AZIENDA SANITARIA LOCALE DI PESCARA
Via Renato Paolini, 47 – 65124 Pescara (PE)

DELIBERAZIONE DEL DIRETTORE GENERALE
AZIENDA SANITARIA LOCALE DI PESCARA

ANNO: 2025 N. 564

Data 14/04/2025

OGGETTO: RECEPIMENTO DGR N. 41 DEL 31/01/2025 DELLA REGIONE ABRUZZO E APPROVAZIONE SCHEMA TIPO CONVENZIONE

IL DIRETTORE GENERALE

Oggetto: Recepimento DGR n. 41 del 31/01/2025 della Regione Abruzzo "CONVENZIONE TRA LA REGIONE ABRUZZO E LA REGIONE LOMBARDIA PER IL RIUSO DEL SOFTWARE "CELIACHI@RL" (SISTEMA REGIONALE PER L'EROGAZIONE DEI PRODOTTI DIETETICI SENZA GLUTINE) ADOZIONE NUOVE MODALITÀ DI EROGAZIONE A CARICO SSN - REVISIONE DELLA DISCIPLINA REGIONALE DI CUI ALLE DGR 277/2005 E DGR 83/2020". APPROVAZIONE SCHEMA DI CONVENZIONE PER LA DISTRIBUZIONE DI PRODOTTI SENZA GLUTINE.

Sulla seguente relazione del Direttore, Dott.ssa Manuela Fazia, in qualità di Direttrice della "UOC Direzione Amministrativa Distrettuale e dei Servizi di Prevenzione", nominata con deliberazione del Direttore Generale n.1968 del 30/12/2024, nell'esercizio delle funzioni delegate che qui si riporta integralmente

Premesso:

- DGR n. 277 dell'8 marzo 2005, recante "D.M. 08.06.2001: Assistenza sanitaria integrativa relativa ai prodotti destinati ad una alimentazione particolare – Morbo Celiaco" con la quale sono state tra l'altro stabilite le modalità di riconoscimento del diritto alla fruizione di prodotti dietoterapici per pazienti celiaci e quelle di erogazione dei relativi prodotti da parte degli operatori commerciali autorizzati;
- DGR n.117 del 18 febbraio 2008, recante "Assistenza integrativa relativa ai progetti destinati ad alimentazione particolare: Nuove modalità di erogazione gratuita di prodotti dietetici senza glutine ai soggetti affetti da celiachia", con la quale in particolare è stata modificata la DGR 277/2005 – punto dell'allegato B-, per la parte concernente le modalità di erogazione dei prodotti senza glutine;
- DATO ATTO che ai sensi della vigente normativa in materia di assistenza sanitaria integrativa
  concernente la fruizione di prodotti dietoterapici privi di glutine con spesa a carico del SSN, è prevista per i pazienti celiaci specifica autorizzazione;
- PRESO ATTO che con D.G.R. n. 83 del 18.2.2020 avente ad oggetto: "Livelli Essenziali di Assistenza di cui al DPCM 12 gennaio 2017. Assistenza sanitaria integrativa destinata ai pazienti affetti da morbo celiaco: disposizioni modificative ed integrative sulle modalità di erogazione dei prodotti dietoterapici privi di glutine" l'Esecutivo Regionale ha deliberato, tra l'altro, di dare mandato al Dipartimento Sanità, attraverso il Servizio competente in materia di sanità digitale, di procedere alla valutazione delle misure attuative necessarie per pervenire alla dematerializzazione dei buoni cartacei per l'acquisto dei prodotti dietoterapici destinati ai pazienti celiaci;
- VISTA la DGR n. 100 del 28.02.2023 recante "Legge 4 luglio 2005, n. 123. Dematerializzazione dei buoni spesa cartacei per l'acquisto di prodotti dietoterapici privi di glutine destinati a pazienti celiaci – Approvazione dello Schema di Convenzione tra la Regione Abruzzo e la Regione Lombardia per il Riuso del software "Celiachi@RL (Sistema Regionale per l'erogazione dei prodotti dietetici senza glutine)" con la quale la Regione Abruzzo ha approvato lo schema di Convenzione per il Riuso del software Celiachi@RL;
- SPECIFICATO che il nuovo sistema di gestione dei buoni per celiaci di cui alla Convenzione per il Riuso del Sistema Celiachi@RL, prevede una gestione integralmente dematerializzata del processo, sia nella fase di erogazione sia in quella di rendicontazione dei buoni per celiaci, avendo come precipuo obiettivo il raggiungimento di un sistema regionale centralizzato e che uniformi le procedure su tutte le Aziende sanitarie, le razionalizzi in termini di flusso di rendicontazione mensile e le semplifichi per i pazienti che, una volta ottenuta la diagnosi, potranno gestire il proprio budget mensile su tutto il territorio regionale, come da "Documento sulle Modalità di erogazione a carico SSN dei prodotti senza glutine a favore di soggetti celiaci attraverso il software Celiachi@RL"

- PRESO ATTO che al fine di consentire il pieno funzionamento del nuovo sistema dematerializzato di gestione dei buoni per celiaci, nonché la completa dematerializzazione e digitalizzazione di tutto il processo erogativo e di rendicontazione la Regione Abruzzo ha adottato la DGR n. 41 del 31/01/2025 Convenzione tra la Regione Abruzzo e la Regione Lombardia per il riuso del Software "CELIACHI@RL" (Sistema Regionale per l'erogazione dei prodotti dietetici senza glutine) adozione delle nuove modalità di erogazione a carico del SSN – Revisione della disciplina regionale di cui alle DGR 277/2005 E DGR 83/2020,
- la citata determina regionale ha proposto uno schema di convenzione da adottare per il convenzionamento tra le Asl e gli esercizi commerciali e detto schema è stato revisionato ed adattato secondo le esigenze e regole di questa azienda;

Ritenuto di dover recepire la DGR n. 41 del 31/01/2025 della Regione Abruzzo e perfezionare il citato schema di convenzione sia sotto il profilo giuridico sia sotto il profilo tecnico con ulteriori documenti elaborati dalla competente UOSD Sevizio e Territoriale e Ufficio Privacy quali allegati integranti e sostanziali al testo tipo di convenzione da approvarsi;

Evidenziato che la fattispecie di cui trattasi non comporterà oneri economici per l'Azienda;

Acquisito il parere tecnico favorevole in merito espresso dal Dirigente proponente, ai sensi della Legge 07 agosto 1990, n.241 e s.m.i che ne attesta la regolarità e la completezza;

