DELIBERAZIONE DEL DIRETTORE GENERALE

n° 253 del - 8 NOV. 2019

OGGETTO: Regolamento UE 679/2916 relativo alla protezione dei dati personali (GDPR). Adozione sistema di Gestione della Protezione Dati e approvazione Regolamento Aziendale.

Il DIRETTORE GENERALE, dott. Roberto Testa, nominato con atto di Giunta Regionale d'Abruzzo n° 542 del 11.09.2019, su conformi istruttoria e proposta dell'Ufficio Privacy, in data 31.10.2019, adotta la presente deliberazione.

PREMESSO che:

- a far data dal 25 maggio 2018 è divenuto definitivamente applicabile in tutti i Paesi UE il Regolamento n.679/2016, di seguito anche GDPR, relativo " alla protezione delle persone fisiche con riguardo al trattamento dei dati personali…" approvato nella seduta del Parlamento europeo e del Consiglio dell'UE del 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016;
- in data 4 settembre 2018 è stato pubblicato in Gazzetta Ufficiale il decreto legislativo 10 agosto 2018, n. 101 recante le " Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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…" con il quale il Legislatore Italiano ha adeguato il D.lgs 30 giugno 2013, n.196 - " Codice in materia di protezione dei dati personali " – alle disposizioni di detto Regolamento;

ATTESO che:

- il principio cardine introdotto dal GDPR, ovvero il principio di "responsabilizzazione" *(c.d. accountability)*, pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dati, con l'adozione di misure tecniche e organizzative, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o *compliance* nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR;

- nell'ottica del legislatore europeo, quindi, in materia di privacy, ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli risponde delle proprie e azioni e deve essere in grado, in qualsiasi momento di darne conto verso l'esterno;

DATO ATTO che questa Azienda (in qualità di Titolare) in linea con il succitato principio di *"accountability"*, al fine di dotarsi degli idonei strumenti tecnico-organizzativi per adeguare la propria gestione alla nuova normativa in materia di Protezione dei Dati Personal, ha provveduto :

- con deliberazione n 2141 del 30 Novembre 2017, ad aderire all'Accordo Quadro Consip SPC2 per la fornitura di servizi di connettività informatica e servizi connessi e con successiva sottoscrizione del relativo contratto esecutivo, registrato al protocollo generale n 0236799 del 27.12.2017, ad affidare a Fastweb Spa la fornitura dei servizi oggetto del predetto accordo Quadro per la durata anni quattro;
- con deliberazione n 831 del 26 Aprile 2018 e successiva modifica n 968 del 16 maggio 2019, ad istituire un apposito ufficio denominato "Ufficio Privacy", collocato in staff alla Direzione Strategica, con compiti operativi cui demandare l'implementazione, il coordinamento ed il controllo della attività previste dalla nuova normativa europea;
- con deliberazione n. 1575 del 17.08.2018, a prendere atto del contratto di subappalto in essere tra Fasweb spa e INFOTEAM srl, debitamente autorizzato da Consip, per la fornitura dei servizi di supporto specialistico (STRA-1 e STRA-2) compresi nel contratto esecutivo summenzionato e ad approvare il piano operativo di adeguamento al GDPR da realizzarsi in un arco temporale di quattro anni;
- con deliberazione n 1266 del 17 Luglio 2019, a seguito della risultanze della procedura di gara, su piattaforma MEPA, per l'acquisizione di beni e servizi sotto soglia Comunitaria, ad affidare il servizio di Responsabile per la protezione dei dati (RPD) alla società NBCONSULTING Srl che in Azienda succede nel suo compito alla Società Creasys precedentemente designata (giusti provvedimenti n.1009/2018, n.13/2019 e n. 87/2019);

DATO ATTO, inoltre, che per adempiere alle novità introdotte dal GDPR, in linea con il piano di lavoro allegato alla succitata deliberazione n. 1575/2018, coinvolgendo i Direttori/Responsabili delle Strutture Organizzative aziendali, sono state espletate attività di formazione sulla normativa in materia di Protezione dei dati personali e di rilevazione dei trattamenti e criticità, propedeutiche alla predisposizione di un Regolamento per il trattamento e la tutela dei dati personali all'interno della Azienda, del Registro dei Trattamenti, delle Procedure organizzative (es.: Procedura per la gestione delle Violazioni dei Dati Personali), della modulistica (es.: modelli di informative e consensi), degli atti di nomina e designazione per interni ed esterni alla struttura del Titolare:

DATO ATTO, altresì, che in attuazione della nota del Direttore Generale pro tempore, prot. n. 0240947 del 06.12.2018, è stato dato avvio al processo di nomina dei Soggetti Autorizzati con Delega al Trattamento (ex responsabili interni del trattamento) a seguito della deliberazione n.2155 del 23.11.2018 e s.m.i. secondo le indicazioni dell'allora Responsabile della Protezione Dati, identificati nei seguenti ruoli:

- Direttore Sanitario e Direttore Amministrativo
- Direttori di Dipartimento
- Direttori di UOC (Unità Operativa Complessa)
- Responsabile di UOSD (Unità Operativa Semplice Dipartimentale)

ESAMINATO l'allegato "*Regolamento aziendale per protezione dei dati personali* " predisposto in schema con il coordinamento dell'Ufficio Privacy, che consta di n.31 (trentuno) articoli e dei seguenti n.7 (sette) allegati:

