, dovrà essere esaminata caso per caso con l'ausilio del Responsabile della Protezione dei Dati (RPD);

- b) Negli altri casi (acquisizione di servizi che non prevedano la fornitura/utilizzo di sistemi informatici e/o tecnologici), nominare direttamente il Responsabile del Trattamento sulla base di quanto previsto dalla procedura di assegnazione del servizio (capitolato, contratto, scheda tecnica, ecc...), assolvendo a tutti gli obblighi previsti dalla procedura di Nomina del Responsabile (fare riferimento allo specifico modello di nomina). L'individuazione dei compiti e responsabilità, relativi alla protezione dei dati personali, in capo al fornitore/Responsabile, con conseguenti oneri di controllo da parte del Delegato, dovrà essere esaminata caso per caso con l'ausilio del Responsabile della Protezione dei Dati (RPD);
- 4) Il Delegato si impegna a informare anticipatamente il Titolare e il Responsabile della Protezione dei Dati, con mezzi elettronici (e-mail e/o PEC), laddove il Responsabile intenda, per l'erogazione dei servizi e/o delle forniture, avvalersi e, di conseguenza, nominare, sostituire o cessare il rapporto con un Sub-responsabile del Trattamento che agisca in nome e per conto del Responsabile. La nomina, sostituzione o cessazione si intenderà accettata dal Titolare esclusivamente a seguito di formale positivo riscontro.
- 5) Qualora il Titolare sollevi obiezioni su uno o più Responsabili o sub-responsabili del Trattamento, egli darà indicazioni al Delegato sulle relative motivazioni. In tal caso, il Delegato potrà:
- a) proporre altro Responsabile/Sub-responsabile del Trattamento in sostituzione del Responsabile/Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni;
o
b) adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
- 6) **Il Delegato è responsabile, in base ai compiti e responsabilità attribuitegli, nei confronti del Titolare per l'assolvimento da parte del/i Responsabile/i e del/i Sub-responsabile/i del Trattamento degli adempimenti previsti dal Regolamento, dalle normative vigenti in materia, delle istruzioni impartite (ved. Art. 3).**
- 7) Nel caso in cui il Delegato abbia necessità di ricorrere a un Responsabile o un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Delegato dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Delegato dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR e delle normative vigenti in materia, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

Articolo 7 – Assistenza

- 1) Tenendo conto della natura del trattamento dei dati personali svolto dal Delegato, come descritto nel Registro dei Trattamenti, questi si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative al fine di adempiere al proprio obbligo di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 22 del GDPR.
- 2) Il Delegato dovrà informare il Titolare ed il Responsabile della Protezione dei Dati, senza ingiustificato ritardo, laddove un Terzo Interessato eserciti uno dei diritti di cui agli Artt. da 12 a 22 del GDPR riguardanti i propri dati personali, con particolare riferimento, a titolo esemplificativo e ove applicabile, al diritto di accesso, al diritto di chiedere la rettifica e cancellazione (c.d. "diritto all'oblio"), al diritto di limitarne il trattamento o di opporvisi, al

diritto alla "portabilità", al diritto di opporsi a una decisione basata unicamente sul trattamento automatizzato ai sensi dell'Art. 22 del GDPR.

- 3) Tenendo conto della natura del trattamento come descritto nel Registro dei Trattamenti e nel presente Atto e delle informazioni di volta in volta messe a disposizione, il Delegato si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR.

Articolo 8 – Cancellazione

- 1) I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Delegato, nell'ambito dell'esecuzione delle attività previste dalle funzioni istituzionali assegnategli, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine previsto dal Registro Aziendale dei Trattamenti.

Articolo 9 – Violazioni di Dati Personali (cd. "Data Breach")

- 1) Il Delegato si impegna ad informare immediatamente il Titolare ed il Responsabile della Protezione dei Dati, senza ingiustificato ritardo e comunque entro e non oltre 6 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti 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.
- 2) Il Delegato si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a propria disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
- 3) La comunicazione dovrà avvenire a mezzo mail rispettivamente agli indirizzi info.urp@ausl.pe.it e dpo@ausl.pe.it.

Articolo 10 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

- 1) Il Delegato si impegna, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

Articolo 11 – Soggetti Autorizzati al Trattamento

- 1) Fatto salvo quanto previsto all'articolo 6, il Delegato garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai Soggetti Autorizzati al Trattamento, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

- 2) Il Delegato si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.
- 3) Il Delegato si impegna a mantenere aggiornato l'elenco dei Soggetti Autorizzati al Trattamento dei Dati Personali (SAT) sotto la propria responsabilità: essi devono essere da Lui incaricati prima dell'avvio delle operazioni di trattamento dando opportuna e tempestiva comunicazione all'UOSD Sistemi Informativi e Telecomunicazioni (a mezzo posta elettronica all'indirizzo sicurezzainformatica@ausl.pe.it) dell'incarico richiedendo le opportune abilitazioni ai sistemi informatici in uso. Nel caso in cui il SAT, nell'ambito delle proprie attività lavorative, fosse assegnato a più UO, Egli dovrà essere incaricato anche dai rispettivi SATD delle ulteriori UO di assegnazione con appositi e distinti atti di incarico.
- 4) Il Delegato si impegna a revocare l'autorizzazione al Trattamento di Dati Personali ad un SAT qualora lo stesso venisse a cessare a qualunque titolo (quiescenza, trasferimento, ecc...) la propria attività sotto la responsabilità del Delegato. Tale revoca dovrà essere opportunamente e tempestivamente comunicata all'UOSD Sistemi Informativi e Telecomunicazioni (a mezzo posta elettronica all'indirizzo sicurezzainformatica@ausl.pe.it) per le necessarie revocazioni di autorizzazione di accesso ai dati personali trattati dall'UO revocante.
- 5) In caso di assenza prolungata di un SAT (di almeno 90 giorni consecutivi), il Delegato si impegna a sospendere l'autorizzazione al Trattamento al Soggetto Autorizzato comunicando tempestivamente la sospensione all'UOSD Sistemi Informativi e Telecomunicazioni (a mezzo posta elettronica all'indirizzo sicurezzainformatica@ausl.pe.it) per le necessarie azioni conseguenti sui diritti di accesso ai dati personali trattati dall'UO di appartenenza del SAT.

Articolo 12 – Amministratori di Sistema

- 1) (Solo per Delegati della UOSD Sistemi Informativi e Telecomunicazioni e dell'UOC Servizio Tecnologico) Il Delegato si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.
- 2) In riferimento ai sistemi informatici di trattamento dei dati del Titolare, per i quali Soggetti Autorizzati alle dipendenze del Delegato esercitano attività di Amministrazione di Sistema, il Delegato si impegna a:
 - a) designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare e al Responsabile della Protezione dei Dati, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
 - b) effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;

- c) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
 - d) comunicare periodicamente al Titolare e al Responsabile della Protezione dei Dati l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
 - e) verificare annualmente l'operato degli amministratori di sistema, informando il Titolare e il Responsabile della Protezione dei Dati circa le risultanze di tale verifica;
 - f) mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento;
 - g) garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.
- 3) In riferimento ai sistemi informatici di trattamento dei dati del Titolare, per i quali Soggetti Esterni (previamente nominati Responsabili del Trattamento dal Delegato) esercitano attività di Amministrazione di Sistema, il Delegato si impegna a chiedere al Responsabile l'elenco degli Amministratori di Sistema ed il rispetto dei punti da a) a g) del precedente capoverso (par. 2) mediante opportuna comunicazione periodica scritta che dovrà essere tempestivamente aggiornata e comunicata ad ogni variazione di tale elenco.

Articolo 13 – Rapporti con le Autorità

- 1) È fatto obbligo al Delegato di interagire con il Garante in caso di richiesta di informazioni o effettuazione di controlli ed accessi da parte dell'Autorità;
- 2) Il Delegato, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

Articolo 14 – Ulteriori Obblighi e Responsabilità

- 1) Il Delegato 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 e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.
- 2) Il Titolare darà comunicazione al Delegato della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata.
- 3) Il Titolare fornirà al Delegato una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.
- 4) Il Delegato si impegna altresì a:
 - a) effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
 - b) collaborare, se richiesto dalla ASL, con gli altri Delegati al trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;

- c) 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, nei limiti dei compiti affidati con il presente atto di designazione;
- d) 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, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati.
- 5) Resta inteso che qualora il Delegato determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

Articolo 15 – Disposizioni Finali

- 1) La presente designazione non comporta alcun diritto per il Delegato ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la ASL.
- 2) Gli allegati alla presente designazione fanno parte integrante della stessa.
- 3) Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.
- 4) Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nel Contratto di Lavoro.
- 5) Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679, del Codice e della normativa vigente in materia di Protezione dei Dati Personali.

IL DIRETTORE GENERALE

Dr. Armando Mancini

Per ricezione ed integrale accettazione del
Delegato

Dr./Dr.ssa

9 ALLEGATO 1 – Ambito del Trattamento

Nell'ambito dei servizi erogati dalla UO dal lei diretta, risulta che le categorie di attività di sua competenza (art. 30.2 del Regolamento) siano di supporto ai seguenti trattamenti censiti:

Cod.	Sub.	Requisito	Descrizione
1		<u>Trattamento 1</u>	
	1.1	Categorie di interessati	
	1.2	Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati)	-
	1.3	Finalità del trattamento	-
	1.4	Tempo di Conservazione	-



www.ausl.pe.it

Regione Abruzzo

ASL 03 Pescara

**LETTERA DI INCARICO DEL SOGGETTO
AUTORIZZATO AL TRATTAMENTO DEI DATI
PERSONALI**

Art. 29 Regolamento UE 679/2016,

Art. 2-quaterdecies D. Lgs. 196/2003 (come modificato dal D.
Lgs. 101/2018)

Regolamento Aziendale
Privacy – Allegato 6

Rev. 01/2018

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530982

**IL SOGGETTO AUTORIZZATO
AL TRATTAMENTO CON DELEGA (SATD)**

Dr./Dr.ssa _____

Ruolo: _____

Prot. n. _____/

Pescara, Il _____

Dr./Sig./Dr.ssa/Sig.ra _____

Ruolo: _____

UO _____

Posta Elettronica _____

Oggetto: Lettera di Incarico a Soggetto Autorizzato al Trattamento dei dati personali (SAT) ai sensi dell'Art. 29 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation), dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore.