Dato atto dell'attestazione resa dai competenti Dirigenti Responsabili in ordine alla regolarità amministrativo-contabile e tecnica del presente provvedimento nonché la registrazione al centro di costo e al conto economico dell'esercizio di competenza:

1. Dirigente proponente nella sua qualità di responsabile della UOC/UOSD/UOS competente;

2. Dirigente della UOC Controllo di Gestione;

3.Dirigente della UOC Bilancio e Gestione Economico-Finanziaria;

Acquisiti, per quanto di competenza, i pareri favorevoli espressi in merito dal Direttore Amministrativo d'Azienda e dal Direttore Sanitario d'Azienda;

DELIBERA

Per tutto quanto indicato e che qui si intende integralmente richiamato

1) **DI RECEPIRE** la DGR n. 41 del 31/01/2025 Convenzione tra la Regione Abruzzo e la regione Lombardia per il riuso del Software "CELIACHI@RL" (Sistema Regionale per l'erogazione dei prodotti dietetici senza glutine) adozione delle nuove modalità di erogazione a carico del SSN – Revisione della disciplina regionale di cui alle DGR 277/2005 E DGR 83/2020;

2) **DI APPROVARE** l'allegato schema di convenzione con tutti i suoi allegati, schema-tipo che sarà utilizzato per la stipula delle convenzioni tra l'Azienda e gli esercizi commerciali che vorranno convenzionarsi, aventi ad oggetto "erogazione prodotti senza glutine" in conformità a tutti i requisiti di legge richiesti;

3) **DI INDIVIDUARE**, quale referente delle convezioni di cui trattasi, il Direttore della UOSD Servizio Farmaceutico Territoriale, Dott.ssa Emanuela D'Angelo;

4) **DI DARE ATTO** che il presente provvedimento non comporta oneri economici aggiuntivi a carico della ASL di Pescara;

5) **DI DISPORRE** che la UOC Affari Generali e Legali provveda a trasmettere copia del presente provvedimento alla UOSD Servizio Farmaceutico Territoriale, all'Ufficio Privacy, alla UOC Bilancio e GEF, per tutti gli adempimenti di rispettiva competenza;

6) **DI DARE ATTO CHE** il presente provvedimento debba essere pubblicato nell'albo pretorio online della ASL ai sensi del D.Lgs. 33/2013;

7) **DI CONFERIRE** alla presente deliberazione immediata esecutività.

CONVENZIONE PER L'EROGAZIONE Dl PRODOTTI DIETETICI SENZA GLUTINE DA PARTE Dl ESERCIZI COMMERCIALI EX D.LGS.114/1998

TRA

L'Azienda Sanitaria Locale di Pescara, C.F./P.IVA 01397530682, con sede legale e domicilio fiscale in Pescara, Via Renato Paolini 47, rappresentata dal Direttore Generale, Dott. Michitelli Vero, domiciliato per la carica presso la sede della ASL, di seguito *Azienda*

E

La **Ditta/Società** _____, con sede legale in _____, _____ codice fiscale/Partita IVA 0_____, iscritta al registro delle imprese presso la Camera di Commercio di _____ al nr. _____, i cui esercizi commerciali denominati "Senza" sono ubicati in _____, _____

si conviene e si stipula quanto segue

ART.I - OGGETTO E FINALITA'

1 . Oggetto della presente convenzione è la erogazione di prodotti dietetici senza glutine - indicati nella sezione A2 del Registro Nazionale dei prodotti destinati ad un'alimentazione particolare di cui all'articolo 7 D.M. 08.06.2001, istituito presso la Direzione Generale della sicurezza degli alimenti e della nutrizione del Ministero della Salute - a favore di soggetti celiaci ed effettuata a carico del Servizio Sanitario Regionale per il tramite di esercizio commerciale rientrante nella tipologia e definizione resa dal D.Lgs.114/1998.

ART. 2 - OBBLIGHI DELLE PARTI

1 . La Ditta /Società _____, si impegna a:

- Garantire congruo assortimento dei prodotti siccome inseriti nel Registro Nazionale dei prodotti destinati ad un'alimentazione particolare: sezione 2 - di cui all'art. 7 D.M. 08.06.2001, istituito presso la Direzione generale della Sanità pubblica veterinaria degli alimenti della nutrizione del Ministero della Salute;
- Garantire la fruibilità dei buoni rilasciati a favore dei soggetti celiaci nei limiti del tetto di spesa ivi previsto, nel rispetto delle modalità definite dal D.M. 4 MAGGIO 2006 e s.m.i.;
- Trasmettere telematicamente il flusso di rendicontazione contenente il dettaglio di tutte le transazioni mensili (di tutte le erogazioni di alimenti per celiaci rimborsabili dal SSN effettuate dal primo all'ultimo giorno del mese) al sistema Celiachi@_RL.
- Il flusso deve essere necessariamente inviato entro il 10 del mese successivo a quello di riferimento, in quanto diversamente il sistema non lo accetta.
- Trasmettere alla ASL competente per territorio, sempre entro il 10 del mese successivo, anche la relativa fattura, emessa nel rispetto delle linee guida previste dal Ministero Economia e Finanza per il Nodo smistamento ordini – NSO.

2 . La A.S.L. di Pescara provvederà a

- Inserire l’esercizio commerciale nel sistema Celiachi@RL, che autorizza i documenti di credito dematerializzati con valore cumulativo mensile - ovvero buoni frazionabili - conformi ai tetti di spesa previsti dal D.M. 18 Agosto 2018, siccome distinti per sesso e per età.

ART. 3 - TRATTAMENTO DEI DATI

1. E' fatto divieto espresso alle Parti di utilizzare le informazioni acquisite in esecuzione della presente Convenzione per usi diversi da quelli previsti dalla Convenzione stessa, ovvero di cederle o consentirne la consultazione a terzi.

2. Ciascuna delle Parti si impegna ad osservare la massima riservatezza, a non divulgare, né utilizzare per alcuno scopo diverso da quello necessario per lo svolgimento delle attività previste, le informazioni di carattere sanitario, aziendale e più in generale le informazioni di volta in volta qualificate confidenziali e/o riservate che siano state prodotte dall'altra Parte nell'ambito delle attività di cui alla presente Convenzione.