A- Registro delle attività di Trattamento
B- Piano di Sicurezza
C- Procedura di Gestione delle Violazioni di Dati Personali
D- Procedura per l'Esercizio dei Diritti degli Interessati
E- Procedura per la Gestione delle Informative e Consensi
F- Procedura di Gestione di Accordi, Nomine e Designazioni
G- Clausola di Garanzia da inserire nei contratti con Terzi

DATO ATTO, infine, che il documento di cui al superiore capoverso è stato validato dal Responsabile per la Protezione dei dati Personali (RPD/DPO);

RITENUTO, pertanto, necessario provvedere all'approvazione del Regolamento suddetto;

DELIBERA

Per le ragioni esposte in narrativa, che qui si intendono integralmente trascritte:

1. di approvare il documento denominato "*Regolamento Aziendale per la protezione dei dati personali*", allegato al presente atto quale parte integrale e sostanziale, costituito da n.31 articoli e da n.7 allegati;
2. di precisare che le procedure unite al presente Regolamento sono integrate e completate dalla relativa modulistica (anch'essa allegata), necessaria per gli adempimenti previsti dalla normativa in materia di privacy;
3. di disporre che i documenti allegati all'anzidetto Regolamento denominati " *Registro delle attività di Trattamento*" e " *Piano di Sicurezza*" non vengano pubblicati sull'Albo Pretorio per ragioni di riservatezza ;

4. di dare mandato all'Ufficio Privacy di pubblicare l'allegato Regolamento (con le eccezioni su indicate) sul sito internet aziendale – nell' apposita sezione denominata "Protezione Dati Personali" - nonché sull'Intranet Aziendale, così da garantirne la più ampia diffusione;

5. di dare mandato, inoltre, al suddetto Ufficio di provvedere ad una capillare divulgazione interna di questo Regolamento Aziendale con apposite sessioni formative, mirate ad aumentare il livello di conoscenza della norma e di sensibilizzazione in materia di protezione dei dati personali e della libera circolazione degli stessi;

6. di dichiarare il presente atto immediatamente esecutivo in applicazione dell'art.21 quater della legge 7 agosto 1990 n.241;

7. di inviare questa deliberazione all'Ufficio proponente e alla UOC Affari Generali e Legali.

Si attesta che il presente provvedimento è stato proposto previa istruttoria dell'ufficio competente, ai sensi del capo II della Legge 07.08.1990 n° 241 e s.m.i..

L'ISTRUTTORE
(dott. Cesare Marco Di Girolamo)

IL RESPONSABILE DELL'UFFICIO
(dott.ssa Emanuela Modestini)

In relazione all'art. 3 comma 7 del Decreto Legislativo 30.12.1992 n° 502, come sostituito dall'art. 4 punto c) del Decreto Legislativo 07.12.1993 n° 517 e come ulteriormente modificato dall'art. 3 del D. L.vo 19.06.1999, n° 229, esprime parere:

IL DIRETTORE AMMINISTRATIVO ff
(dott. Stefano Di Rocco)

IL DIRETTORE SANITARIO
(d.ssa_Maria Simonetta Santini)

IL DIRETTORE GENERALE
(dott. Roberto Testa)

Regolamento Aziendale per la Protezione dei Dati Personali della ASL 01 Abruzzo

in base a quanto previsto dal

Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) e D.Lgs. 196/03
Codice in Materia di Protezione dei Dati Personali
come mod. dal D. Lgs. 101/2018

SOMMARIO

ART. 1 OGGETTO E FINALITÀ 3
ART. 2 AMBITO DI APPLICAZIONE 3
ART. 3 DEFINIZIONI E ACRONIMI 3
ART. 4 TRATTAMENTO DI DATI PERSONALI 6
ART. 5 PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI 9
ART. 6 CRITERI PER L'ESECUZIONE DEL TRATTAMENTO DEI DATI PERSONALI 10
ART. 7 CONDIZIONI DI LICEITÀ 10
ART. 8 COMUNICAZIONE E DIFFUSIONE DEI DATI 12
ART. 9 INFORMAZIONI ALL'INTERESSATO E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI 13
ART. 10 REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI 14
ART. 11 IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI 15
ART. 12 RESPONSABILE DELLA PROTEZIONE DEI DATI (R.P.D. O D.P.O.) 17
ART. 13 RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI 18
ART. 14 SUB-RESPONSABILI DEL TRATTAMENTO 21
ART. 15 AMMINISTRATORI DI SISTEMA 22
ART. 16 SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI CON DELEGA (SATD). 23
ART. 17 SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI (SAT) 25
ART. 18 PERSONA FISICA ESTERNA ALLA STRUTTURA DEL TITOLARE AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI 26
ART. 19 DIRITTI DELL'INTERESSATO 26
ART. 20 UFFICIO PRIVACY 26
ART. 21 STRATEGIA PER LA TENUTA IN SICUREZZA DEI DATI 27
ART. 22 MISURE DI SICUREZZA INFORMATICHE GENERALI 27
ART. 23 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI 28
ART. 24 ACCORGIMENTI E SOLUZIONI PARTICOLARI IN AMBITO SANITARIO 28
ART. 25 TRATTAMENTI PER RICERCA SCIENTIFICA E PER FINI STATISTICI 29
ART. 26 FORMAZIONE 30
ART. 27 NOTIFICA DI UNA VIOLAZIONE DI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO 30
ART. 28 RINVIO 30
ART. 29 ABROGAZIONI 31
ART. 30 NOTE FINALI 31
ART. 31 ALLEGATI 32