Il/La sottoscritto Dr./Dr.ssa _____

in qualità di Soggetto Autorizzato al Trattamento dei dati personali con Delega (SATD) da parte della ASL di Pescara – Titolare del trattamento dei dati personali - considerato che:

- a) La ASL di Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;
- b) La nomina a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;
- c) L'equivalente funzione, per soggetti alle dipendenze della struttura del Titolare, viene assegnata a Soggetti Autorizzati al Trattamento di dati personali con Delega (SATD), ai sensi degli artt. 28 e 29 del Regolamento UE 679/2016 e dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018);
- d) La presente nomina integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di Pescara e sul Soggetto Autorizzato al Trattamento di dati personali (di seguito "Soggetto Autorizzato") derivanti dall'esecuzione degli incarichi organizzativi previsti per il Soggetto Autorizzato in base alle funzioni ad egli attribuite ed ai trattamenti afferenti alla propria UO di appartenenza;

con il presente atto incarica

ai sensi dell'art. 29 del Reg. UE 679/2016 e

dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018)

Soggetto Autorizzato al Trattamento di dati personali (SAT)

Il/la Dr./Sig./Dr.ssa/Sig.ra _____

per i dati trattati dall'Unità Operativa _____

La presente nomina si applica a tutte le attività svolte dal Soggetto Autorizzato nell'ambito del trattamento dei dati personali di Terzi Interessati, in base alle funzioni ad esso attribuite ed ai trattamenti afferenti alla propria UO di appartenenza, ai sensi del Regolamento UE 679/2016 (di seguito "Regolamento" o "GDPR"), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito "Codice" – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore.

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

- 1) Il presente incarico si applica al trattamento dei dati personali svolto dal Soggetto Autorizzato al Trattamento (di seguito "SAT") per conto della ASL presso l'UO di assegnazione, quale titolare del trattamento ("Titolare del Trattamento"), e definisce gli obblighi del SAT in materia di tutela dei dati personali.
- 2) L'ambito del trattamento è definito da tutti i trattamenti di dati personali effettuati dall'UO di assegnazione a cui Lei ha accesso;
- 3) Natura e finalità del trattamento: il Soggetto Autorizzato tratta i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte dall'Unità Operativa

di assegnazione. Le attività di trattamento sono correlate allo svolgimento delle Sue funzioni (Contratto di Lavoro) nell'ambito dei profili di autorizzazione a Lei attribuiti.

- 4) Il SAT è responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali e delle istruzioni impartite dal Titolare e dal Soggetto Autorizzato al Trattamento con Delega scrivente (SATD).
- 5) Nell'ambito definito, sarà compito del Soggetto Autorizzato al Trattamento fare in modo che i dati personali, trattati nell'ambito della propria attività lavorativa per conto dell'UO di assegnazione, siano:
 - a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
 - b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
 - c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
 - e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
 - f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Articolo 2 – Tipologie di dati personali e categorie di interessati

- 1) I soggetti i cui dati personali sono oggetto del trattamento da parte del SAT ai sensi del presente incarico possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL, terzi incaricati, a qualunque titolo, dalla ASL, pazienti, controparti contrattuali della ASL e, in generale, terze parti rispetto alle quali la ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore. I dati personali trattati possono consistere, a titolo esemplificativo e non esaustivo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

Articolo 3 – Istruzioni

- 1) Il SAT effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare e dallo scrivente SATD in forma documentata. Il presente incarico costituisce parte delle istruzioni della ASL per il trattamento dei dati personali da parte del Soggetto Autorizzato che potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare e/o dello scrivente SATD.

- 2) Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto dal presente incarico deve essere fornita dal Titolare o dal SATD per iscritto (es. Procedure operative, ecc...) per mezzo dei canali di comunicazione istituzionali (ad es.: posta elettronica ordinaria).
- 3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, comunicazioni, Regolamenti, Materiale didattico per la formazione e quanto attinente alla materia pubblicato sul sito aziendale nella sezione Privacy.
- 4) È fatto obbligo al Soggetto Autorizzato di:
 - a) classificare i dati personali, al fine di distinguere quelli appartenenti a particolari categorie di dati (es.: dati sanitari), osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
 - b) conservare separatamente i dati appartenenti a particolari categorie di dati (Art. 9 GDPR);
 - c) consultare esclusivamente i documenti contenenti dati personali necessari per lo svolgimento dell'attività lavorativa prestando particolare attenzione alla custodia ed archiviazione degli stessi;
 - d) custodire e non divulgare le credenziali di autenticazione (UserID e password) necessarie per accedere ai sistemi informatici e tecnologici ed ai dati in essi contenuti necessari per lo svolgimento delle attività di trattamento previste dalla Sua mansione lavorativa;
 - e) custodire e tutelare l'accessibilità agli strumenti elettronici soprattutto mentre è in corso una sessione di lavoro;
 - f) utilizzare gli strumenti ed i programmi in conformità ai regolamenti ("policies") aziendali al fine di proteggere i sistemi informativi e i dati ivi contenuti;
 - g) utilizzare, custodire ed archiviare i supporti rimovibili contenenti dati personali in conformità ai regolamenti aziendali.
 - h) effettuare le operazioni di trattamento solo dei dati personali necessari per lo svolgimento dell'attività lavorativa, nel rispetto dei principi di cui all'art. 5 del GDPR, e delle misure di sicurezza predisposte dal Titolare del trattamento ex art. 32 del GDPR, a tutela della riservatezza degli interessati;
 - i) non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati. In caso di allontanamento, anche temporaneo, dal luogo ove si svolge il trattamento dei dati personali, è necessario verificare che non vi sia possibilità da parte di terzi non autorizzati e/o non legittimati di accedere ai dati personali per i quali era in corso il trattamento;
 - j) limitare l'accesso ai dati necessari all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
 - k) comunicare solo i dati personali preventivamente autorizzati dal Titolare e/o dal SATD;
 - l) informare prontamente il Titolare e/o il SATD di ogni questione rilevante ai fini del rispetto della normativa in materia di protezione dei dati personali;
 - m) informare, tempestivamente e senza ingiustificato ritardo (comunque entro e non oltre 24 ore dalla ricezione), il Titolare e/o il SATD in merito a qualsiasi richiesta di accesso e di esercizio dei diritti da parte degli interessati;
 - n) partecipare ai corsi di formazione in materia di protezione dei dati personali organizzati dal Titolare.
 - o) Gli obblighi relativi alla riservatezza ed alla comunicazione dovranno essere osservati anche in seguito a modifica della presente autorizzazione e/o cessazione del rapporto di lavoro.

- 5) Qualsiasi altra informazione/istruzione al SAT potrà essere fornita dal Titolare e/o dal Soggetto Autorizzato al Trattamento con Delega (SATD) che provvedono anche alla formazione. Per ogni altra misura ed istruzione qui non prevista si rinvia alle procedure aziendali comunicate dal Titolare e/o dal SATD.

Articolo 4 – Riservatezza

- 1) Il presente incarico costituisce l'impegno da parte del SAT all'obbligo del mantenimento della riservatezza dei dati personali a cui il Soggetto Autorizzato ha accesso nell'ambito delle funzioni ad esso attribuite.

Articolo 5 – Sicurezza del trattamento

- 1) Il Soggetto Autorizzato si impegna ad adottare le misure richieste dalla normativa di settore e dalle Regolamentazioni Aziendali ed ogni altra istruzione ad esso impartita.

Articolo 6 – Assistenza

- 1) Tenendo conto della natura del trattamento dei dati personali svolto dal SATD, come descritto nel Registro dei Trattamenti, il SAT si impegna ad assistere il Titolare ed il SATD, approntando le adeguate misure tecniche e organizzative secondo le istruzioni impartitegli.

Articolo 7 – Violazioni di Dati Personali (cd. "Data Breach")

- 1) Il Soggetto Autorizzato si impegna ad informare immediatamente il SATD, senza ingiustificato ritardo dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti 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.
- 2) Il Soggetto Autorizzato si impegna inoltre, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, a prestare ogni necessaria collaborazione al SATD in relazione all'adempimento degli obblighi gravanti sul Titolare relativi alla notifica delle suddette violazioni al Garante per la Protezione dei Dati Personali ai sensi dell'art. 33 del GDPR o di comunicazione delle stesse agli interessati ai sensi dell'art. 34 del GDPR.

Articolo 8 – Ulteriori Obblighi e Responsabilità

- 1) Il Soggetto Autorizzato mette a disposizione del SATD e 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 e del SATD di cui alla presente lettera di incarico e consente al Titolare del trattamento ed al SATD l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso, dal SATD o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui alla presente lettera.
- 2) Il SATD darà comunicazione al Soggetto Autorizzato della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata.

- 3) Il SAT si impegna altresì a:
- a) collaborare con gli altri Soggetti Autorizzati al Trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
 - b) 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, nei limiti dei compiti affidati con la presente lettera di incarico;
 - c) informare prontamente il SATD di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati.
- 4) Resta inteso che qualora il SAT determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare e/o dal SATD, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

Articolo 9 – Disposizioni Finali

- 1) Resta inteso che la presente lettera di incarico non comporta alcun diritto per il Soggetto Autorizzato ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la ASL.
- 2) Per tutto quanto non previsto dalla presente lettera di incarico si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.
- 3) La mancata sottoscrizione delle presenti istruzioni non consentirà di dare attuazione a quanto previsto nel Contratto di Lavoro.
- 4) Una volta dato riscontro positivo alla presente lettera di incarico, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679, del Codice e della vigente normativa in materia di protezione dei dati personali.

Il Soggetto Autorizzato al Trattamento con
Delega (SATD)

Per ricezione ed integrale accettazione del
Soggetto Autorizzato (SAT)

Dr./Dr.ssa

Dr./Sig./Dr.ssa/Sig.ra

Data

	Regione Abruzzo ASL 03 Pescara	MOD-RT-001
	LETTERA DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI Art. 28 Regolamento UE 679/2016	Caso 1 - Ad uso del Professionisti

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530982

II SOGGETTO AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI CON DELEGA (SATD)

Prot. n. _____/

Pescara, li _____

Spett.le _____

Indirizzo: _____

CF/P.IVA _____

Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Ditta _____ *Accordo per la Protezione dei Dati (APD)* ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e della vigente normativa di settore. In applicazione della Delibera ASL Pescara n. _____ del ___/___/___.

Il sottoscritto Dr. _____ in qualità di Soggetto Autorizzato al Trattamento con Delega (di seguito anche SATD) della ASL Pescara – Titolare del trattamento dei dati personali - considerato che:

- e) La ASL Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;

- f) La nomina a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;
- g) Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL Pescara n. _____ del ___/___/___ (di seguito la "Delibera") tra la ASL Pescara (di seguito "ASL PE" o "Titolare") e il Professionista _____ (di seguito il "Fornitore" o il "Responsabile") con particolare riferimento agli obblighi di protezione dei dati;

con il presente accordo designa

ai sensi dell'art. 28 del Reg. UE 679/2016 e

il Professionista _____

quale **Responsabile del Trattamento**

dei dati personali trattati per conto della ASL PE nell'ambito del servizio

_____ (oggetto della Delibera)

Il presente Accordo sulla Protezione dei Dati (di seguito anche APD) si applica a tutte le attività svolte dal Responsabile nell'ambito del trattamento dei dati personali ai sensi del Regolamento UE 679/2016 (di seguito "Regolamento" o "GDPR"), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito "Codice" – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore, nell'ambito della Delibera, ivi comprese le attività svolte dai propri soggetti autorizzati al trattamento o terze parti (es.: sub-responsabili), nominate dal Responsabile, che trattino dati per conto del Titolare (ASL PE).