3. Le Parti accettano di rivelare le informazioni confidenziali a Parti terze esclusivamente quando necessario per lo svolgimento delle attività contemplate nel presente atto, o previa esplicita autorizzazione della Parte interessata, o secondo quanto previsto dalla legge.

4. Nello svolgimento attività oggetto della presente Convenzione, Le Parti si impegnano al rispetto del Regolamento (Ue) 2016/679 recante il "Regolamento generale sulla protezione dei dati" (di seguito denominato "Regolamento"), del D.lgs. 30 giugno 2003, n. 196, come novellato dal D.lgs. 10 agosto 2018, n. 101 (di seguito denominato il "Codice della privacy") e di ogni altra disposizione e/o normativa, nazionale e/o comunitaria, applicabile in materia di protezione dei dati personali, nonché dei provvedimenti del Garante per la protezione dei dati personali (di seguito denominato il "Garante").

Considerato che i soggetti coinvolti nel flusso di informazioni risultano essere i seguenti:

a) la Asl di Pescara

b) gli esercizi commerciali di cui al DLgs 1 14/98 ubicati nel territorio della Asl di Pescara, si individua la seguente situazione che necessita di essere regolamentata nelle modalità che si specifica:

- il Soggetto di cui alla precedente lettera a) assume la qualifica di Titolare del trattamento e designerà, ai sensi dell'art 28 GDPR, gli esercizi commerciali di cui al precedente punto b), quale Responsabile del trattamento dei dati personali.

Il Dirigente Responsabile UOSD Farmacia Territoriale (in qualità di Satd della Asl di Pescara) garantirà la corretta applicazione della normativa in materia di protezione dei dati personali, con il supporto dell'Ufficio Privacy e Sicurezza delle Informazioni e la supervisione del D.P.O. aziendale. ln allegato alla presente Convezione si annovera il Modello di designazione a Responsabile del trattamento **(Allegato 1)** dei dati personali degli esercizi commerciali di cui al DLgs 1 14/98 ubicati nel territorio della Asl di Pescara (all. 1)

Il Responsabile del trattamento dei dati personali si impegnerà, a titolo esemplificativo e non esaustivo:

A. Ad adottare le misure di sicurezza adeguate previste dal Regolamento, Dal Codice della privacy e da ogni altra norma applicabile in tema di trattamento di dati personali;

B. A prestare idonea informativa agli interessati, nonché — ove previsto dal Regolamento e dal Codice della privacy — richiedere il relativo consenso;

C. A dare tempestivo riscontro alle istanze degli interessati, ai sensi degli artt. da 15 a 22 del Regolamento, nonché alle istanze o richieste da qualsiasi autorità legittimata, eventualmente collaborando con l'altra Parte nel caso esse abbiano ad oggetto operazioni di trattamento di competenza di entrambe;

D. A trattare i dati nel rispetto dei principi di legalità, proporzionalità e necessità previsti dal Regolamento.

ART. 4 - DURATA DELLA CONVENZIONE E RECESSO

1. La durata della convenzione è fissata in 1 anno decorrente dalla data di stipula della stessa.

2. Entrambe le parti possono recedere dalla convenzione in qualsiasi momento con un preavviso di almeno 30 (trenta) giorni solari - da comunicarsi all'altro contraente con comunicazione a mezzo raccomandata A.R. o Posta Elettronica Certificata (PEC)-specificando che in difetto la convenzione è prorogata per un ulteriore anno.

3. La convenzione cessa i suoi effetti nei confronti di entrambi i contraenti qualora intervengano modifiche normative o di carattere provvedimentale rese dall'Organo Centrale o dalla Regione Abruzzo, tali da rendere illegittima la prosecuzione del rapporto.

4. ln entrambi i casi di cui ai punti 2 e 3, la ditta/società _____ ha diritto al pagamento delle prestazioni eseguite nei mesi di effettivo servizio prestato e sino alla data di recesso o di entrata in vigore dell'atto normativo ovvero del provvedimento statale o regionale.

5. ln caso di mancato recesso, dopo il 2° anno, la convenzione si intende tacitamente prorogata di anno in anno, fatto salvo il diritto di recesso da esercitare nei modi e nei termini di cui al punto 2 del presente articolo.

ART. 5 - RISOLUZIONE DELLA CONVENZIONE

1. Nel caso in cui l'inadempimento da parte di ciascuna contraente, anche di uno solo degli obblighi assunti, si protragga oltre il termine di 15 (quindici) giorni - che verrà assegnato a mezzo raccomandata a.r. o Posta Elettronica Certificata (PEC) dalle parti medesime per porre fine all'inadempimento - quest'ultima ha la facoltà di considerare risolto di diritto il rapporto convenzionale;

2. ln ogni caso, si prevede che la ASL di Pescara possa risolvere di diritto il rapporto ai sensi dell'art. 1456 del cod.civ., previa dichiarazione da comunicarsi a controparte con raccomandata a.r. o Posta Elettronica Certificata (PEC), nei seguenti casi:

- Mancato adempimento delle prestazioni contrattuali a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nella presente convezione.
- Incorrendo la ditta/società nella violazione dell'art.3 della Convenzione (Obblighi di Riservatezza).

ART. 6 - FORO COMPETENTE

1. Per ogni controversia riguardante la validità, l'interpretazione, l'esecuzione o la risoluzione della presente convenzione e, comunque, relativa ad essa, le Parti preliminarmente si impegnano a comporre in via bonaria ogni eventuale conflitto e, solo nella impossibilità di raggiungere un accordo,

le Parti espressamente convengono di accettare, in via esclusiva, la giurisdizione del Tribunale di Pescara.

2. E' esclusa ogni competenza arbitrale.

ART.7 - NORMA Dl RINVIO

Per tutto quanto non previsto dalla presente convenzione valgono, in quanto applicabili, le disposizioni del codice civile in materia di contratti.

Sottoscritto con firma digitale ai sensi dell'art. 15, comma 2 bis, della Legge n. 241/1990 e secondo quanto disposto dal D.Lgs. 82/2005 e s.m.i e norme collegate

Letto, confermato e sottoscritto con firma digitale elettronica.