ART. 1 OGGETTO E FINALITÀ

1. Il presente Regolamento disciplina, per l'Azienda Sanitaria Locale di Avezzano, Sulmona, L'Aquila (di seguito: "ASL 01", "Azienda" o il "Titolare"), la tutela delle persone fisiche e degli altri soggetti con riguardo al trattamento dei dati personali e alle norme relative alla libera circolazione dei dati, nel rispetto di quanto previsto dal D.lgs. n. 196/2003 ("Codice in materia di protezione dei dati personali" di seguito "Codice") – come modificato dal D.Lgs. 101/2018 – e dal Regolamento UE 2016/679 (di seguito Regolamento UE o GDPR)
2. Lo scopo del presente Regolamento è di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con la ASL 01.
3. La ASL 01 adotta misure tecniche e organizzative per garantire un livello di sicurezza adeguato ai rischi di distruzione o perdite, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
4. L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi degli articoli di cui al Capo 3 del Regolamento UE.

ART. 2 AMBITO DI APPLICAZIONE

1. Il presente Regolamento si applica a tutti i trattamenti interamente o parzialmente automatizzati di dati personali e ai trattamenti non automatizzati di dati personali contenuti in archivi o destinati a figurarvi effettuati nell'ambito delle attività svolte dalle strutture sotto la titolarità della ASL di Avezzano, Sulmona, L'Aquila o per conto di esse, come individuate dall'Atto Aziendale adottato con Deliberazione 1207/18 e ss.mm.ii..

ART. 3 DEFINIZIONI E ACRONIMI

1. 1. Ai fini del presente Regolamento, in base a quanto previsto dalla normativa vigente in materia di Protezione dei Dati Personali, si riportano le seguenti definizioni:

n.	TERMINE	DEFINIZIONE
1)	**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;
2)	**Autorità di controllo**	l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. In Italia è Costituita dall'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy)
3)	**Autorità di controllo interessata**	un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
4)	**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;
5)	**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;

n.	TERMINE	DEFINIZIONE
6)	**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;
7)	**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;
8)	**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;
9)	**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;
10)	**Gruppo imprenditoriale**	un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
11)	**Impresa**	la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
12)	**Interessato**	una persona fisica identificata o identificabile,
13)	**Limitazione di trattamento**	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
14)	**Norme vincolanti d'impresa**	le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
15)	**Obiezione pertinente e motivata**	un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente Regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente Regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
16)	**Organizzazione internazionale**	un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.
17)	**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

n.	TERMINE	DEFINIZIONE
18)	**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;
19)	**Rappresentante**	la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente Regolamento;
20)	**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;
21)	**Servizio della società dell'informazione**	il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio
22)	**Stabilimento principale**	a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente Regolamento;
23)	**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;
24)	**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;
25)	**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

n.	TERMINE	DEFINIZIONE
26)	**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;
27)	**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;
28)	**Comunicazione**	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies del D.Lgs. 196/03, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
29)	**Diffusione**	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
30)	**Particolari categorie di dati personali**	Sono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
31)	**Contratto**	Contratto (o Contratto Principale), è il contratto esistente tra le parti (Titolare e Responsabile del Trattamento
32)	**SATD**	Soggetto Autorizzato al Trattamento dei dati personali con Delega;
33)	**SAT**	Soggetto Autorizzato al Trattamento dei dati personali;
34)	**RT**	Responsabile del Trattamento dei dati personali;
35)	**SRT**	Sub-Responsabile del Trattamento dei dati personali;
36)	**CT**	Contitolare del Trattamento dei dati personali;
37)	**UOC**	Unità Operativa Complessa
38)	**UOSD**	Unità Operativa Semplice Dipartimentale;
39)	**DPO - RPD**	Data Protection Officer o Responsabile della Protezione Dati.

ART. 4 TRATTAMENTO DI DATI PERSONALI

1. Con l'espressione "trattamento", ai sensi dell'art. 4, GDPR , deve intendersi 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;
2. I trattamenti da effettuarsi da parte delle strutture della ASL 01 devono essere effettuati esclusivamente per l'esercizio delle funzioni istituzionali dell'Azienda e con finalità compatibili con tali funzioni, con particolare riferimento all'ambito sanitario;
3. Tutti i trattamenti di dati personali effettuati dalla ASL 01 devono rispettare i principi di trattamento di cui al successivo articolo 5 del presente Regolamento.

4. Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento, dei Responsabili, dei Soggetti Autorizzati al trattamento dei dati personali con delega (di seguito anche SATD) e dei Soggetti Autorizzati al trattamento dei dati personali (di seguito anche SAT). Non è consentito il trattamento di dati personali da parte di persone non autorizzate.
5. Il trattamento dei dati personali raccolti direttamente dall'Azienda o ad essa comunicati da altri soggetti è effettuato sia con che senza l'ausilio di strumenti elettronici.
6. I trattamenti effettuati dall'Azienda, concernenti i dati personali, sono finalizzati prevalentemente all'erogazione delle prestazioni sanitarie, nonché all'espletamento dei compiti attribuiti dal Servizio Sanitario Nazionale ed agli adempimenti amministrativi e contabili di organizzazione e di controllo preordinati alla predetta erogazione, come regolamentati dalla Legge 833/78, dal D.Lgs. 502/92 e ss.mm.ii., dal DL 13 settembre 2012 n.158 convertito nella Legge 8 novembre 2012 n.189 – Legge Balduzzi oltre che da tutta la normativa applicabile allo specifico settore di appartenenza.
   A titolo esemplificativo e non esaustivo, le macro-categorie di trattamento possono essere classificate nel seguente elenco:
   a) prevenzione collettiva e di sanità pubblica, anche a supporto delle Autorità Sanitarie;
   b) diagnostica strumentale e di laboratorio;
   c) prevenzione delle malattie, cura e riabilitazione in regime ambulatoriale sia in sede distrettuale che ospedaliera;
   d) ricovero ordinario, in day surgery ed in day hospital;
   e) ricovero in regime residenziale e semiresidenziale;
   f) prestazioni sanitarie a rilevanza sociale;
   g) attività o servizi socio-assistenziali su delega dei singoli enti locali;
   h) medicina legale;
   i) ricerca e sperimentazione, nonché elaborazione statistica, epidemiologica e sociologica.