Di seguito verranno intesi il Responsabile e la ASL PE congiuntamente come le "Parti" e ciascuna singolarmente come la "Parte"; inoltre ogni riferimento al Titolare dovrà essere inteso come effettuato al SATD ed ogni comunicazione al Titolare dovrà essere trasmessa congiuntamente al Soggetto Autorizzato con Delega scrivente (email: _____@_____), all'Ufficio Privacy (email: ufficioprivacy@ausl.pe.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo@ausl.pe.it).

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

- 1) Il presente APD si applica al trattamento dei dati personali svolto dal Fornitore in qualità di Responsabile del Trattamento per conto della ASL PE, quale Titolare del Trattamento, ai sensi della Delibera e definisce gli obblighi delle Parti in materia di tutela dei dati personali;
- 2) La Natura, la finalità e l'ambito del trattamento sono definiti da tutti i trattamenti di dati personali effettuati nell'esecuzione dei servizi previsti dalla Delibera e riportati nell'Allegato 1 al presente Accordo sulla Protezione dei Dati (APD);
- 3) Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali;
- 4) Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.

- 5) La durata del trattamento dei dati personali dei Terzi Interessati da parte del Fornitore corrisponde alla durata riportata nella Delibera sulla base di quanto indicato nel Contratto;
- 6) Nell'Ambito di Trattamento definito, sarà compito del Responsabile fare in modo che i dati personali, trattati per conto del Titolare, siano:
 - a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
 - b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
 - c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
 - e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
 - f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Articolo 2 – Tipologie di dati personali e categorie di interessati

- 1) I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente APD possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL PE, terzi incaricati, a qualunque titolo, dalla ASL PE, pazienti, controparti contrattuali della ASL PE e, in generale, terze parti rispetto alle quali la ASL PE agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore. I dati personali trattati possono consistere, a titolo esemplificativo e non esaustivo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

Articolo 3 – Istruzioni

- 1) Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 1 al presente APD. Il presente APD e la Delibera con i suoi allegati costituiscono parte delle istruzioni fornite dal Titolare per il trattamento dei dati personali, per il tramite del Soggetto Autorizzato al Trattamento con Delega, al Fornitore e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.
- 2) Qualsiasi istruzione aggiuntiva o modificata rispetto a quanto previsto nella Delibera e nel presente APD dovrà essere trasmessa dalla ASL PE al Fornitore per iscritto e comunicata via PEC e/o raccomandata a/r. Tale ulteriore istruzione diverrà efficace entro 30 giorni dalla data di comunicazione (invio).

- 3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Materiale didattico per la formazione e inoltre tutto quanto attinente alla materia pubblicato sul sito aziendale nella sezione Privacy.
- 4) È fatto obbligo al Responsabile di:
- a) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 del presente APD;
 - b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32, come previsto dall'art. 5 del presente APD;
 - c) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'art. 6 del presente APD;
 - d) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 7 del presente APD;
 - e) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'art.8 del presente APD;
 - f) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'art.9 del presente APD;
 - g) nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 28.3.b) del Reg. UE 679/2016 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione come previsto dall'art. 10 del presente APD;
 - h) ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 679/2016, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall'art. 11 del presente APD;
 - i) ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall'art. 12 del presente APD;
 - j) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 del presente APD;
 - k) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 del presente APD;
 - l) redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e degli eventuali sub-Responsabili e verificare annualmente l'ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell'assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);
 - m) controllare le operazioni di trattamento svolte dagli autorizzati ed eventualmente dai sub-Responsabili e la conformità all'ambito di trattamento consentito;
 - n) attuare gli obblighi di informazione (Informativa ex Artt. 13-14 del Regolamento) ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
 - o) comunicare immediatamente al titolare non oltre le 12 ore successive al loro ricevimento (da parte propria o dei propri sub-Responsabili), ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
 - p) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;

q) rispettare tutto quanto ulteriormente disciplinato dal presente APD.

Articolo 4 – Riservatezza

- 1) Il Fornitore si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
- 2) Il Fornitore garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto (Soggetti Autorizzati e Sub-Responsabili) si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

Articolo 5 – Sicurezza del trattamento

- 1) Il Fornitore si impegna ad adottare tutte le misure richieste dall'Art. 32 del GDPR e le procedure tecniche e organizzative in materia stabilite dal Titolare.
- 2) In particolare - in considerazione dello stato dell'arte, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Fornitore si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 2 al presente APD di cui si richiede la compilazione per la descrizione delle modalità di implementazione.
- 3) Come ulteriore garanzia per la sicurezza del trattamento, il Fornitore si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti secondo quanto previsto dall'Allegato 3.
- 4) Qualora il Fornitore intendesse apportare modifiche alle misure tecniche e organizzative da lui descritte nell'Allegato 2 e/o alle indicazioni fornite nell'Allegato 3, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva idonea comunicazione, via posta elettronica ordinaria, al Soggetto Autorizzato con Delega sottoscritto e all'Ufficio Privacy, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure adottate in precedenza.

Articolo 6 – Assistenza

- 1) Tenendo conto della natura del trattamento dei dati personali svolto dal Fornitore, come descritto nel Contratto allegato alla Delibera, il Fornitore si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 15 a 22 del GDPR.
- 2) Il Fornitore dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti o di uno dei sub-responsabili (ved. Art. 11 del presente APD) uno dei diritti di cui agli Artt. da 15 a 22 del GDPR.
- 3) Tenendo conto della natura del trattamento, come descritto nel Contratto allegato alla Delibera e nel presente APD, e delle informazioni di volta in volta messe a disposizione, il Fornitore si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR.

Articolo 7 – Conservazione, Riconsegna e Cancellazione

- 1) I dati personali trattati dal Titolare, che siano oggetto di trattamento da parte del Responsabile nell'ambito dell'esecuzione delle attività previste dal Contratto allegato alla Delibera, in base ai termini di conservazione previsti nei registri di trattamento, devono essere periodicamente cancellati dal Responsabile ove ne ricorra il termine. Alla cessazione del Contratto allegato alla Delibera, i dati oggetto di Trattamento da parte del Responsabile, per i quali non sia maturato il termine di cancellazione, devono essere restituiti al Titolare entro un termine massimo di 30 giorni dalla cessazione dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.
- 2) In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

Articolo 8 – Violazioni di Dati Personali (cd. “Data Breach”)

- 1) Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti 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.
- 2) Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
- 3) La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi dpo.aslpe@pec.it e dpo@ausl.pe.it.

Articolo 9 – Valutazione D'impatto (CD. “DATA PROTECTION IMPACT ASSESSMENT”)

- 1) Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

Articolo 10 – Soggetti Autorizzati al Trattamento

- 1) Il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto e formalmente autorizzati (ex art. 2-*quaterdecies* del Codice), il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

- 2) Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

Articolo 11 – Sub-responsabili del Trattamento

- 1) Per l'esecuzione di specifiche attività per conto della ASL PE nell'ambito del Contratto, il Responsabile potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente APD tra il Titolare del trattamento e il Responsabile, 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. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.
- 2) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell'art. 8 del presente APD), laddove intenda designare o sostituire un Sub-responsabile del Trattamento. La comunicazione al Titolare dovrà contenere l'elencazione dettagliata delle attività, previste dal Contratto, affidate al sub-Responsabile e dovrà essere effettuata 30 giorni prima dell'operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 30 giorni dalla ricezione della comunicazione da parte del Responsabile.
- 3) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell'art. 8 del presente APD), laddove intenda cessare il rapporto esistente con un sub-Responsabile del Trattamento senza procedere ad una sua sostituzione. Questa operazione prevede che le attività affidate al sub-Responsabile vengano riprese in carico da parte del Responsabile o riassegnate ad uno degli altri sub-Responsabili già nominati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 30 giorni prima dell'operazione di cessazione.
- 4) Qualora il Titolare sollevi obiezioni su uno o più Sub-responsabili del Trattamento, darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, quest'ultimo potrà:
- a) proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; o
 - b) adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
- 5) L'elenco completo ed aggiornato dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto allegato alla Delibera dovrà essere periodicamente (ogni anno entro il 31 gennaio) fornito al Titolare.

- 6) Il Fornitore è responsabile nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi previsti dalla normativa vigente in materia di Protezione dei Dati Personali e dal presente APD.
- 7) Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

Articolo 12 – Rapporti con le Autorità

- 1) Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

Articolo 13 – Ulteriori Obblighi e Responsabilità

- 1) Il Responsabile 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 e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente APD.
- 2) Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.
- 3) Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.
- 4) Il Responsabile si impegna altresì a:
 - a) effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
 - b) collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
 - c) 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, nei limiti dei compiti affidati con il presente atto di designazione;
 - d) 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, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato 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 illecito o impossibile agire secondo le istruzioni ricevute dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

- 5) Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità (art. 28.10 del Regolamento).

Articolo 14 – Disposizioni Finali

- 1) La presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto allegato alla Delibera.
- 2) Gli allegati al presente APD fanno parte integrante dello stesso: essi costituiscono parte integrante del Registro dei Trattamenti del Responsabile e dovranno essere mantenuti aggiornati da parte del Responsabile.
- 3) Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nel Contratto allegato alla Delibera.
- 4) Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/01 di ogni anno.
- 5) Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente APD, costituisce una violazione del Contratto, di cui il presente APD è parte integrante, del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018) oltre che di quanto disposto dal Codice Civile e dal Codice Penale.
- 6) Il presente Accordo sulla Protezione dei Dati Personali deve essere restituito, opportunamente sottoscritto digitalmente entro 7 giorni dal ricevimento a mezzo PEC. La restituzione dovrà anch'essa essere effettuata a mezzo PEC all'indirizzo protocollo.aslpe@pec.it
- 7) Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il Soggetto Autorizzato al Trattamento con
Delega (SATD)

Dr./ssa

Per ricezione ed integrale accettazione del
Responsabile

10 ALLEGATO 1 – Ambito di Trattamento, Categorie di attività e Impatto

Scheda n. _____

Nella scheda seguente (una per ogni trattamento), nell'ambito dei servizi erogati per conto della ASL PE, vengono definiti i seguenti punti: l'ambito di Trattamento, le categorie di attività svolte dal Responsabile, e l'impatto sulla protezione dei dati; le informazioni sotto riportate sono necessarie per la compilazione dei Registri di Trattamento da parte del Responsabile (art. 30.2 del Regolamento).