Per la Ditta/ Società	**Il Direttore Generale**
	Asl Pescara
Il Legale Rappresentante	Dott. Michitelli Vero

Allegato 1

www.asl.pe.it	**Regione Abruzzo – ASL 03 Pescara** **ACCORDO PER IL TRATTAMENTO DEI DATI** **Art. 28 Regolamento UE 2016/679**	**Accordo per il trattamento ex art. 28 GDPR** **PRY-RT-001** **Rev. 3.2** **Del 8/10/2024**

Sede Legale:

Via Renato Paolini, 45

65124 Pescara

P. IVA 01397530982

Accordo per il trattamento di dati personali con il Responsabile del Trattamento

Prot. n. _____ **Pescara, lì** _____

Spett.le _____

Via _____

Località _____

P.IVA _____

p.c. _____

_____

Oggetto: Accordo per il trattamento dei dati personali con il Responsabile del trattamento ai sensi dell'Art. 28 del Regolamento UE Generale sulla Protezione dei Dati n. 2016/679 (GDPR – General Data Protection Regulation) e della vigente normativa di settore.

In applicazione della Delibera ASL PE n. ___ del _____.

Il/La sottoscritta/o Dr./ssa _____, UOC/UOSD_____, 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. 2016/679 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;

Il presente accordo, ai sensi dell'art. 28 del Reg. UE 2016/679, integra e specifica gli obblighi derivanti dai documenti allegati alla Delibera sopra citata tra la ASL di Pescara (di seguito "ASL PE" o "Titolare") e l'impresa (di seguito il "Fornitore" o il "Responsabile") con particolare riferimento agli obblighi di protezione dei dati;

Il presente Accordo sulla Protezione dei Dati (di seguito anche ATD) si applica a tutte le attività svolte dal Responsabile nell'ambito del trattamento dei dati personali ai sensi del Regolamento UE 2016/679 (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), designate 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 della Asl di Pescara ed ogni comunicazione al Titolare dovrà essere trasmessa al seguente indirizzo PEC protocollo.aslpe@pec.it all'att.ne del Direttore Generale sopra indicato e per conoscenza all'Ufficio Privacy e Sicurezza delle Informazioni.

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

1) Il presente ATD si applica al trattamento dei dati personali svolto dall'Associazione 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 (ATD);
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 Responsabile corrisponde alla durata riportata nella Delibera sulla base di quanto indicato nel Contratto;
6) Nell'Ambito di Trattamento definito, il Titolare chiede al Responsabile di trattare i dati nel rispetto dei seguenti principi:
   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 ATD 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.

2) I dati personali trattati consistono, nei dati identificativi (solo il nome del paziente minorenne),

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 ATD. Il presente ATD 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 Responsabile 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 ATD dovrà essere trasmessa dalla ASL al Responsabile 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, Disciplinari, Materiale didattico per la formazione, ecc…

4) È fatto obbligo al Responsabile di:

a) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 del presente ATD;

b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32 del GDPR, come previsto dall'art. 5 del presente ATD;

c) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'art. 6 del presente ATD;

d) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 7 del presente ATD;

e) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'art.8 del presente ATD;

f) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'art.9 del presente ATD;

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 2016/679 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 ATD;

h) ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 2016/679, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall'art. 11 del presente ATD;

i) ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall'art. 12 del presente ATD;

j) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 del presente ATD;

k) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 del presente ATD;

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) comunicare immediatamente al titolare non oltre le 24 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. Ciò in applicazione sia dell'art. 33, par. 1 Reg. UE 2016/679 e dell'art. 1, par. 2 della L.90/2024

o) 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;

p) rispettare tutto quanto ulteriormente disciplinato dal presente ATD.

Articolo 4 – Riservatezza

1) Il Responsabile si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
2) Il Responsabile 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 Responsabile 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 Responsabile si impegna a mettere in atto le misure tecniche e organizzative identificate dal Titolare e indicate nell'Allegato 2 al presente ATD.

3) In caso di non completa attuazione delle misure previste nell'Allegato 2, il Responsabile, entro 30 giorni dalla sottoscrizione del presente ATD, predispone un piano di implementazione finalizzato a colmare le eventuali lacune e la cui scadenza verrà concordata con il SATD, sentito il parere del DPO, con la collaborazione dell'Ufficio Privacy/Protezione Dati.

4) L'allegato 2 al presente ATD, ai sensi dell'art. 28.3 lett. h) del Regolamento, verrà preso a riferimento come parte *delle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato*.

5) Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative previste nell'Allegato 2 al presente ATD, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva idonea comunicazione, via PEC (protocollo.aslpe@pec.it), al Titolare e, per conoscenza, al Soggetto Autorizzato con Delega sottoscritto e all'Ufficio Privacy e Sicurezza delle Informazioni, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure di cui all'Allegato 2 al presente accordo.

Articolo 6 – Assistenza

1) Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nel Contratto allegato alla Delibera, esso 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 Responsabile 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 ATD) 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 ATD, e delle informazioni di volta in volta messe a disposizione, il Responsabile 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, alla cessazione del Contratto stesso, dovranno essere restituiti al Titolare entro un termine massimo di 30 giorni dalla cessazione dei servizi.

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 o del sub-responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile (o il sub-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 24 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. Ciò in applicazione sia dell'art. 33, par. 1 Reg. UE 2016/679 e dell'art. 1, par. 2 della L.90/2024

2) Il Responsabile si impegna inoltre, ai sensi dell’art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua 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 essere trasmessa all’att.ne del Titolare mediante comunicazione a mezzo PEC all’indirizzo protocollo.aslpe@pec.it. Tale comunicazione dovrà essere inviata per conoscenza anche al DPO e all’Ufficio Privacy e Sicurezza delle Informazioni.

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 propria disposizione, a fornire al Titolare ogni elemento utile all’effettuazione della valutazione di impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment), 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 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 previsti dal Contratto allegato alla Delibera.

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 (art. 28.2/28.4). 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 ATD 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 (indirizzo PEC indicato nelle premesse e nell'art. 8 del presente ATD), 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 15 giorni prima dell'operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 15 giorni dalla ricezione della comunicazione da parte del Responsabile.

3) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzo PEC indicato nelle premesse e nell'art. 8 del presente ATD), 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 designati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 15 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:
   1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; o
   2. 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 dovrà essere inviato al Titolare, all'indirizzo PEC protocollo.aslpe@pec.it, entro 30 giorni dalla sottoscrizione del presente ATD. Tale comunicazione dovrà essere inviata per conoscenza anche all'Ufficio Privacy e Sicurezza delle Informazioni.

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 ATD.

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) nomini uno o più Amministratori di Sistema (di seguito anche "AdS"), il Responsabile si impegna a:
   1. 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;
   2. 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;
   3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
   4. comunicare periodicamente (almeno una volta l'anno, entro il 31/12) 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;
   5. 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;
   6. verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
   7. conservare, ove di competenza, 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);
   8. 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 ATD.