   Sono altresì effettuati nell'ambito dell'Azienda i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti:
   j) la gestione del personale dipendente, ivi comprese le procedure di assunzione;
   k) la gestione dei soggetti che intrattengono rapporti giuridici con la ASL, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Azienda stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i tirocinanti, i volontari;
   l) la gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni e servizi (anche di natura informatica e di Ingegneria Clinica), nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
   m) la gestione dei rapporti con i soggetti accreditati o convenzionati, associazioni anche di volontariato ed altri Enti ed Organismi Pubblici;
   n) la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.
7. L'elenco dei macro-ambiti di trattamento previsti dalle funzioni istituzionali può essere sintetizzato nel seguente elenco:
   1. Tutela dai rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro
   2. Sorveglianza epidemiologica delle malattie infettive e diffusive e delle tossinfezioni alimentari
   3. Attività amministrative e certificatorie correlate alle vaccinazioni e alla verifica assolvimento obbligo vaccinale
   4. Attività amministrative correlate ai programmi di diagnosi precoce
   5. Attività fisica e sportiva
   6. Attività di assistenza socio-sanitaria a favore di fasce deboli di popolazione e di soggetti in regime di detenzione
   7. Medicina di base – pediatria di libera scelta continuità assistenziale (guardia medica notturna e festiva, guardia turistica).

8. Assistenza sanitaria di base: riconoscimento del diritto all'esenzione per patologia/invalidità/reddito e gestione archivio esenti
9. Assistenza sanitaria di base: assistenza sanitaria in forma indiretta
10. Cure all'estero urgenti e programmate
11. Assistenza sanitaria di base: assistenza agli stranieri in Italia (particolari categorie)
12. Assistenza integrativa
13. Assistenza protesica
14. Assistenza domiciliare programmata e integrata
15. Attività amministrative correlate all'assistenza a soggetti non autosufficienti, a persone con disabilità fisica, psichica e sensoriale e a malati terminali nei regimi residenziale, semiresidenziale ambulatoriale (ex art. 26 della L. 833/1978) e domiciliare
16. Assistenza termale
17. Attività amministrativa, programmatoria, gestionale e di valutazione relativa all'assistenza ospedaliera in regime di ricovero
18. Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività immuno-trasfusionale
19. Attività amministrativa, programmatoria gestionale e di valutazione concernente la donazione, il trapianto di organi, tessuti e cellule
20. Soccorso sanitario di emergenza/urgenza sistema "118". Assistenza sanitaria di emergenza
21. Attività amministrative correlate ad assistenza specialistica, ambulatoriale e riabilitazione.
22. Promozione e tutela della salute mentale
23. Attività sanitarie e amministrative correlate alle dipendenze: tossicodipendenza, alcolismo, farmacodipendenza, gioco d'azzardo, tabagismo, HIV (solo per gli aspetti psico-sociali)
24. Assistenza socio-sanitaria per la tutela della salute materno-infantile ed esiti della gravidanza
25. Attività amministrative correlate all'assistenza farmaceutica territoriale e ospedaliera
26. Sperimentazione Clinica
27. Farmacovigilanza e rilevazione reazioni avverse a vaccini e farmaci
28. Attività amministrative correlate all'erogazione a totale carico del servizio sanitario nazionale, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dall'Agenzia Italiana del Farmaco
29. Attività amministrative correlate all'assistenza a favore delle categorie protette (morbo di Hansen).
30. Attività amministrativa programmatoria, gestionale e di valutazione concernente l'assistenza ai nefropatici cronici in trattamento dialitico
31. Attività medico-legale inerente l'istruttoria delle richieste di indennizzo per danni da vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati
32. Attività medico-legale inerente gli accertamenti finalizzati al sostegno delle persone con disabilità (riconoscimento dello stato di invalidità, cecità e sordità civili, della condizione di handicap ai sensi della L. 104/92, accertamenti per il collocamento mirato al lavoro delle persone con disabilità ai sensi della L. 68/99)
33. Attività medico-legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego: idoneità allo svolgimento di attività lavorative; controllo dello stato di malattia dei dipendenti pubblici e privati; accertamenti sanitari di assenza di tossicodipendenza o di assunzione di sostanze stupefacenti o psicotrope in lavoratori addetti a mansioni che comportino particolari rischi per la sicurezza, l'incolumità e la salute di terzi)
34. Attività medico-legale inerente l'accertamento dell'idoneità al porto d'armi, ai fini della sicurezza sociale