Cod.	Voce	Descrizione
1	AMBITO DI TRATTAMENTO	
1.1	Trattamento	
1.2	Finalità del trattamento	
1.3	Categorie di interessati	
1.4	Categorie di Dati Personali oggetto di trattamento	
1.5	Categorie di Destinatari	
1.6	Durata del trattamento	
1.7	Durata della Conservazione	
1.8	Trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale	
2	CATEGORIE DI ATTIVITÀ RELATIVE AL TRATTAMENTO (OPERAZIONI DI TRATTAMENTO)	
2.1	Raccolta	
2.2	Registrazione	
2.3	Organizzazione	
2.4	Strutturazione	
2.5	Conservazione	
2.6	Adattamento o Modifica	
2.7	Estrazione	
2.8	Consultazione	
2.9	Uso	
2.10	Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione	
2.11	Raffronto o Interconnessione	
2.12	Limitazione	
2.13	Cancellazione o Distruzione	
2.14	Trasferimento verso un paese terzo o una organizzazione internazionale	
2.15	Manutenzione	

11 ELENCO ALLEGATI al presente Accordo

- 1) ALLEGATO 1 – Ambito di Trattamento
- 2) _____
- 3) _____
- 4) _____
- 5) _____
- 6) _____
- 7) _____
- 8) _____
- 9) _____
- 10) _____
- 11) _____
- 12) _____
- 13) _____
- 14) _____
- 15) _____
- 16) _____
- 17) _____
- 18) _____
- 19) _____
- 20) _____
- 21) _____
- 22) _____
- 23) _____

	Regione Abruzzo ASL 03 Pescara	MOD-RT-002
	LETTERA DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI Art. 28 Regolamento UE 679/2016	Caso 2 - Servizi non Tecnologici /Complessi

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530992

II SOGGETTO AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI CON DELEGA (SATD)

Prot. n. _____/

Pescara, il _____

Spett.le _____

Indirizzo: _____

CF/P.IVA _____

Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Ditta _____ *Accordo per la Protezione dei Dati (APD)* ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e della vigente normativa di settore. In applicazione della Delibera ASL PE n. _____ del ___/___/___.

Il sottoscritto Dr. _____ in qualità di Soggetto Autorizzato al Trattamento con Delega (di seguito anche SATD) della ASL di Pescara – Titolare del trattamento dei dati personali - considerato che:

- h) La ASL di Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;

- i) La nomina a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;
- j) Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL Pescara n. _____ del ___/___/___ (di seguito la "Delibera") tra la ASL di Pescara (di seguito "ASL PE" o "Titolare") e la società _____ (di seguito il "Fornitore" o il "Responsabile") con particolare riferimento agli obblighi di protezione dei dati;

con il presente accordo designa

ai sensi dell'art. 28 del Reg. UE 679/2016 e

la società _____

quale Responsabile del Trattamento

dei dati personali trattati per conto della ASL PE nell'ambito del servizio

_____ (oggetto della Delibera)

Il presente Accordo sulla Protezione dei Dati (di seguito anche APD) si applica a tutte le attività svolte dal Responsabile nell'ambito del trattamento dei dati personali ai sensi del Regolamento UE 679/2016 (di seguito "Regolamento" o "GDPR"), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito "Codice" – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore, nell'ambito della Delibera, ivi comprese le attività svolte dai propri soggetti autorizzati al trattamento o terze parti (es.: sub-responsabili), nominate dal Responsabile, che trattino dati per conto del Titolare (ASL PE).

Di seguito verranno intesi il Responsabile e la ASL PE congiuntamente come le "Parti" e ciascuna singolarmente come la "Parte"; inoltre ogni riferimento al Titolare dovrà essere inteso come effettuato al SATD ed ogni comunicazione al Titolare dovrà essere trasmessa congiuntamente al Soggetto Autorizzato con Delega scrivente (email: _____@_____), all'Ufficio Privacy (email: ufficioprivacy@ausl.pe.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo.aslpe@pec.it).

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

- 1) Il presente APD si applica al trattamento dei dati personali svolto dal Fornitore in qualità di Responsabile del Trattamento per conto della ASL PE, quale Titolare del Trattamento, ai sensi della Delibera e definisce gli obblighi delle Parti in materia di tutela dei dati personali;
- 2) La Natura, la finalità e l'ambito del trattamento sono definiti da tutti i trattamenti di dati personali effettuati nell'esecuzione dei servizi previsti dalla Delibera e riportati nell'Allegato 1 al presente Accordo sulla Protezione dei Dati (APD);
- 3) Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali;
- 4) Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.
- 5) La durata del trattamento dei dati personali dei Terzi Interessati da parte del Fornitore corrisponde alla durata riportata nella Delibera sulla base di quanto indicato nel Contratto;

- 6) Nell'Ambito di Trattamento definito, sarà compito del Responsabile fare in modo che i dati personali, trattati per conto del Titolare, siano:
- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
 - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
 - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
 - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
 - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
- 7) Le evidenze relative al rispetto del punto 6) sono riportate nell'Allegato 2 al presente documento.

Articolo 2 – Tipologie di dati personali e categorie di interessati

- 1) I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente APD possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL, terzi incaricati, a qualunque titolo, dalla ASL, pazienti, controparti contrattuali della ASL e, in generale, terze parti rispetto alle quali la ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore. I dati personali trattati possono consistere, a titolo esemplificativo e non esaustivo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

Articolo 3 – Istruzioni

- 1) Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 1 al presente APD. Il presente APD e la Delibera con i suoi allegati costituiscono parte delle istruzioni fornite dal Titolare per il trattamento dei dati personali, per il tramite del Soggetto Autorizzato al Trattamento con Delega, al Fornitore e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.
- 2) Qualsiasi istruzione aggiuntiva o modificata rispetto a quanto previsto nella Delibera e nel presente APD dovrà essere trasmessa dalla ASL PE al Fornitore per iscritto e comunicata via PEC e/o raccomandata a/r. Tale ulteriore istruzione diverrà efficace entro 30 giorni dalla data di comunicazione (invio).

- 3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Materiale didattico per la formazione e inoltre tutto quanto attinente alla materia pubblicato sul sito aziendale nella sezione Privacy.
- 4) È fatto obbligo al Responsabile di:
- i) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 del presente APD;
 - ii) adottare le misure di sicurezza richieste ai sensi dell'Art. 32, come previsto dall'art. 5 del presente APD;
 - iii) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'art. 6 del presente APD;
 - iv) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 7 del presente APD;
 - v) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'art.8 del presente APD;
 - vi) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'art.9 del presente APD;
 - vii) nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 28.3.b) del Reg. UE 679/2016 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione come previsto dall'art. 10 del presente APD;
 - viii) ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 679/2016, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall'art. 11 del presente APD;
 - ix) ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall'art. 12 del presente APD;
 - x) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 del presente APD;
 - xi) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 del presente APD;
 - xii) redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e degli eventuali sub-Responsabili e verificare annualmente l'ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell'assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);
 - xiii) controllare le operazioni di trattamento svolte dagli autorizzati ed eventualmente dai sub-Responsabili e la conformità all'ambito di trattamento consentito;
 - xiv) attuare gli obblighi di informazione (Informativa ex Artt. 13-14 del Regolamento) ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
 - xv) comunicare immediatamente al titolare non oltre le 12 ore successive al loro ricevimento (da parte propria o dei propri sub-Responsabili), ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
 - xvi) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;

xvii) rispettare tutto quanto ulteriormente disciplinato dal presente APD.

Articolo 4 – Riservatezza

- 1) Il Fornitore si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
- 2) Il Fornitore garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto (Soggetti Autorizzati e Sub-Responsabili) si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

Articolo 5 – Sicurezza del trattamento

- 1) Il Fornitore si impegna ad adottare tutte le misure richieste dall'Art. 32 del GDPR e le procedure tecniche e organizzative in materia stabilite dal Titolare.
- 2) In particolare - in considerazione dello stato dell'arte, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Fornitore si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 2 al presente APD di cui si richiede la compilazione per la descrizione delle modalità di implementazione.
- 3) Come ulteriore garanzia per la sicurezza del trattamento, il Fornitore si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti secondo quanto previsto dall'Allegato 3.
- 4) Qualora il Fornitore intendesse apportare modifiche alle misure tecniche e organizzative da lui descritte nell'Allegato 2 e/o alle indicazioni fornite nell'Allegato 3, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva idonea comunicazione, via posta elettronica ordinaria, al Soggetto Autorizzato con Delega sottoscritto e all'Ufficio Privacy, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure adottate in precedenza.

Articolo 6 – Assistenza

- 1) Tenendo conto della natura del trattamento dei dati personali svolto dal Fornitore, come descritto nel Contratto allegato alla Delibera, il Fornitore si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 15 a 22 del GDPR.
- 2) Il Fornitore dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti o di uno dei sub-responsabili (ved. Art. 11 del presente APD) uno dei diritti di cui agli Artt. da 15 a 22 del GDPR.
- 3) Tenendo conto della natura del trattamento, come descritto nel Contratto allegato alla Delibera e nel presente APD, e delle informazioni di volta in volta messe a disposizione, il Fornitore si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR.

Articolo 7 – Conservazione, Riconsegna e Cancellazione

- 1) I dati personali trattati dal Titolare, che siano oggetto di trattamento da parte del Responsabile nell'ambito dell'esecuzione delle attività previste dal Contratto allegato alla Delibera, in base ai termini di conservazione previsti nei registri di trattamento, devono essere periodicamente cancellati dal Responsabile ove ne ricorra il termine. Alla cessazione del Contratto allegato alla Delibera, i dati oggetto di Trattamento da parte del Responsabile, per i quali non sia maturato il termine di cancellazione, devono essere restituiti al Titolare entro un termine massimo di 30 giorni dalla cessazione dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.
- 2) In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

Articolo 8 – Violazioni di Dati Personali (cd. “Data Breach”)

- 1) Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti 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.
- 2) Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
- 3) La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi dpo.aslpe@pec.it e dpo@ausl.pe.it.

Articolo 9 – Valutazione D'impatto (CD. “DATA PROTECTION IMPACT ASSESSMENT”)

- 1) Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

Articolo 10 – Soggetti Autorizzati al Trattamento

- 1) Il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto e formalmente autorizzati (ex art. 2-*quaterdecies* del Codice), il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

- 2) Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

Articolo 11 – Sub-responsabili del Trattamento

- 1) Per l'esecuzione di specifiche attività per conto della ASL nell'ambito del Contratto, il Responsabile potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente APD tra il Titolare del trattamento e il Responsabile, 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. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.
- 2) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell'art. 8 del presente APD), laddove intenda designare o sostituire un Sub-responsabile del Trattamento. La comunicazione al Titolare dovrà contenere l'elencazione dettagliata delle attività, previste dal Contratto, affidate al sub-Responsabile e dovrà essere effettuata 30 giorni prima dell'operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 30 giorni dalla ricezione della comunicazione da parte del Responsabile.
- 3) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell'art. 8 del presente APD), laddove intenda cessare il rapporto esistente con un sub-Responsabile del Trattamento senza procedere ad una sua sostituzione. Questa operazione prevede che le attività affidate al sub-Responsabile vengano riprese in carico da parte del Responsabile o riassegnate ad uno degli altri sub-Responsabili già nominati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 30 giorni prima dell'operazione di cessazione.
- 4) Qualora il Titolare sollevi obiezioni su uno o più Sub-responsabili del Trattamento, darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, quest'ultimo potrà:
 - a) proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; o
 - b) adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
- 5) L'elenco completo ed aggiornato dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto allegato alla Delibera dovrà essere periodicamente (ogni anno entro il 31 gennaio) fornito al Titolare.