2) Il titolare effettuerà verifica delle dichiarazioni rese nel presente accordo dal responsabile per tutto il periodo di vigenza contrattuale, e se del caso anche prima dell'avvio del contratto stesso. L'inosservanza delle prescrizioni presenti nel presente accordo potrà comportare la risoluzione del contratto fra le parti ed ogni conseguenza per quanto previsto dalla normativa vigente.

3) 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.

4) Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

5) Il Responsabile si impegna altresì a:
   1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e relativi adempimenti eseguiti) ed alle conseguenti risultanze;
   2. 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;
   3. 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;
   4. 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 o ritenga a suo parere che il trattamento dei Dati Personali violi la normativa vigente o presenti, comunque, rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato.

6) 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 – Descrizione dettagliata dell'attività

Al fine di valutare l'attività che si intende adeguare alla normativa vigente in materia di protezione dei dati personali, *si richiede al SATD (Direttore/Dirigente della UO richiedente) di descrivere brevemente il contesto* in cui avviene il trattamento. Le informazioni fornite serviranno anche per la redazione dei documenti necessari a soddisfare i requisiti cogenti posti dalla legge, ovvero il registro dei trattamenti del titolare e l'informativa del trattamento. I documenti di riferimento sono la Procedura per la Gestione di Accordi, Nomine e Designazioni rev. 1.1 - marzo 2019 (Del. 427 del 4/4/2019), Procedura per la gestione della conformità in materia di protezione dei dati personali nelle procedure di acquisizione di lavori, servizi e forniture rev. 1.0 - marzo 2020 (Circolare 1/2020), disponibili su asl.pe.it/datipersonali . Per la consultazione dei riferimenti normativi citati si rimanda al seguente link https://www.garanteprivacy.it/garante/document?ID=6264597

Cod.	Voce	Descrizione
1	**AMBITO DI TRATTAMENTO**	
1.1	Descrivere l'attività che si intende effettuare, in ogni fase, nel suo completo ciclo di vita	

	Art. 30, par. 1, lett. a) GDPR	
1.2	Descrivere quali attività di trattamento vengono complessivamente svolte da tutti i soggetti coinvolti Artt.4, par.2, 30, par. 1, lett. a) GDPR	[ ] Raccolta [ ] Registrazione [ ] Organizzazione [ ] Strutturazione [ ] Conservazione [ ] Adattamento o Modifica [ ] Estrazione [ ] Consultazione [ ] Uso [ ] Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione [ ] Raffronto o Interconnessione [ ] Limitazione [ ] Cancellazione o Distruzione [ ] Trasferimento verso un paese terzo o una organizzazione internazionale
1.3	Quali sono le finalità del trattamento? Art. 30, par. 1, lett. b) GDPR	[ ] a) Diagnosi e cura [ ] b) Ricerca scientifica [ ] c) Gestione del personale [ ] d) Obbligo legale (indicare la legge):_____ [ ] e) Altro:_____
1.4	Quali sono le categorie delle persone interessate dal trattamento? (es. assistiti, clienti, fornitori, dipendenti) Art. 30, par. 1, lett. c) GDPR	[ ] a) Dipendenti/Consulenti [ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali) [ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori [ ] d) Soggetti che ricoprono cariche sociali [ ] e) Beneficiari o assistiti [ ] f) Assistiti [ ] g) Minori [ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) [ ] i) Altro:_____
1.5	Quali sono le categorie di dati personali trattati? (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati)	[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) [ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)

	Art. 30, par. 1, lett. c) GDPR	[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…) [ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) [ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…) [ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza [ ] g) Dati di profilazione [ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) [ ] i) Dati relativi all'ubicazione [ ] l) Dati che rivelano l'origine razziale o etnica [ ] m) Dati che rivelano le opinioni politiche [ ] n) Dati che rivelano le convinzioni religiose o filosofiche [ ] o) Dati che rivelano l'appartenenza sindacale [ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale [ ] q) Dati relativi alla salute [ ] r) Dati genetici [ ] s) Dati biometrici [ ] t) Altro. Indicare:
1.6	Chi sono tutti i soggetti coinvolti in ogni fase, nel suo completo ciclo di vita, del trattamento? (es. fornitori, altri enti convenzionati) Art. 30, par. 1, lett. d) GDPR	[ ] a) Destinatari interni (indicare l'UO di appartenenza) _____ [ ] b) Fornitori (indicare la denominazione) _____ [ ] c) Altri Enti (indicare la denominazione) _____ [ ] d) Altro: _____
1.7	Qual è la durata prevista del trattamento? (es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione") Art. 30, par. 1, lett. f) GDPR	[ ] a) 10 anni dalla cessazione del trattamento principale [ ] b) Come da massimario di scarto aziendale [ ] b) Altro (indicare la durata) :_____
1.8	Dove vengono trattati i dati? Art. 30, par. 1, lett. e) GDPR	[ ] a) All'interno dell'Unione Europea [ ] b) Altro (indicare la località) :_____
1.9	Specificare la natura e le modalità del trattamento. (es. trattamento dati in formato cartaceo, trattamento informatizzato con archivio digitale)	[ ] a) Trattamento su supporti cartacei (riportare il dettaglio in descrizione al punto 1.1) [ ] b) Trattamento informatizzato (riportare il dettaglio in descrizione al punto 1.1)

	Art. 24, 25, 32 GDPR	
1.10	Nel caso in cui i dati personali non siano raccolti presso l'Interessato, specificare la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico Art. 14, par. 2, lett. g) GDPR	[ ] a) I dati vengono forniti direttamente dalla persona interessata [ ] b) I dati della persona interessata vengono forniti da un altro soggetto (indicare la denominazione) :_____
1.11	Quali strumenti vengono utilizzati nel trattamento? Art. 24, 25, 32 GDPR	[ ] a) Dispositivo/Apparecchiatura (indicare la denominazione)_____ [ ] b) Sistema (indicare la denominazione) _____ [ ] c) Software (indicare la denominazione) _____ [ ] d) Altro (indicare la denominazione) _____
1.12	Quali misure di sicurezza sono presenti nel trattamento? Art. 24, 25, 32 GDPR	[ ] a) I dati sono trattati in misura minima [ ] b) La comunicazione dei dati avviene in modo protetto [ ] c) I fornitori hanno fornito una DPIA – Valutazione d'impatto [ ] d) I fornitori hanno la certificazione ISO27001 [ ] e) I fornitori hanno designato il Responsabile della Protezione dei Dati [ ] f) Altro (indicare quali) _____