35. Attività medico-legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
36. Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza delle infermità da causa di servizio
37. Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari e consulenze e pareri in materia di bioetica
38. Attività medico-legale in ambito necroscopico
39. Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
40. Attività amministrative correlate alla gestione e verifica sull'attività delegata a soggetti accreditati o convenzionati del SSN
41. Gestione Risorse Umane e Trattamento Economico del Personale

8. L'elenco completo dei trattamenti effettuati dall'Azienda è inserito nel Registro dei Trattamenti secondo quanto previsto dall'Art. 30 del GDPR; tale elenco deve essere puntualmente aggiornato dal Titolare e dai Soggetti Autorizzati al Trattamento con Delega in base alla propria area di competenza e di Responsabilità.
9. Qualora un trattamento di dati personali venga affidato in tutto o in parte a soggetti esterni (es.: Responsabili del Trattamento), deve essere previsto, nell'ambito del documento di accordo, il riferimento allo specifico trattamento previsto nel Registro Aziendale dei Trattamenti di Dati Personali.

ART. 5 PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

1. Ogni trattamento di dati personali effettuato dalla ASL 01 deve rispettare i seguenti principi:
   a) **«liceità, correttezza e trasparenza»**: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
   b) **«limitazione della finalità»**: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del GDPR, considerato incompatibile con le finalità iniziali;
   c) **«minimizzazione dei dati»**: i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   d) **«esattezza»**: i dati personali devono essere 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;
   e) **«limitazione della conservazione»**: i dati personali devono essere 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato;
   f) **«integrità e riservatezza»**: i dati personali devono essere 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.
2. La ASL 01, in qualità di titolare del trattamento, secondo quanto previsto dal principio di responsabilizzazione, è competente per il rispetto dei principi di trattamento indicati nel paragrafo 1.
3. Al fine di dimostrare il rispetto dei principi di trattamento indicati ai paragrafi 1 e 2, il presente documento costituisce il Regolamento aziendale generale per tutti i trattamenti di dati personali effettuati dalle strutture della ASL 01: è responsabilità del Titolare e dei soggetti da esso autorizzati al trattamento,

rispettare quanto previsto dal presente Regolamento, dai documenti ad esso correlati e dalla normativa vigente applicabile.

ART. 6 CRITERI PER L'ESECUZIONE DEL TRATTAMENTO DEI DATI PERSONALI

1. Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e delle libertà fondamentali delle persone fisiche nonché delle norme relative alla libera circolazione di tali dati.
2. Oggetto del trattamento devono essere solo i dati essenziali per lo svolgimento delle attività istituzionali nel rispetto del Principio di Minimizzazione come previsto dall'art. 5.1.c) del presente Regolamento.
3. I dati personali devono essere trattati in modo lecito, corretto e trasparente, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati nel rispetto dei principi previsti dall'art. 5.1 lettere a) e b) del presente Regolamento. Le condizioni di liceità ammissibili per i trattamenti dei dati personali effettuati dalle strutture della ASL 01 sono stabilite nell'art. 7 del presente Regolamento.
4. Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi nel rispetto sia di quanto previsto dall'art. 5.1.c) del presente Regolamento che dall'art. 25 del GDPR "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita".
5. È compito delle persone fisiche autorizzate al trattamento dei dati personali con delega (SATD), ai sensi dell'art. 29 del Regolamento UE e dell'art. 2-quaterdecies del Codice, censire e verificare periodicamente la liceità e la correttezza dei trattamenti della propria area di competenza, verificarne l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.
6. I dati che, anche a seguito di verifiche effettuate dai SATD o dal RPD, risultassero eccedenti, non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione dell'atto che li contiene, a norma di legge e/o in base a quanto previsto dal Massimario di Conservazione della ASL 01.
7. I trattamenti di dati effettuati impiegando banche dati di più titolari diversi dall'Azienda (interconnessione di banche dati) sono utilizzati nelle sole ipotesi previste da espressa disposizione di legge.
8. Ai sensi dell'art. 9 del GDPR, i dati personali appartenenti a particolari categorie sono conservati, ove possibile, in base ad opportune misure tecniche e organizzative applicabili secondo i criteri stabiliti dall'art. 32 del GDPR, separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.
9. In ogni caso devono essere adottate misure tecniche e organizzative tali da garantire che i dati personali siano accessibili alle sole persone fisiche autorizzate al trattamento dei dati personali e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

ART. 7 CONDIZIONI DI LICEITÀ

1. Le condizioni di liceità, in presenza delle quali il Titolare compie operazioni di trattamento dei dati personali sono quelle indicate nell'art. 6.1 del Regolamento UE come di seguito riportate:
   a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
   b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