- 6) Il Fornitore è responsabile nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi previsti dalla normativa vigente in materia di Protezione dei Dati Personali e dal presente APD.
- 7) Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

Articolo 12 – Amministratori di Sistema

- 1) Ove applicabile in relazione ai prodotti e servizi forniti, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.
- 2) In riferimento ai sistemi informatici (interni o esterni alle strutture dell'Azienda Sanitaria) di trattamento dei dati del Titolare, per i quali il Responsabile (o un suo Sub-responsabile) nomina uno o più Amministratori di Sistema (di seguito anche “AdS”), il Responsabile si impegna a:
 - a) designare quali Amministratori di Sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
 - b) effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
 - c) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
 - d) comunicare periodicamente (almeno una volta l'anno, entro il 31/01) al Titolare l'elenco aggiornato degli Amministratori di Sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) ed i dati di contatto per l'attivazione di eventuali procedure di emergenza;
 - e) comunicare tempestivamente (entro 3 giorni dall'ingresso, sostituzione o cessazione degli AdS) al Titolare eventuali variazioni che saranno riportate nell'elenco, specificando eventuali ingressi, sostituzioni o cessazioni, l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) e le eventuali credenziali di autenticazione introdotte o dismesse e, solo per i nuovi AdS, i dati di contatto per l'attivazione di eventuali procedure di emergenza;
 - f) verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
 - g) conservare i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili) o renderli disponibili per la conservazione da parte del Titolare (qualora i sistemi siano installati presso le strutture del Titolare);

- h) garantire una rigida separazione dei compiti tra chi autorizza e/o assegna i privilegi di accesso (credenziali di Amministratore) e chi effettua le attività tecnico-sistemistiche sui medesimi sistemi.

Articolo 13 – Rapporti con le Autorità

- 2) Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

Articolo 14 – Ulteriori Obblighi e Responsabilità

- 1) Il Responsabile 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 e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente APD.
- 2) Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.
- 3) Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.
- 4) Il Responsabile si impegna altresì a:
- a) effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
 - b) collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
 - c) 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, nei limiti dei compiti affidati con il presente atto di designazione;
 - d) 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, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato 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 illecito o impossibile agire secondo le istruzioni ricevute dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.
- 5) Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità (art. 28.10 del Regolamento).

Articolo 15 – Disposizioni Finali

- 1) La presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto allegato alla Delibera.
- 2) Gli allegati al presente APD fanno parte integrante dello stesso: essi costituiscono parte integrante del Registro dei Trattamenti del Responsabile e dovranno essere mantenuti aggiornati da parte del Responsabile.
- 3) Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nel Contratto allegato alla Delibera.
- 4) Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/01 di ogni anno.
- 5) Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente APD, costituisce una violazione del Contratto, di cui il presente APD è parte integrante, del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018) oltre che di quanto disposto dal Codice Civile e dal Codice Penale.
- 6) Il presente Accordo sulla Protezione dei Dati Personali deve essere restituito, opportunamente sottoscritto digitalmente entro 7 giorni dal ricevimento a mezzo PEC. La restituzione dovrà anch'essa essere effettuata a mezzo PEC all'indirizzo protocollo.aslpe@pec.it.
- 7) Una volta che il Fornitore abbia restituito il presente accordo a mezzo PEC, avrà a disposizione 30 giorni per la restituzione degli allegati 2 e 3 al presente APD. Tale termine per la compilazione degli allegati consentirà al Responsabile di poter indicare in maniera puntuale quanto richiesto e di essere eventualmente supportato (se richiesto) dal SATD e/o dal DPO in caso di necessità.
- 8) Gli allegati 2 e 3 al presente APD, forniti in formato editabile, dovranno essere restituiti da parte del Fornitore, compilati e sottoscritti digitalmente, inviandoli a mezzo PEC all'indirizzo protocollo.aslpe@pec.it.
- 9) Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il Soggetto Autorizzato al Trattamento con
Delega (SATD)

Dr./ssa

Per ricezione ed integrale accettazione del
Responsabile

ALLEGATO 1 – Ambito di Trattamento, Categorie di attività e Impatto

Scheda n. _____

Nella scheda seguente (una per ogni trattamento), nell'ambito dei servizi erogati per conto della ASL di Pescara, vengono definiti i seguenti punti: l'ambito di Trattamento, le categorie di attività svolte dal Responsabile, e l'impatto sulla protezione dei dati; le informazioni sotto riportate sono necessarie per la compilazione dei Registri di Trattamento da parte del Responsabile (art. 30.2 del Regolamento).

Cod.	Voce	Descrizione
1	AMBITO DI TRATTAMENTO	
1.1	Trattamento	
1.2	Finalità del trattamento	
1.3	Categorie di interessati	
1.4	Categorie di Dati Personali oggetto di trattamento	
1.5	Categorie di Destinatari	
1.6	Durata del trattamento	
1.7	Durata della Conservazione	
1.8	Trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale	
2	CATEGORIE DI ATTIVITÀ RELATIVE AL TRATTAMENTO (OPERAZIONI DI TRATTAMENTO)	
2.1	Raccolta	
2.2	Registrazione	
2.3	Organizzazione	
2.4	Strutturazione	
2.5	Conservazione	
2.6	Adattamento o Modifica	
2.7	Estrazione	
2.8	Consultazione	
2.9	Uso	
2.10	Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione	
2.11	Raffronto o Interconnessione	
2.12	Limitazione	
2.13	Cancellazione o Distruzione	
2.14	Trasferimento verso un paese terzo o una organizzazione internazionale	
3	VALUTAZIONE DI IMPATTO	
3.1	Livello di Impatto Potenziale del Trattamento (prima dell'adozione delle misure di sicurezza previste nell'Al 2)	

3.2

Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure indicate nell'Al 2)

Il livello di impatto indicato nella precedente tabella (punto 3) è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (riga 3.1 "Livello di Impatto Potenziale"), che successivamente all'implementazione delle stesse (riga 3.2 "Livello di Impatto residuo").

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **1- Impatto trascurabile:** gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **2 - Impatto limitato:** gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **3 - Impatto significativo:** gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e non oltre le 24 ore);
- **4 - Impatto massimo:** gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

ALLEGATO 2 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei principi di trattamento, dei diritti degli interessati e l'adozione delle misure di sicurezza, secondo le indicazioni del Regolamento UE 679/2016, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) e del CNIL – (Garante francese per la protezione dei dati personali, indicato dal Garante italiano come riferimento per le attività di Valutazione di Impatto), nell'ambito delle attività svolte per conto del Titolare.

La decisione in merito all'applicabilità delle misure è del Titolare del Trattamento; nella seguente tabella è necessario dare opportuna indicazione dell'adozione di adeguate misure per il rispetto dei principi di trattamento e dei diritti degli interessati:

- Nel caso in cui la misura sia stata adottata, selezionare nel campo "Stato" la voce "A" per "Adottato" fornendo dettagli riguardanti la misura nel campo "Descrizione".
- Nel caso in cui per l'attuazione della misura siano state programmate azioni con relative scadenze si prega di indicare nel campo "Stato" la voce "P" per "Programmato" fornendo dettagli e scadenze riguardanti la misura nel campo "Descrizione".
- Nel caso in cui una misura sia ritenuta non adottabile o non prevista è necessario darne opportuna indicazione (nel campo Stato selezionando la voce "NP") e motivazione (da indicarsi nel campo "Descrizione").

Le indicazioni fornite nel presente allegato relative alle misure di sicurezza dovranno essere riportate all'interno del Registro dei Trattamenti del Responsabile.

Principi di Trattamento e Diritti degli Interessati

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione
A.1	Art. 5.1.a – liceità	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.2	Art. 5.1.b – limitazione della finalità	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.3	Art. 5.1.c – minimizzazione dei dati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.4	Art. 5.1.d – esattezza/qualità dei dati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione
A.5	Art. 5.1.e Limitazione della conservazione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.6	Artt. 12, 13 e 14 – Informazioni per gli interessati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.6	Art. 7 – Gestione del Consenso al Trattamento	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.7	Art. 15 Diritto di Accesso dell'interessato	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.8	Art. 16 – Diritto di Rettifica	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.9	Art. 17 – Diritto alla Cancellazione ("Oblio")	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.10	Art. 18 – Diritto alla Limitazione del Trattamento	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.11	Art. 19 – Obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione delle modalità operative per tenere traccia dei destinatari e garanzia dei diritti</i>
A.12	Art. 20 – Diritto alla portabilità dei dati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.13	Art. 21 – Diritto di Opposizione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.14	Art. 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione delle modalità di gestione del processo decisionale automatizzato e delle modalità per garantire l'esercizio del diritto in oggetto.</i>

Misure di Sicurezza

Ai sensi degli Artt. 5.1.f), 25, 32 del Regolamento, si chiede di descrivere quali misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti al Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non adottabili e darne motivazione.

11.1.1 Misure Organizzative (MO)

N.	Descrizione
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Misure per la Sicurezza dei Dati (CSD)

N.	Descrizione
1	
2	
3	
4	
5	

6	
7	
8	
9	
10	

Misure per la Sicurezza Generale (CSG)

N.	Descrizione
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

ELENCO ALLEGATI al presente Accordo

1. ALLEGATO 1 – Ambito di Trattamento
2. ALLEGATO 2 – Principi, Diritti e Misure Tecniche e Organizzative
3. ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto

4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____
23. _____
24. _____
25. _____



www.ausl.pe.it

Regione Abruzzo

ASL 03 Pescara

**LETTERA DI DESIGNAZIONE A RESPONSABILE DEL
TRATTAMENTO DEI DATI PERSONALI**

Art. 28 Regolamento UE 679/2016

Regolamento Aziendale
PrivacyCaso 3 - Servizi
Tecnologici complessi
 Sede Legale:
 Via Renato Paolini, 45
 65124 Pescara
 P. IVA 01397530982

II SOGGETTO AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI CON DELEGA (SATD)

Prot. n. _____/

Pescara, li _____

Spett.le _____

Indirizzo: _____

CF/P.IVA _____

Oggetto: Accordo per la Designazione a Responsabile del Trattamento dei Dati Personali della Ditta _____ *Accordo per la Protezione dei Dati (APD)* ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e della vigente normativa di settore. In applicazione della Delibera ASL PE n. _____ del __/__/__.

Il sottoscritto Dr. _____ in qualità di Soggetto Autorizzato al Trattamento con Delega (di seguito anche SATD) della ASL di Pescara – Titolare del trattamento dei dati personali - considerato che:

- a) la ASL di Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;

- b) la designazione a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;
- c) il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL PE n. _____ del ___/___/___ (di seguito la "Delibera") tra la ASL di Pescara (di seguito "ASL PE" o "Titolare") e la società _____ (di seguito il "Fornitore" o il "Responsabile") con particolare riferimento agli obblighi di protezione dei dati;

con il presente accordo designa

ai sensi dell'art. 28 del Reg. UE 679/2016 e

la società _____

quale **Responsabile del Trattamento**

dei dati personali trattati per conto della ASL di Pescara nell'ambito del servizio

_____ (oggetto della Delibera)

Il presente Accordo sulla Protezione dei Dati (di seguito anche APD) si applica a tutte le attività svolte dal Responsabile nell'ambito del trattamento dei dati personali ai sensi del Regolamento UE 679/2016 (di seguito "Regolamento" o "GDPR"), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito "Codice" – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore, nell'ambito della Delibera, ivi comprese le attività svolte dai propri soggetti autorizzati al trattamento o terze parti (es.: sub-responsabili), nominate dal Responsabile, che trattino dati per conto del Titolare (ASL PE).