Articolo 16 – Recapiti della persona referente commerciale/amministrativo e del Responsabile della Protezione dei Dati (DPO) del fornitore

Nome e Recapito telefonico del referente	
Indirizzo E-mail del referente	
Indirizzo PEC del referente	
Recapito del DPO [(1)]	

[(1)] ove il responsabile della protezione dei dati non sia stato designato ai sensi dell'art. 37 del GDPR, il responsabile del trattamento allega al presente documento copia del documento attestante le valutazioni effettuate a tal proposito

Articolo 17 – Soggetti sub-responsabili (sub-fornitori)

ID	Ragione sociale	Sede legale	E-mail/PEC	Recapito del DPO	Ambito di trattamento
1					
2					
3					
Ultimo aggiornamento dell'allegato			_____ /_____ /_____		

[ ] Il responsabile del trattamento NON affida a sub-fornitori attività che implichino trattamento di dati personali

Articolo 18 – Amministratori di sistemi

ID	Nome e Cognome [1]	Ragione Sociale [2]	Recapito E-mail/Telefono	Sistemi Amministrati
1				
2				
3				
4				
Ultimo aggiornamento dell'elenco			____/____/____	

[1] se soggetti autorizzati ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03 e dell'art. 29 del Reg. UE 2016/679
[2] se soggetti individuati quali sub-responsabili ai sensi dell'art. 28, parr. 2 e 4, del Regolamento UE 2016/679

[ ] Il responsabile del trattamento NON svolge attività che implichino il ruolo di Amministratore Di Sistema

Articolo 19 – Principi, Diritti e Misure Tecniche e Organizzative – Requisiti/Schede di Audit

Si indicano, in base alla loro applicabilità in relazione al servizio erogato per conto del Titolare, i principi di trattamento, le misure di sicurezza e i diritti degli interessati, secondo le indicazioni del Regolamento UE

2016/679, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) unitamente alle misure di sicurezza previste, per i quali il responsabile si impegna con la sottoscrizione del presente atto.

Le indicazioni fornite nel presente allegato relative alle misure di sicurezza sono estrapolate dalle Linee Guida ENISA relative alla sicurezza dei trattamenti di dati personali: esse dovranno essere riportate all'interno del Registro dei Trattamenti del Responsabile.

1) Principi di Trattamento e Diritti degli Interessati

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)
A.1	Art. 5.1.b – Misure per garantire la limitazione della finalità del trattamento (dati non utilizzati per altre finalità)
A.2	Art. 5.1.c – Misure per garantire la minimizzazione dei dati del trattamento
A.3	Art. 5.1.d – Misure per garantire la esattezza/qualità dei dati
A.4	Art. 5.1.e – Misure per garantire la limitazione della conservazione
A.5	Art. 15 – Misure per garantire il diritto di Accesso dell'interessato
A.6	Art. 16 – Misure per garantire il diritto di Rettifica
A.7	Art. 17 – Misure per garantire il diritto alla Cancellazione ("Oblio") – ove applicabile
A.8	Art. 18 – Misure per garantire il diritto alla Limitazione del Trattamento
A.9	Art. 19 – Misure per garantire l'obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento
A.10	Art. 20 – Misure per garantire il diritto alla portabilità dei dati – ove applicabile
A.11	Art. 21 – Misure per garantire il diritto di Opposizione
A.12	Art. 22 - Misure per garantire la sicurezza in caso di processo decisionale automatizzato relativo alle persone fisiche, compresa la *profilazione*

2) Misure di Sicurezza

Il perimetro di sicurezza definito come ambito di applicazione delle misure di sicurezza di seguito elencate è costituito dal servizio effettuato dal Responsabile per conto della ASL di Pescara; di conseguenza le seguenti misure sono applicabili all'organizzazione, alle informazioni/dati, agli strumenti HW, SW e di rete ed al personale coinvolti nell'erogazione del servizio contrattualizzato.