2. Come previsto dall'art. 6.3 lett. b) del Regolamento UE, secondo quanto disposto dall'art. 2-ter del D.Lgs. 196/03, il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento rif. comma 1.e) del presente articolo – deve essere basato su una norma di legge o, nei casi previsti dalla legge, di Regolamento. Pertanto, per i trattamenti fondati su tale base giuridica, è necessaria l'individuazione specifica della legislazione di riferimento da indicarsi nel Registro Aziendale dei Trattamenti.
3. Ai sensi dell'art. 9.2 del GDPR, è possibile effettuare il trattamento di particolari categorie di dati personali (vedere definizione riportata nell'Art. 3 del presente Regolamento), in base alle seguenti basi giuridiche applicabili al contesto delle attività svolte per fini istituzionali dalla ASL 01:
   a) 9.2.a) del GDPR: l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri disponga che tale base giuridica (consenso) non sia applicabile;
   b) 9.2.b) del GDPR: il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c) 9.2.c) del GDPR: il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) 9.2.f) del GDPR: il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
   e) 9.2.g) del GDPR: il trattamento è necessario per **motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri**, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
   f) 9.2.h) del GDPR: il trattamento è necessario per **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (di seguito "finalità di cura"** come indicato dal Garante nel Provvedimento n. 55 del 7 marzo 2019) sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3. Tale base giuridica prevede anche il caso di trattamento di particolari categorie di dati personali anche per finalità di medicina del lavoro, valutazione della capacità lavorativa del dipendente
   g) 9.2.i) del GDPR: il trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
   h) 9.2.j) del GDPR: il trattamento è necessario a fini di archiviazione nel pubblico interesse, di **ricerca scientifica** o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla

protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

4. Per trattamenti per "finalità di cura", sulla base dell'art. 9, par. 2, lett. h) e par. 3 del GDPR, sono propriamente quelli effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.
5. Per trattamenti di dati personali di cui all'art. 9, par. 2, lett. h) del GDPR, si intendono quelli "necessari" al perseguimento delle specifiche "finalità di cura" previste dal GDPR, cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute.
6. Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del GDPR).
7. I trattamenti delle categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante ai sensi dell'articolo 9.2, lettera g) del GDPR sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 2-sexies c.1 del Codice).
8. Fermo quanto previsto dal precedente comma, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati dalla ASL 01, nell'ambito dello svolgimento di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie indicate dall'art. 2-sexies c.2) del Codice.
9. I trattamenti di dati personali relativi a condanne penali e reati, come previsti dall'art. 10 del GDPR, sono regolamentati dallo stesso e dall'articolo 2-octies del Codice.
10. Secondo quanto previsto dall'articolo 2-quater c.4) del Codice il rispetto delle disposizioni contenute nelle regole deontologiche promosse dall'Autorità Garante per la Protezione dei Dati costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.

ART. 8 COMUNICAZIONE E DIFFUSIONE DEI DATI

1. La comunicazione da parte dell'Azienda ad altri titolari di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del Regolamento UE e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento UE, è lecita nei seguenti casi:
   a) si basa sul consenso dell'interessato;
   b) è necessaria all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) è necessaria per adempiere un obbligo legale al quale è soggetta la ASL 01;
   d) è necessaria per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
   e) è necessaria per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita la ASL 01.
2. La comunicazione di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del Regolamento UE e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento UE, nei casi previsti dal comma 1 lett. c) ed e) del presente articolo, da parte dell'Azienda ad altri titolari è ammessa solo quando sia prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di 45 giorni dalla data di comunicazione obbligatoriamente preventiva al Garante e non sia stata adottata dall'Autorità diversa determinazione.
3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità

sono ammesse unicamente se previste da una norma di legge o, nei casi previsti dalla legge, di regolamento.

4. I dati genetici, biometrici e relativi alla salute, possono essere oggetto di comunicazione in presenza di una delle condizioni previste dall'art. 7.3 del presente Regolamento ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dall'articolo 2-septies del Codice;
5. I dati genetici, biometrici e relativi alla salute non possono essere diffusi secondo quanto previsto dall'art. 2-septies del Codice.
6. La comunicazione e la diffusione dei dati per finalità di ricerca scientifica o di statistica, sono consentite qualora si tratti di dati anonimi e comunque tali da non consentire l'identificazione degli interessati.
7. Il trasferimento di dati personali verso Stati appartenenti all'Unione Europea, è consentito nel rispetto di quanto previsto nei commi precedenti, senza necessità di autorizzazione del Garante.
8. Qualora i dati personali siano oggetto di trasferimento verso Stati non appartenenti all'Unione Europea, debbono essere osservate le ulteriori cautele previste dal Regolamento UE.
9. Ulteriori precisazioni sono specificate nella Procedura Aziendale di Gestione delle Informative e dei Consensi, allegata al presente Regolamento, e nella normativa vigente applicabile.

ART. 9 INFORMAZIONI ALL'INTERESSATO E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

1. Le informazioni all'interessato sono l'elemento propedeutico al trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.
2. Le informazioni all'interessato sono sempre dovute a prescindere dall'obbligo di acquisizione del consenso. L'informativa deve contenere gli elementi tassativamente indicati dagli artt. 13 e 14 del Regolamento UE e più specificatamente:
   a) le finalità e le modalità con le quali vengono trattati i dati personali;
   b) l'obbligatorietà o meno del conferimento dei dati;
   c) le conseguenze di un eventuale rifiuto a fornire i dati;
   d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Autorizzati (con o senza delega) e l'ambito di diffusione dei dati medesimi;
   e) i diritti dell'interessato di cui all'art. 20 del presente Regolamento;
   f) gli estremi identificativi del Titolare e del Responsabile della Protezione dei Dati.
3. Le predette informazioni all'interessato possono essere rese anche tramite affissione di appositi manifesti nei locali di accesso all'utenza o loro pubblicazione sul sito aziendale nella apposita sezione Privacy.
4. Ai sensi dell'art. 13 del Regolamento UE, in caso di raccolta presso l'interessato dei dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
   a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
   b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) qualora il trattamento si basi sull'art. 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
   e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
   f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.
5. In aggiunta alle informazioni di cui sopra, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'art. 6, paragrafo 1, lettera a), oppure sull'art. 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (solo nel caso in cui i dati non siano stati raccolti presso l'interessato);
f) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
g) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

6. Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.
7. Le modalità di gestione e prestazione del Consenso al Trattamento dei Dati Personali, ove richiesto, sono specificate nella Procedura Aziendale di Gestione delle Informative e dei Consensi e nella normativa vigente applicabile.
8. Ulteriori indicazioni operative per la gestione delle Informative sono contenute nella Procedura Aziendale di Gestione delle Informative e dei Consensi, allegata al presente Regolamento, e nella normativa vigente applicabile.