Di seguito verranno intesi il Responsabile e la ASL di Pescara congiuntamente come le "Parti" e ciascuna singolarmente come la "Parte"; inoltre ogni riferimento al Titolare dovrà essere inteso come effettuato al SATD ed ogni comunicazione al Titolare dovrà essere trasmessa congiuntamente al Soggetto Autorizzato con Delega scrivente (email: _____@ausl.pe.it), all'Ufficio Privacy (email: ufficioprivacy@ausl.pe.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo@ausl.pe.it).

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

- 1) Il presente APD si applica al trattamento dei dati personali svolto dal Fornitore in qualità di Responsabile del Trattamento per conto della ASL di Pescara, quale Titolare del Trattamento, ai sensi della Delibera e definisce gli obblighi delle Parti in materia di tutela dei dati personali;
- 2) La Natura, la finalità e l'ambito del trattamento sono definiti da tutti i trattamenti di dati personali effettuati nell'esecuzione dei servizi previsti dalla Delibera e riportati nell'Allegato 1 al presente Accordo sulla Protezione dei Dati (APD);
- 3) Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali;
- 4) Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.

- 5) La durata del trattamento dei dati personali dei Terzi Interessati da parte del Fornitore corrisponde alla durata riportata nella Delibera sulla base di quanto indicato nel Contratto;
- 6) Nell'Ambito di Trattamento definito, sarà compito del Responsabile fare in modo che i dati personali, trattati per conto del Titolare, siano:
 - a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
 - b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
 - c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
 - e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
 - f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
- 7) Le evidenze relative al rispetto del punto 6) sono riportate nell'Allegato 2 al presente documento.

Articolo 2 – Tipologie di dati personali e categorie di interessati

- 1) I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente APD possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL, terzi incaricati, a qualunque titolo, dalla ASL, pazienti, controparti contrattuali della ASL e, in generale, terze parti rispetto alle quali la ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore. I dati personali trattati possono consistere, a titolo esemplificativo e non esaustivo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

Articolo 3 – Istruzioni

- 1) Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 1 al presente APD. Il presente APD e la Delibera con i suoi allegati costituiscono parte delle istruzioni fornite dal Titolare per il trattamento dei dati personali, per il tramite del Soggetto Autorizzato al Trattamento con Delega, al Fornitore e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.
- 2) Qualsiasi istruzione aggiuntiva o modificata rispetto a quanto previsto nella Delibera e nel presente APD dovrà essere trasmessa dalla ASL al Fornitore per iscritto e comunicata via PEC e/o raccomandata a/r. Tale ulteriore istruzione diverrà efficace entro 30 giorni dalla data di comunicazione (invio).

- 3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Materiale didattico per la formazione e inoltre tutto quanto attinente alla materia pubblicato sul sito aziendale nella sezione Privacy.
- 4) È fatto obbligo al Responsabile di:
- a) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 del presente APD;
 - b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32, come previsto dall'art. 5 del presente APD;
 - c) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'art. 6 del presente APD;
 - d) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 7 del presente APD;
 - e) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'art.8 del presente APD;
 - f) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'art.9 del presente APD;
 - g) nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 28.3.b) del Reg. UE 679/2016 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione come previsto dall'art. 10 del presente APD;
 - h) ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 679/2016, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall'art. 11 del presente APD;
 - i) ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall'art. 12 del presente APD;
 - j) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 del presente APD;
 - k) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 del presente APD;
 - l) redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e degli eventuali sub-Responsabili e verificare annualmente l'ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell'assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);
 - m) controllare le operazioni di trattamento svolte dagli autorizzati ed eventualmente dai sub-Responsabili e la conformità all'ambito di trattamento consentito;
 - n) attuare gli obblighi di informazione (Informativa ex Artt. 13-14 del Regolamento) ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
 - o) comunicare immediatamente al titolare non oltre le 12 ore successive al loro ricevimento (da parte propria o dei propri sub-Responsabili), ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
 - p) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;

q) rispettare tutto quanto ulteriormente disciplinato dal presente APD.

Articolo 4 – Riservatezza

- 1) Il Fornitore si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
- 2) Il Fornitore garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto (Soggetti Autorizzati e Sub-Responsabili) si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

Articolo 5 – Sicurezza del trattamento

- 1) Il Fornitore si impegna ad adottare tutte le misure richieste dall'Art. 32 del GDPR e le procedure tecniche e organizzative in materia stabilite dal Titolare.
- 2) In particolare - in considerazione dello stato dell'arte, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Fornitore si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 2 al presente APD di cui si richiede la compilazione per la descrizione delle modalità di implementazione.
- 3) Come ulteriore garanzia per la sicurezza del trattamento, il Fornitore si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti secondo quanto previsto dall'Allegato 3.
- 4) Qualora il Fornitore intendesse apportare modifiche alle misure tecniche e organizzative da lui descritte nell'Allegato 2 e/o alle indicazioni fornite nell'Allegato 3, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva idonea comunicazione, via posta elettronica ordinaria, al Soggetto Autorizzato con Delega sottoscritto e all'Ufficio Privacy, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure adottate in precedenza.

Articolo 6 – Assistenza

- 1) Tenendo conto della natura del trattamento dei dati personali svolto dal Fornitore, come descritto nel Contratto allegato alla Delibera, il Fornitore si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 15 a 22 del GDPR.
- 2) Il Fornitore dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti o di uno dei sub-responsabili (ved. Art. 11 del presente APD) uno dei diritti di cui agli Artt. da 15 a 22 del GDPR.
- 3) Tenendo conto della natura del trattamento, come descritto nel Contratto allegato alla Delibera e nel presente APD, e delle informazioni di volta in volta messe a disposizione, il Fornitore si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR.

Articolo 7 – Conservazione, Riconsegna e Cancellazione

- 1) I dati personali trattati dal Titolare, che siano oggetto di trattamento da parte del Responsabile nell'ambito dell'esecuzione delle attività previste dal Contratto allegato alla Delibera, in base ai termini di conservazione previsti nei registri di trattamento, devono essere periodicamente cancellati dal Responsabile ove ne ricorra il termine. Alla cessazione del Contratto allegato alla Delibera, i dati oggetto di Trattamento da parte del Responsabile, per i quali non sia maturato il termine di cancellazione, devono essere restituiti al Titolare entro un termine massimo di 30 giorni dalla cessazione dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.
- 2) In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

- 1) Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti 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.
- 2) Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
- 3) La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi dpo.aslpe@pec.it e dpo@ausl.pe.it.

Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

- 1) Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

Articolo 10 – Soggetti Autorizzati al Trattamento

- 1) Il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto e formalmente autorizzati (ex art. 2-*quaterdecies* del Codice), il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

- 2) Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

Articolo 11 – Sub-responsabili del Trattamento

- 1) Per l'esecuzione di specifiche attività per conto della ASL nell'ambito del Contratto, il Responsabile potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente APD tra il Titolare del trattamento e il Responsabile, 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. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.
- 2) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell'art. 8 del presente APD), laddove intenda designare o sostituire un Sub-responsabile del Trattamento. La comunicazione al Titolare dovrà contenere l'elencazione dettagliata delle attività, previste dal Contratto, affidate al sub-Responsabile e dovrà essere effettuata 30 giorni prima dell'operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 30 giorni dalla ricezione della comunicazione da parte del Responsabile.
- 3) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell'art. 8 del presente APD), laddove intenda cessare il rapporto esistente con un sub-Responsabile del Trattamento senza procedere ad una sua sostituzione. Questa operazione prevede che le attività affidate al sub-Responsabile vengano riprese in carico da parte del Responsabile o riassegnate ad uno degli altri sub-Responsabili già nominati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 30 giorni prima dell'operazione di cessazione.
- 4) Qualora il Titolare sollevi obiezioni su uno o più Sub-responsabili del Trattamento, darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, quest'ultimo potrà:
 - a) proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; o
 - b) adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
- 5) L'elenco completo ed aggiornato dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto allegato alla Delibera dovrà essere periodicamente (ogni anno entro il 31 gennaio) fornito al Titolare.

- 6) Il Fornitore è responsabile nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi previsti dalla normativa vigente in materia di Protezione dei Dati Personali e dal presente APD.
- 7) Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

Articolo 12 – Amministratori di Sistema

- 1) Ove applicabile in relazione ai prodotti e servizi forniti, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.
- 2) In riferimento ai sistemi informatici (interni o esterni alle strutture dell'Azienda Sanitaria) di trattamento dei dati del Titolare, per i quali il Responsabile (o un suo Sub-responsabile) nomina uno o più Amministratori di Sistema (di seguito anche “AdS”), il Responsabile si impegna a:
 - a) designare quali Amministratori di Sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
 - b) effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
 - c) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
 - d) comunicare periodicamente (almeno una volta l'anno, entro il 31/01) al Titolare l'elenco aggiornato degli Amministratori di Sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) ed i dati di contatto per l'attivazione di eventuali procedure di emergenza;
 - e) comunicare tempestivamente (entro 3 giorni dall'ingresso, sostituzione o cessazione degli AdS) al Titolare eventuali variazioni che saranno riportate nell'elenco, specificando eventuali ingressi, sostituzioni o cessazioni, l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) e le eventuali credenziali di autenticazione introdotte o dismesse e, solo per i nuovi AdS, i dati di contatto per l'attivazione di eventuali procedure di emergenza;
 - f) verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
 - g) conservare i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili) o renderli disponibili per la conservazione da parte del Titolare (qualora i sistemi siano installati presso le strutture del Titolare);

- h) garantire una rigida separazione dei compiti tra chi autorizza e/o assegna i privilegi di accesso (credenziali di Amministratore) e chi effettua le attività tecnico-sistemistiche sui medesimi sistemi.

Articolo 13 – Rapporti con le Autorità

- 1) Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

Articolo 14 – Ulteriori Obblighi e Responsabilità

- 1) Il Responsabile 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 e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente APD.
- 2) Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.
- 3) Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.
- 4) Il Responsabile si impegna altresì a:
- a) effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
 - b) collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
 - c) 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, nei limiti dei compiti affidati con il presente atto di designazione;
 - d) 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, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato 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 illecito o impossibile agire secondo le istruzioni ricevute dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.
- 5) Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità (art. 28.10 del Regolamento).