Le presenti misure di sicurezza verranno utilizzate quale riferimento per l'esecuzione degli audit previamente concordati.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Politiche di sicurezza e procedure per la protezione dei dati personali	1.1	Il Responsabile deve disporre di una propria regolamentazione (o politica di sicurezza) in materia di protezione dei dati personali conforme alla normativa vigente e che disciplini i servizi erogati per conto del Titolare.
	1.2	La regolamentazione di cui al punto precedente deve essere riesaminata e aggiornata almeno su base annuale.
	1.3	La regolamentazione deve essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.
	1.4	La regolamentazione deve disciplinare almeno i seguenti punti: ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili e sub-responsabili del trattamento dei dati e per le altre terze parti coinvolte nel trattamento dei dati personali.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Ruoli e responsabilità	2.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.
	2.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
	2.3	Deve essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
Riservatezza del personale	3.1	Il Responsabile deve garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di attivazione del Servizio/Contratto.
	3.2	Prima di assumere i propri compiti, il personale del Responsabile deve essere invitato a riesaminare e concordare la Regolamentazione di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
Formazione	4.1	Il Responsabile deve garantire che tutto il personale sia adeguatamente formato sui controlli di sicurezza previsti per il servizio e per gli eventuali sistemi informatici ad esso correlati. Il personale coinvolto nel trattamento dei dati personali deve inoltre essere adeguatamente informato e periodicamente aggiornato in merito ai requisiti in materia di protezione dei dati e agli obblighi previsti dalla normativa vigente attraverso regolari campagne di sensibilizzazione.
	4.2	Il Responsabile deve disporre programmi di formazione (relativi alla protezione dei dati personali e alla sicurezza delle informazioni) strutturati e regolari per il proprio personale, compresi programmi specifici per l'inserimento di eventuali nuovi arrivati (es.: job rotation, nuove assunzioni, ecc...).
Politica controllo accessi	5.1	Specifici diritti di accesso devono essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
	5.2	Deve essere definita una politica di controllo degli accessi. Nel documento l'organizzazione deve determinare le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.
	5.3	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata.
Controllo accessi e autenticazione	6.1	Ove fornita dall'Organizzazione, deve essere attuata la politica di controllo accessi applicabile a tutti gli utenti che accedono ai sistemi IT, con particolare riguardo agli aspetti relativi alla creazione, approvazione, riesame ed eliminazione degli account.
	6.2	L'uso di account generici (non personali) deve essere evitato. Nei casi in cui ciò sia necessario, l'utilizzo deve essere autorizzato dal referente dell'Organizzazione. Qualora tale autorizzazione fosse fornita, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
	6.3	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, deve essere presente un meccanismo di autenticazione che consenta l'accesso che sia in linea con la politica di controllo degli accessi ove fornita dall'Organizzazione. Come minimo deve essere utilizzata una combinazione di user-id e password.
	6.4	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, il sistema di controllo degli accessi deve essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano i criteri definiti al punto precedente.
	6.5	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio deve essere possibile configurare i seguenti parametri relativi alle password: complessità, maximum age, password history, lunghezza e il numero di tentativi di accesso non riusciti accettabili. I criteri dovranno essere concordati con il referente dell'Organizzazione (in base alla politica di controllo accessi).
Gestione risorse e degli asset	7.1	Deve essere predisposto un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete), in funzione di quanto applicabile al servizio esternalizzato. Il compito di mantenere e aggiornare il registro deve essere esplicitamente assegnato.
	7.2	Le risorse IT all'interno del registro essere riesaminate e aggiornate regolarmente.
	7.3	I ruoli che hanno accesso alle risorse devono essere definiti e documentati. In particolare devono essere definite le responsabilità in relazione alle risorse.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Sicurezza fisica	8.1	Il perimetro fisico dei locali in cui è ospitata l'infrastruttura IT utilizzata a fini di erogazione del servizio o vengono effettuati trattamenti di dati personali del Titolare deve essere accessibile esclusivamente a personale esplicitamente autorizzato da parte del Responsabile.
	8.2	Il personale autorizzato all'accesso ai locali di trattamento o ai locali in cui è ospitata l'infrastruttura IT per l'erogazione del servizio deve essere dotato di strumenti di identificazione personali (es. badge identificativi, PIN personali).
	8.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Deve essere mantenuto e monitorato in modo sicuro un registro fisico o una traccia elettronica del controllo di tutti gli accessi.
	8.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.
	8.5	Dovrebbero essere predisposte barriere fisiche per impedire l'accesso fisico non autorizzato.
	8.6	Le aree dei locali non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate.
	8.7	Nella sala server devono essere predisposti opportuni sistemi antincendio automatici, sistemi dedicati di climatizzazione e gruppi di continuità (UPS) che garantiscano l'erogazione sicura del servizio secondo quanto stabilito contrattualmente.
	8.8	Il personale di supporto esterno deve avere accesso limitato alle aree protette.
Change management	9.1	L'organizzazione deve adottare un processo di cambiamento che consenta di assicurarsi che tutte le modifiche al sistema/servizio siano opportunamente registrate (anche con eventuali aggiornamenti dell'inventario delle risorse) e monitorate.
	9.2	Ogni Cambiamento al sistema/servizio deve essere previamente segnalato al referente interno dell'organizzazione (committente) e da questi autorizzato. Nella segnalazione devono essere documentati: gli estremi del cambiamento (es.: cambiamento di versione), le tempistiche, eventuali prescrizioni aggiuntive che prevedano azioni da adottare prima che il cambiamento sia operativo (es.: formazione utenti).
	9.3	Lo sviluppo del software deve essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali in produzione. Quando è necessario eseguire i test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, il fornitore deve predisporre specifiche procedure per la protezione dei dati personali utilizzati nei test.
Logging e monitoraggio	10.1	I log devono essere attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	10.2	I log devono essere registrati e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica fonte temporale di riferimento (server NTP).
	10.3	È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.
	10.4	Non deve essere possibile la cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio effettuato per la rilevazione di attività insolite.
	10.5	Deve essere configurato un sistema di monitoraggio per l'elaborazione dei log e la produzione di rapporti sullo stato del sistema e notifica di potenziali allarmi.
Protezione dal malware	12.1	Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
Backup	14.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità; devono essere definite e documentate le strategie di backup da applicare ai dati in maniera coerente con il livello di criticità (RPO) dei servizi a cui afferiscono
	14.2	Ai backup deve essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	14.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	14.4	Le strategie di backup definite devono essere completate regolarmente.
	14.5	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	14.7	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.
	14.8	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare dei dati.
Sicurezza Server e Database	15.1	I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	15.2	I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione.
	15.3	Nei sistemi utilizzati per l'erogazione del servizio, devono essere considerate soluzioni di crittografia per i dati at rest, in transit e in use. Qualora non ritenute applicabili, deve essere data adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati
	15.4	Nei sistemi utilizzati per l'erogazione del servizio, ove possibile, devono essere applicate tecniche di pseudonimizzazione attraverso la separazione dei dati dagli identificatori al fine di evitare il collegamento diretto con l'interessato. In caso non fosse possibile, deve essere fornita adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati.
Network/Communication security	16.1	Deve essere predisposta e monitorato il rispetto di una policy per la Sicurezza di Rete (Network Security Policy) e per la gestione delle Comunicazioni Sicure (Network Communication Security) che preveda l'adozione di misure di cifratura delle comunicazioni nell'ambito dei processi di trattamento effettuati (TLS/Https, VPN, SSH, ecc…).
Sicurezza desktop/laptop/mobile	17.1	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza.
	17.2	Le applicazioni anti-virus e le relative signatures devono essere configurate regolarmente in maniera continuativa.
	17.3	Gli utenti non devono avere i privilegi per installare applicazioni software non autorizzate o disattivare applicazioni autorizzate
	17.4	I sistemi utilizzati per l'erogazione del servizio, devono disporre di un timeout di sessione nel caso in cui l'utente non sia stato attivo per un determinato periodo di tempo (max 10 min).
	17.5	Gli aggiornamenti critici di sicurezza rilasciati dalle case produttrici di software di sistema devono essere installati regolarmente.
	17.6	Non è consentito il trasferimento di dati personali dai Database dei sistemi aziendali alle workstation utilizzate a fini di assistenza tecnica, se non previa esplicita autorizzazione del Responsabile dei Sistemi Informativi. I dati temporaneamente memorizzati devono essere cancellati alla fine della sessione di lavoro.
	17.7	Non deve essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	17.8	Deve essere abilitata la crittografia dei dischi delle postazioni di lavoro/laptop/device mobili utilizzate nell'ambito dell'erogazione del servizio
Dispositivi portatili	18.1	Le procedure di gestione dei dispositivi mobili e portatili devono essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	18.2	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati: non è consentito l'utilizzo di dispositivi personali, salvo eventuali specifiche autorizzazioni.
	18.3	I dispositivi mobili devono essere soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali (client).
	18.4	Il Responsabile deve individuare e comunicare al Titolare un proprio referente a cui attribuire la responsabilità della gestione dei dispositivi mobili e portatili utilizzati nell'ambito dell'erogazione del servizio.
	18.5	Il Responsabile deve essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso, nel caso in cui questo sia utilizzato nell'ambito dell'erogazione del servizio.
	18.6	In caso di utilizzo promiscuo dei dispositivi mobili (fini di erogazione del servizio al titolare e fini privati) deve essere prevista, mediante opportuni software containers sicuri, la separazione dell'uso privato dall'uso aziendale del dispositivo.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	18.7	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
Sicurezza del ciclo di vita delle applicazioni	19.1	Lo sviluppo degli applicativi deve essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID.
Sub-responsabile del trattamento	20.1	Il Responsabile ed i suoi sub-responsabili adottano le linee guida e le procedure relative al trattamento dei dati personali contenute nell'atto di designazione e nei suoi allegati (tra cui il presente documento).
	20.2	Il Responsabile del Trattamento deve osservare le indicazioni fornite nell'atto di designazione in caso di violazione di dati personali e nelle presenti misure di sicurezza.
	20.3	Il Responsabile deve sottoscrivere l'atto di designazione in cui sono contenuti requisiti formali e obblighi. Il Responsabile del trattamento deve, in risposta, fornire prove documentate sufficienti di conformità (es.: certificazioni di sicurezza, schede tecniche relative alle misure di sicurezza adottate per il servizio/sistema): in caso alternativo, verrà adottata una specifica politica di auditing.
	20.4	Il Responsabile dovrebbe verificare regolarmente la conformità del sub-responsabile al livello concordato di requisiti e obblighi.
	20.5	Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione.
Gestione degli incidenti / Violazione dei dati personali	21.1	Il Responsabile deve predisporre un proprio piano di risposta agli incidenti con procedure dettagliate che preveda la comunicazione al titolare (committente), secondo le indicazioni fornite nell'atto di designazione, al fine di garantire una risposta efficace e ordinata agli incidenti e violazioni relativi ai dati personali.
	21.2	Le violazioni dei dati personali, di competenza del Titolare, devono essere segnalate immediatamente alla Direzione. In qualità di Responsabile devono essere adottate specifiche procedure di supporto al Titolare per la notifica e la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
	21.3	La procedura di gestione delle violazioni di cui al punto precedente, deve essere documentata: essa deve includere un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.
	21.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.
Business Continuity	22.1	Il Responsabile deve predisporre un proprio Piano di Continuità Operativa (BCP - Business Continuity Plan) in relazione all'erogazione dei servizio, in linea con quanto previsto dall'Organizzazione (Committente). Tale Piano deve stabilire procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del servizio (ad es.: in caso di incidente / violazione dei dati personali o interruzione del servizio).
	22.2	Il Piano di Continuità Operativa indicato al punto precedente deve includere azioni chiare e assegnazione di ruoli.
	22.3	Il Piano di Continuità Operativa deve essere in linea con il livello di qualità del servizio da garantire all'Organizzazione (Committente), con particolare riguardo alla sicurezza dei dati personali dei processi fondamentali di erogazione.
Cancellazione/eliminazione dei dati	23.1	I supporti di memorizzazione da dismettere devono essere distrutti fisicamente; in caso in cui ciò non sia possibile (es.: per indicazioni contrattuali relative all'assistenza dei dispositivi), prima della loro eliminazione (o riconsegna al fornitore) devono essere sottoposti a tecniche di distruzione dei dati (es.: ripetute operazioni di sovrascrittura con tecniche di clearing/purging).
	23.2	La distruzione di documenti deve avvenire mediante opportuni dispositivi di triturazione.
	23.3	Se sono utilizzati servizi di terzi per eliminare in modo sicuro i supporti di memorizzazione o documenti cartacei, è necessario stipulare uno specifico contratto di servizio e produrre un formale attestato di distruzione.