ART. 10 REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

1. L'Azienda (il Titolare) redige, conserva ed aggiorna il Registro delle attività di trattamento svolte sotto la propria responsabilità. Esso viene predisposto per contenere la rilevazione dei trattamenti dei dati suddivisi per tipologie e per strutture organizzative, come presupposto necessario per adempiere agli obblighi di legge. Per ogni tipologia di trattamento sono indicate le informazioni di cui ai successivi commi 2 e 3.
2. Il registro contiene tutte le informazioni previste dall'art. 30 del Regolamento UE:
   a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
   b) le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
   e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'articolo 49.2 del Regolamento UE, la documentazione delle garanzie adeguate;
   f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento UE.
3. Al fine di dare completezza alla descrizione dei trattamenti, le ulteriori informazioni che dovranno essere compilate nel registro sono le seguenti:

a) ulteriori finalità e relative modalità di verifica di compatibilità (art. 6.4 del Regolamento UE) con la finalità per la quale i dati personali erano stati inizialmente raccolti;
b) Condizioni di Liceità, ai sensi dell'art. 6.1 e 9.2 del Regolamento UE
c) L'eventuale base giuridica su cui si fonda il trattamento dei dati

4. Il Registro dei Trattamenti è redatto e tenuto a cura dell'Ufficio Privacy, in formato elettronico stampabile, con il supporto dell'UOSD Sistemi Informativi ed in collaborazione con i Soggetti Autorizzati al Trattamento dei Dati Personali con Delega, che dovranno comunicare e aggiornare l'elenco dei trattamenti effettuati nell'ambito della propria struttura, con il Direttore Responsabile dell'UOSD Sistemi Informativi e con gli Amministratori di Sistema.
5. Il Registro dei Trattamenti deve riportare la data della sua prima istituzione, unitamente alla data di eventuali aggiornamenti.
6. Il Registro dei Trattamenti viene aggiornato periodicamente in caso di modifiche ai trattamenti effettuati dalla ASL 01. È compito dei singoli SATD, sotto la propria responsabilità e nell'ambito dei trattamenti afferenti alla propria struttura, comunicare tempestivamente al Titolare, per il tramite dell'Ufficio Privacy, casi di attivazione di nuovi trattamenti, modifiche o cessazioni di trattamenti in essere; nei casi di nuovo trattamento sarà cura del Titolare valutare la necessità di acquisire un preventivo parere in merito da parte del RPD.
7. Nel caso in cui la ASL 01 sia designata Responsabile del trattamento, deve tenere, altresì, un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare di riferimento. Tale Registro dovrà contenere:
   a) il nome e i dati di contatto del Titolare del Trattamento di riferimento e, ove applicabile, del Responsabile della Protezione dei Dati;
   b) le categorie dei trattamenti effettuati per conto del Titolare del Trattamento di riferimento;
   c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
   d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento UE.
8. Su richiesta, la ASL 01, in qualità di titolare del trattamento o, ove applicabile, di responsabile del trattamento, mettono il registro a disposizione dell'autorità di controllo.
9. Il Registro dei Trattamenti, allegato 1 al presente Regolamento, viene istituito a seguito della rilevazione dei trattamenti di dati personali effettuati presso le Unità Operative/Strutture aziendali, mediante opportuni questionari ed interviste con i Direttori/Responsabili delle strutture organizzative aziendali.

ART. 11 IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

1. Il "Titolare" del trattamento dei dati personali è «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;»
2. Il Titolare del trattamento è la Asl di Avezzano – Sulmona – L'Aquila, con sede in via Via Saragat - località Campo di Pile - 67100 L'Aquila che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Gli indirizzi di posta elettronica del Titolare sono i seguenti: PEC: protocollogenerale@pec.asl1abruzzo.it; PEO (Posta Elettronica Ordinaria): direzionegenerale@asl1abruzzo.it.
3. Il Titolare dovrà mettere in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che i trattamenti posti in essere sono conformi al GDPR.
4. Il Titolare, avvalendosi della supervisione e collaborazione del Responsabile della Protezione dei Dati aziendale (anche Data Protection Officer, di seguito, R.P.D. o D.P.O.), provvede:

a) a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale necessità di comunicazione;
b) a individuare i Direttori/Responsabili delle strutture organizzative aziendali da nominare, con successivo atto, quali SATD, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione alle informazioni da rendere agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dagli artt. 15-22 del GDPR, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
c) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
d) a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente alla vigente normativa di settore in materia di protezione dei dati personali oltre che al presente Regolamento.