Articolo 15 – Disposizioni Finali

- 1) La presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto allegato alla Delibera.
- 2) Gli allegati al presente APD fanno parte integrante dello stesso: essi costituiscono parte integrante del Registro dei Trattamenti del Responsabile e dovranno essere mantenuti aggiornati da parte del Responsabile.
- 3) Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nel Contratto allegato alla Delibera.
- 4) Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/01 di ogni anno.
- 5) Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente APD, costituisce una violazione del Contratto, di cui il presente APD è parte integrante, del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018) oltre che di quanto disposto dal Codice Civile e dal Codice Penale.
- 6) Il presente Accordo sulla Protezione dei Dati Personali deve essere restituito, opportunamente sottoscritto digitalmente entro 7 giorni dal ricevimento a mezzo PEC. La restituzione dovrà anch'essa essere effettuata a mezzo PEC all'indirizzo protocollo.aslpe@pec.it
- 7) Una volta che il Fornitore abbia restituito il presente accordo a mezzo PEC, avrà a disposizione 30 giorni per la restituzione degli allegati 2 e 3 al presente APD. Tale termine per la compilazione degli allegati consentirà al Responsabile di poter indicare in maniera puntuale quanto richiesto e di essere eventualmente supportato (se richiesto) dal SATD e/o dal DPO in caso di necessità.
- 8) Gli allegati 2 e 3 al presente APD, forniti in formato editabile, dovranno essere restituiti da parte del Fornitore, compilati e sottoscritti digitalmente, inviandoli a mezzo PEC all'indirizzo protocollo.aslpe@pec.it.
- 9) Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il Soggetto Autorizzato al Trattamento con
Delega (SATD)

Dr./ssa

Per ricezione ed integrale accettazione del
Responsabile

ALLEGATO 1 – Ambito di Trattamento, Categorie di attività e Impatto

Scheda n. _____

Nella scheda seguente (una per ogni trattamento), nell'ambito dei servizi erogati per conto della ASL di Pescara, vengono definiti i seguenti punti: l'ambito di Trattamento, le categorie di attività svolte dal Responsabile, e l'impatto sulla protezione dei dati; le informazioni sotto riportate sono necessarie per la compilazione dei Registri di Trattamento da parte del Responsabile (art. 30.2 del Regolamento).

Cod.	Voce	Descrizione
1	AMBITO DI TRATTAMENTO	
1.1	Trattamento	
1.2	Finalità del trattamento	
1.3	Categorie di interessati	
1.4	Categorie di Dati Personali oggetto di trattamento	
1.5	Categorie di Destinatari	
1.6	Durata del trattamento	
1.7	Durata della Conservazione	
1.8	Trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale	
2	CATEGORIE DI ATTIVITÀ RELATIVE AL TRATTAMENTO (OPERAZIONI DI TRATTAMENTO)	
2.1	Raccolta	
2.2	Registrazione	
2.3	Organizzazione	
2.4	Strutturazione	
2.5	Conservazione	
2.6	Adattamento o Modifica	
2.7	Estrazione	
2.8	Consultazione	
2.9	Uso	
2.10	Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione	
2.11	Raffronto o Interconnessione	
2.12	Limitazione	
2.13	Cancellazione o Distruzione	
2.14	Trasferimento verso un paese terzo o una organizzazione internazionale	
3	VALUTAZIONE DI IMPATTO	
3.1	Livello di Impatto Potenziale del Trattamento (prima dell'adozione delle misure di sicurezza previste nell'All.2)	

3.2

Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure indicate nell'All 2)

Il livello di impatto indicato nella precedente tabella (punto 3) è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (riga 3.1 "*Livello di Impatto Potenziale*"), che successivamente all'implementazione delle stesse (riga 3.2 "*Livello di Impatto residuo*").

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **1- Impatto trascurabile:** gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **2 - Impatto limitato:** gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **3 - Impatto significativo:** gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e non oltre le 24 ore);
- **4 - Impatto massimo:** gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

ALLEGATO 2 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei principi di trattamento, dei diritti degli interessati e l'adozione delle misure di sicurezza, secondo le indicazioni del Regolamento UE 679/2016, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) e del CNIL – (Garante francese per la protezione dei dati personali, indicato dal Garante italiano come riferimento per le attività di Valutazione di Impatto), nell'ambito delle attività svolte per conto del Titolare.

La decisione in merito all'applicabilità delle misure è del Titolare del Trattamento; nella seguente tabella è necessario dare opportuna indicazione dell'adozione di adeguate misure per il rispetto dei principi di trattamento e dei diritti degli interessati:

- Nel caso in cui la misura sia stata adottata, selezionare nel campo "Stato" la voce "A" per "Adottato" fornendo dettagli riguardanti la misura nel campo "Descrizione".
- Nel caso in cui per l'attuazione della misura siano state programmate azioni con relative scadenze si prega di indicare nel campo "Stato" la voce "P" per "Programmato" fornendo dettagli e scadenze riguardanti la misura nel campo "Descrizione".
- Nel caso in cui una misura sia ritenuta non adottabile o non prevista è necessario darne opportuna indicazione (nel campo Stato selezionando la voce "NP") e motivazione (da indicarsi nel campo "Descrizione").

Le indicazioni fornite nel presente allegato relative alle misure di sicurezza dovranno essere riportate all'interno del Registro dei Trattamenti del Responsabile.

Principi di Trattamento e Diritti degli Interessati

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione
A.1	Art. 5.1.a – liceità	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.2	Art. 5.1.b – limitazione della finalità	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.3	Art. 5.1.c – minimizzazione dei dati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.4	Art. 5.1.d – esattezza/qualità dei dati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.5	Art. 5.1.e Limitazione della conservazione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione
A.6	Art. 12, 13 e 14 – Informazioni per gli interessati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.6	Art. 7 – Gestione del Consenso al Trattamento	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.7	Art. 15 Diritto di Accesso dell'interessato	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	
A.8	Art. 16 – Diritto di Rettifica	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.9	Art. 17 – Diritto alla Cancellazione ("Oblio")	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.10	Art. 18 – Diritto alla Limitazione del Trattamento	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.11	Art. 19 – Obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione delle modalità operative per tenere traccia dei destinatari e garanzia dei diritti</i>
A.12	Art. 20 – Diritto alla portabilità dei dati	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.13	Art. 21 – Diritto di Opposizione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione sia delle modalità operative per l'esercizio del diritto in questione</i>
A.14	Art. 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<i>Indicazione delle modalità di gestione del processo decisionale automatizzato e delle modalità per garantire l'esercizio del diritto in oggetto.</i>

Misure di Sicurezza

Ai sensi degli Artt. 5.1.f), 25, 32 del Regolamento, si chiede di descrivere, secondo i criteri precedentemente esposti, quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti al Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non adottabili e darne motivazione.

11.1.2 Controlli Organizzativi

Req.	Misura	Dettaglio	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione (Per alcune domande è possibile indicare più risposte)
CO.1	Politiche generali per la protezione dei dati	Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CO.2	Organizzazione per la protezione dei dati	Articolazione dell'organizzazione per la Protezione dei Dati Personali (Soggetti Autorizzati, sub-Responsabili, ecc...) per il servizio fornito	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CO.3	DPO – Data Protection Officer (Responsabile della Protezione dei Dati)	Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer)	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CO.4	Gestione della Sicurezza dei Dati trattati dalle risorse umane (dipendenti/collaboratori)	Procedure di gestione dell'ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro. Piano di Formazione periodica sulla Protezione dei Dati Personali	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CO.5	Relazioni con i sub-fornitori	Accordi, requisiti, procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)

Req.	Misura	Dettaglio	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione (Per alcune domande è possibile indicare più risposte)
CO.6	Conformità e Audit	<p>Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni</p> <p>Procedure di Audit interne per assicurare la sicurezza dei trattamenti effettuati per conto dell'Azienda (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative)</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CO.7	Presenza di Polizza Cyber Risk	Polizza cyber-risk ed eventuale dettaglio della stessa	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CO.8	Gestione del Cambiamento	Procedura di gestione dei cambiamenti (Change Management) nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, di servizio o organizzativi, ecc...).	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)

Controlli per la Sicurezza dei Dati (CSD)

Req.	Misura	Dettaglio	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione (Per alcune domande è possibile indicare più risposte)
CSD.1	Cifratura	<p>Procedure e Criteri di utilizzo della cifratura</p> <p><i>Misure per rendere i dati personali incomprensibili a chiunque non abbia un'autorizzazione di accesso (crittografia simmetrica o asimmetrica, uso di algoritmi pubblici noti per essere forti, certificato di autenticazione, ecc.).</i></p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<p>Metodologia di Cifratura:</p> <input type="checkbox"/> nessuna <input type="checkbox"/> a livello Hardware (es.: Storage) <input type="checkbox"/> a livello Middleware (es.: DB) <input type="checkbox"/> a livello Software Applicativo <input type="checkbox"/> a livello protocollo di comunicazione <input type="checkbox"/> altra metodologia _____
CSD.2	Pseudonimizzazione	<p>Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato (rif. art. 4.5 Reg. UE 679/2016)</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.3	Controllo degli accessi logici	<p>Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali</p> <p><i>Misure per limitare i rischi che persone non autorizzate accedano elettronicamente ai dati personali (gestione dei profili utente, meccanismi di autenticazione, politica delle password, ecc.).</i></p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.4	Controllo per il partizionamento - segregazione dei dati	<p>Procedure di gestione della segregazione dei dati</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.5	Tracciabilità (Logging)	<p>Procedure volte ad assicurare che la consultazione e l'azione svolta dagli utenti del trattamento siano registrate e attribuite, in modo tale che sia possibile fornire prove durante le indagini (sistema di registrazione, protezione, analisi, conservazione, ecc.).</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)

Req.	Misura	Dettaglio	Appl. (SI/NO)	Stato (Adottata /Planificata /Non Prevista)	Descrizione (Per alcune domande è possibile indicare più risposte)
CSD.6	Monitoraggio dell'Integrità	Procedure finalizzate ad essere avvisati in caso di modifica indesiderata o sparizione di dati personali (es.: funzioni di hash, codice di autenticazione dei messaggi, firma elettronica, prevenzione di SQL Injection, ecc.).	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.7	Archiviazione	Procedure per preservare e gestire gli archivi elettronici contenenti i dati personali destinati a garantire il loro valore (anche legale)	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.8	Sicurezza dei Documenti Cartacei	Procedure per limitare i rischi di accesso di persone non autorizzate a documenti cartacei contenenti dati personali	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.9	Misure per il rispetto della Privacy by Design (Protezione dei dati fin dalla Progettazione)	Ved. Reg. UE 679/2016 art. 25 <i>Indicare eventuali ulteriori misure adottate rispetto a quelle già indicate</i>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSD.10	Misure per il rispetto della Privacy by Default (Protezione dei Dati per impostazione predefinita)	Ved. Reg. UE 679/2016 art. 25 <i>Indicare eventuali ulteriori misure adottate rispetto a quelle già indicate</i>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)

Controlli per la Sicurezza Generale (CSG)

Req.	Misura	Dettaglio	Appl. (SI/NO)	Stato (Adottata /Pianificata /Non Prevista)	Descrizione (Per alcune domande è possibile indicare più risposte)
CSG.1	Sicurezza Operativa	Descrivere come vengano eseguiti gli aggiornamenti dei software (sistemi operativi, applicazioni, ecc.) e l'applicazione dei controlli correttivi di sicurezza (patches).	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.2	Blocco dei Malware	Indicare quale software antivirus/protezione sia installato e aggiornato a intervalli regolari sulle postazioni di lavoro e sui sistemi (anche server) forniti o sotto la propria responsabilità (anche per il supporto da remoto) nell'ambito del contratto.	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.3	Gestione delle postazioni di lavoro	Descrivere le misure di sicurezza implementate sulle postazioni di lavoro utilizzate nell'ambito del servizio e sotto la propria responsabilità (blocco automatico con timer, firewall, ecc.).	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.4	Sicurezza dei Siti Web	Indicare se siano state implementate misure per la sicurezza dei siti Web facenti parte della fornitura	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.5	Backup	Indicare le modalità di gestione dei backup (Piano di Backup)	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.6	Manutenzione	Descrivere le modalità di gestione della manutenzione hardware ed indicare se questo sia tramite un contratto di subfornitura. Indicare se siano possibili interventi di manutenzione da remoto e quali siano le misure di sicurezza adottate.	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.7	Sicurezza dei Canali Informatici (reti)	Indicare il tipo di rete su cui sono eseguite le elaborazioni (isolata, privata o Internet). Specificare quale sistema firewall, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi siano incaricati di garantire la sicurezza della rete sotto la propria responsabilità	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)