Articolo 20 – 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.
2) Gli allegati al presente ATD 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) La mancata sottoscrizione del presente accordo non consentirà di dare attuazione di quanto previsto nel Contratto.
4) Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/12 di ogni anno.
5) Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente ATD, costituisce una violazione del Contratto, di cui il presente ATD 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 dalla normativa vigente.
6) Il presente Accordo sulla Protezione dei Dati Personali, comprensivo dei relativi allegati, deve essere restituito dal SATD al protocollo, opportunamente sottoscritto digitalmente da entrambe le parti.
   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)	Per ricezione ed integrale accettazione del Responsabile
_____	_____

Il Dirigente Amministrativo, con la presente sottoscrizione, attesta la regolarità tecnica e amministrativa nonché la legittimità del provvedimento

Il Dirigente Amministrativo
Manuela Fazia
firmato digitalmente

Il Direttore dell'UOC Controllo di Gestione attesta che la spesa risulta corrispondente al bilancio di previsione dell'anno corrente.

Il Direttore

firmato digitalmente

Il Direttore dell'UOC Bilancio e Gestione Economica Finanziaria attesta che la spesa risulta imputata sulla voce di conto del Bilancio n.
Anno

Il Direttore

firmato digitalmente

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

IL DIRETTORE AMMINISTRATIVO
Dott. Francesca Rancitelli
firmato digitalmente

Parere favorevole

IL DIRETTORE SANITARIO
Dott. Rossano Di Luzio
firmato digitalmente

IL DIRETTORE GENERALE
Dott. Vero Michitelli
firmato digitalmente

Deliberazione n. 564 **del** 14/04/2025 **ad oggetto:**

RECEPIMENTO DGR N. 41 DEL 31/01/2025 DELLA REGIONE ABRUZZO E APPROVAZIONE SCHEMA TIPO CONVENZIONE

CERTIFICATO DI PUBBLICAZIONE

- Si attesta che il presente atto viene pubblicato, in forma integrale, all'ALBO ON LINE dell'ASL di Pescara (art. 32 L. 69/09 e s.m.i.), in data 14/4/2025 per un periodo non inferiore a 15 giorni consecutivi.

Atto soggetto al controllo della Regione (art. 4, co. 8 L. 412/91): NO

Il Funzionario Incaricato