Req.	Misura	Dettaglio	Appl. (SI/NO)	Stato (Adottata /Pianficata /Non Prevista)	Descrizione (Per alcune domande è possibile indicare più risposte)
CSG.8	Monitoraggio (gestione incidenti)	Indicare se sia implementato il monitoraggio del funzionamento/sicurezza dei sistemi forniti e con quali modalità.	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.9	Controllo degli accessi fisici	Indicare quali siano le procedure di sicurezza per il controllo dell'accesso fisico alle strutture da cui viene erogato il servizio, che ospitano l'elaborazione o da cui venga effettuato supporto remoto (suddivisione in zone, scorta di visitatori, uso di pass, porte chiuse, videosorveglianza e così via).	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.10	Sicurezza Hardware	Indicare i controlli relativi alla sicurezza fisica dei server e delle workstation (archiviazione protetta, cavi di sicurezza, filtri di riservatezza, cancellazione sicura prima della rottamazione/ sostituzione, ecc.).	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.11	Continuità Operativa/ Disaster Recovery	Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa.	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)
CSG.12	Sicurezza dei sistemi applicativi/ ambienti operativi (anche di virtualizzazione o per la gestione del Cloud – acquisizione, manutenzione, sviluppo)	Procedure/Misure di Sicurezza adottate per i sistemi applicativi o ambienti operativi forniti/utilizzati nella gestione dei sistemi/servizi oggetto del contratto con particolare riferimento a sviluppo, acquisizione, gestione operativa/protezione e manutenzione degli stessi	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> A <input type="checkbox"/> P <input type="checkbox"/> NP	<input type="checkbox"/> Descrizione: <input type="checkbox"/> Documento tecnico allegato per dettagli (Num. Allegato: _____)

ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto

Fornire, ove indicate come applicabili rispetto al servizio fornito, le seguenti informazioni: si prega di indicare la risposta nell'apposito riquadro con eventuali documenti e/o schede tecniche da allegare.

Req.	Dettaglio	Appl. (SI/NO)	Descrizione (Per alcune domande è possibile indicare più risposte)
DT.1	<p><u>Descrizione del sistema/servizio fornito e dell'Architettura Organizzativa/Logica/funzionale</u></p> <p><i>È necessario indicare sinteticamente il sistema/servizio fornito comprensivo, nel caso di servizi che utilizzino tecnologia o sistemi informatici, dell'architettura Logico-Funzionale delle infrastrutture tecnologico-informatiche</i></p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.2	<p><u>Elencazione Attrezzature elettromedicali</u> (diagnostiche, strumentali, ecc...) e fornitura di una scheda tecnica per ogni attrezzatura che ne descriva in dettaglio le funzionalità</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.3	<p><u>Elencazione e descrizione architetturale dell'infrastruttura HW, (comprensiva di eventuali sistemi esterni alla struttura del Titolare) e di comunicazione</u> (anche di supporto ad attrezzature o per fini di erogazione del servizio)</p> <p>Indicare analiticamente se l'installazione sia effettuata presso le strutture dell'Azienda (Centro Elaborazione Dati o altra locazione - es. presso Strutture Operative) o presso Strutture Esterne (di proprietà del fornitore o di terzi), indicando la tipologia di infrastruttura prescelta (server fisici o virtuali, hosting, Cloud privato, Cloud pubblico, Cloud ibrido, ecc...)</p> <p>Nel caso di installazione presso strutture esterne indicazione se ne sia prevista la collocazione in paesi UE o extra-UE.</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.4	<p><u>Elencazione dei sistemi applicativi e middleware utilizzati</u> (es.: software asserviti alle attrezzature, moduli applicativi, sistemi database, web server, ecc...) con indicazione delle relative finalità di utilizzo e architettura generale. (logica o funzionale)</p> <p>Specificare se siano <u>moduli propri o di terzi</u> (anche in caso di componenti, Web Services o altro) ed il <u>dettaglio dell'architettura sistemistica asservita</u> (n. server fisici/virtuali, middleware utilizzati e relative versioni, DB principali e DB "intermedi" e/o di confine per gestire la comunicazione tra i vari moduli di propria fornitura e/o di terzi).</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)

Req.	Dettaglio	Appl. (SI/NO)	Descrizione (Per alcune domande è possibile indicare più risposte)
DT.5	<p><u>Elenco dei Sistemi di interfaccia/Interfacciamenti</u> con altre piattaforme/moduli software (anche di terzi): per ogni interfaccia indicare i moduli interfacciati dal singolo sistema di interfacciamento e se i dati vengano solo ricevuti, solo inviati o ricevuti ed inviati.</p> <p>Indicare, per ogni interfacciamento, quali protocolli di comunicazione siano disponibili e quali utilizzati (es.: HL7, DICOM o altro protocollo, se siano utilizzate tecniche di cifratura ed eventualmente quali)</p> <p>Indicare, per ogni interfacciamento, il dettaglio dei dati conservati (tabelle) e scambiati (messaggistica).</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.6	<p><u>Elenco delle Terze parti coinvolte nella fornitura dei prodotti/servizi</u> e del relativo ruolo (es.: erogazione servizi – specificare quali -, manutenzione, produzione attrezzature, produzione di software, hosting, ecc...) e le sedi da cui operano (con indicazione se siano in UE o extra-UE)</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____)
DT.7	<p><u>Elenco, numero e sede delle figure professionali utilizzate nell'erogazione del servizio</u>, e se siano dipendenti, collaboratori o appartenenti a ditte esterne</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____)
DT.8	<p>Descrizione se nei sistemi/servizi forniti sia gestito/possibile gestire il <u>ciclo di vita delle informazioni</u> (creazione, uso, trasferimento, dismissione con tempo di conservazione definito);</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.9	<p>Indicare l'<u>ultima versione rilasciata di ogni singolo modulo software, middleware o asservito all'attrezzatura</u> (elencato nei punti precedenti);</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____)
DT.10	<p>Indicare l'<u>ultima versione installata in utilizzo per l'erogazione del servizio di ogni singolo modulo software, middleware o asservito all'attrezzatura</u> (elencato nei punti precedenti);</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____)
DT.11	<p>Indicare se l'<u>infrastruttura tecnologica</u> fornita sia basata su sistemi operativi, middleware, altri software o sistemi dichiarati dai produttori "fuori supporto" o non più aggiornati/aggiornabili</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.12	<p>Indicare nell'<u>infrastruttura tecnologica</u> fornita la presenza di software "embedded" e le modalità di gestione della sicurezza</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.13	<p>Indicare gli Amministratori di Sistema del servizio/sistema della vostra società e/o di terzi e l'ambito di responsabilità; indicare inoltre le ubicazioni da cui opera tale personale;</p>	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____)

Req.	Dettaglio	Appl. (SI/NO)	Descrizione (Per alcune domande è possibile indicare più risposte)
DT.14	Indicare le modalità di gestione dei <u>Profili di utenza</u> con indicazione del livello di dettaglio che è possibile raggiungere per le abilitazioni (permessi a livello di modulo, funzionalità, utente o a livello di singolo dato); indicare inoltre se tali utenze siano gestibili tramite protocollo LDAP;	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)
DT.15	Indicare se siano stati forniti i manuali operativi/note di rilascio per l'utilizzo dei servizi/sistemi/prodotti forniti ed i relativi aggiornamenti in caso di upgrade.	<input type="checkbox"/> SI <input type="checkbox"/> NO	<input type="checkbox"/> Descrizione: _____ <input type="checkbox"/> Documento allegato per dettagli (Num. Allegato: _____) <input type="checkbox"/> Scheda Tecnica (Num. Allegato: _____)

ELENCO ALLEGATI al presente Accordo

- 1) ALLEGATO 1 – Ambito di Trattamento
- 2) ALLEGATO 2 – Principi, Diritti e Misure Tecniche e Organizzative
- 3) ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto

- 4) _____
- 5) _____
- 6) _____
- 7) _____
- 8) _____
- 9) _____
- 10) _____
- 11) _____
- 12) _____
- 13) _____
- 14) _____
- 15) _____
- 16) _____
- 17) _____
- 18) _____
- 19) _____
- 20) _____
- 21) _____
- 22) _____
- 23) _____
- 24) _____
- 25) _____

Il Direttore U.O.C. Affari Generali e Legali e il responsabile della Protezione dei dati proponenti, con la sottoscrizione, a seguito dell'istruttoria effettuata, attestano la regolarità tecnica e amministrativa nonché la legittimità del presente provvedimento

Il Responsabile per la
Protezione dei dati
Dott. Giovanni Modesti

Il Direttore della U.O.C.
Affari Generali e Legali -
Dott.ssa Francesca Rancitelli

Il Direttore U.O.C. Affari Generali e Legali proponente attesta che la spesa risulta imputata sulla voce di conto n. _____ del bilancio _____

Il Direttore della U.O.C.
Affari Generali e Legali
Dott.ssa Francesca Rancitelli

Ai sensi del D. Lgs. 502/92 e successive modificazioni ed integrazioni, i sottoscritti esprimono il seguente parere sul presente provvedimento:

favorevole

non favorevole per le seguenti motivazioni

IL DIRETTORE AMMINISTRATIVO
Dott. Paolo Zappalà

favorevole

non favorevole per le seguenti motivazioni

IL DIRETTORE SANITARIO
(DOTT. ANTONIO CAFONETTI)

IL DIRETTORE GENERALE
dr. Armando Mancini



Il presente provvedimento viene pubblicato all'albo on line dell'Asl di Pescara in
data _____ ove rimarrà affisso per un periodo non inferiore a n. 15 giorni consecutivi

05 APR. 2019

- Il presente provvedimento è immediatamente esecutivo a seguito della pubblicazione all'albo on line dell'Asl di Pescara
- Il presente provvedimento è soggetto al controllo da parte della Giunta Regionale

Il presente provvedimento viene trasmesso:

per l'esecuzione a:

• UOC Affari Generali e Legali

•

•

per conoscenza a:

•

•

•

alla Giunta Regionale in data _____ con nota prot. _____

alla Conferenza dei Sindaci in data _____ con nota prot. _____

al Collegio Sindacale in data _____ con nota prot. _____

U.O.C. Affari Generali e Legali
Il funzionario incaricato

U.O.C. Affari Generali e Legali
Il Responsabile Affari Generali
(dott. Fabrizio Veri)