5. Le responsabilità del titolare del trattamento sono regolamentate, in termini generali, dall'Art. 24 del Regolamento UE con particolare riferimento ai seguenti punti:
   a) Tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento aziendale. Dette misure devono essere riesaminate e aggiornate qualora necessario.
   b) Le misure di cui sopra includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte della ASL di Avezzano – Sulmona – L'Aquila.
   c) Al fine di dimostrare il rispetto degli obblighi indicati dalla normativa vigente applicabile da parte del titolare del trattamento, può essere prevista l'adesione a codici di condotta di cui all'articolo 40 del Regolamento UE o a un meccanismo di certificazione di cui all'articolo 42 del Regolamento UE.
6. I compiti del Titolare del Trattamento sono indicati nei seguenti punti:
   a) curare la sicurezza del trattamento (art. 32 del Regolamento UE), applicando i principi di "privacy by design e by default" (art. 25 del Regolamento UE);
   b) procedere alla valutazione d'impatto privacy dei trattamenti - c.d. "data protection impact assessment" (art. 35 del Regolamento UE);
   c) implementare un Sistema di Gestione della Protezione dei Dati, costituito da misure tecniche e organizzative adeguate, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR (art. 24, paragrafo 1 del Regolamento UE);
   d) adottare policy sul trattamento dei dati personali (art. 24, paragrafo 2 del Regolamento UE) o aderire a codici di condotta (art. 40) o conseguire certificazioni (art. 42 del Regolamento UE);
   e) curare il rispetto dei principi applicabili al trattamento dei dati personali - c.d. "responsabilizzazione" o "accountability" - (art. 5, paragrafo 2 del Regolamento UE);
   f) nominare direttamente o tramite delega i responsabili del trattamento (artt. 24, paragrafo 1 e 28, paragrafo 1 del Regolamento UE);
   g) designare il Responsabile della Protezione dei Dati (c.d. Data Protection Officer) (art. 37, paragrafo 5 del Regolamento UE) e cooperare con lo stesso (art. 38, paragrafo 1 del Regolamento UE) sostenendolo nella sua attività (art. 38, paragrafo 2 del Regolamento UE) e garantendone indipendenza e autonomia (art. 38, paragrafo 3 del Regolamento UE);
   h) curare, quando ne ricorrono le condizioni, la notifica di una violazione dei dati personali - c.d. "data breach notification" all'Autorità Garante (art. 33 del Regolamento UE) e all'interessato (art. 34 del Regolamento UE);
   i) rendere idonea informativa agli interessati (artt. 13 e 14 del Regolamento UE);

j) fornire idoneo e tempestivo riscontro alle richieste dell'interessato (art. 12, paragrafo 3 del Regolamento UE) nell'esercizio dei suoi diritti (artt. 15-22 del Regolamento UE);
k) cooperare con l'Autorità Garante (art. 31 del Regolamento UE), fornendogli ogni informazione necessaria (art. 58, paragrafo 1 del Regolamento UE);
l) cooperare con gli organismi indipendenti di certificazione (art. 42, paragrafo 6 del Regolamento UE).

ART. 12 RESPONSABILE DELLA PROTEZIONE DEI DATI (R.P.D. O D.P.O.)

1. Il Responsabile della Protezione Dati (c.d. R.P.D. o D.P.O.), è designato dal Titolare del trattamento mediante specifico atto di designazione in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di seguito descritti:
   a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
   b) sorvegliare l'osservanza del Regolamento UE, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Regolamento UE;
   d) cooperare con l'autorità di controllo (in Italia Garante per la Protezione dei Dati Personali);
   e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
3. Il responsabile della protezione dei dati può essere un dipendente del Titolare del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
4. Il Titolare del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.
5. Il Titolare del trattamento e la sua struttura organizzativa composta dai Soggetti Autorizzati al Trattamento con Delega (SATD) si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
6. Il titolare del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui al precedente comma 1 fornendogli quanto eventualmente necessario per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
7. Il titolare del trattamento si assicura che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Come espressamente previsto dall'art. 38.3 del Regolamento UE, il responsabile della protezione dei dati non può essere rimosso o penalizzato dal titolare del trattamento per l'adempimento dei propri compiti. Il Responsabile della Protezione dei Dati riferisce direttamente al vertice gerarchico del titolare del trattamento.
8. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente Regolamento. Il riferimento quale punto di contatto deve essere indicato nelle informative per gli interessati, come previsto dall'art 9 del presente Regolamento.

9. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
10. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

ART. 13 RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

1. In base a quanto previsto dall'art. 4.8 del Regolamento UE, 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 ed è esterno alla struttura del Titolare.
2. Ai sensi dell'art. 28 del Regolamento UE, qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo deve ricorrere 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.
3. I Responsabili sono principalmente riconducibili alla categoria dei fornitori di beni e/o servizi che trattano dati personali per conto del Titolare del trattamento. A tal proposito la ASL 01 designa Responsabili del Trattamento dei Dati Personali tutti i soggetti esterni cui sono affidate attività di competenza aziendale o attività connesse strumentali e di supporto, ivi incluse le attività manutentive che comunque comportano necessariamente il trattamento di dati personali.
4. Il Responsabile dovrà trattare i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro, alla Convenzione, alla Delibera di nomina/aggiudicazione e al Contratto Principale. I servizi che potranno essere svolti dal Responsabile sono indicati nei documenti sopra richiamati e, eventualmente, in altri documenti prodotti dal Titolare.
5. La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile deve corrispondere alla durata indicata nei documenti di cui al precedente punto 4. Nel caso in cui, nell'ambito del trattamento svolto per conto del Titolare, il Responsabile fosse tenuto a conservare dati personali, la durata della conservazione dovrà essere pari alla durata contrattuale se non previsto diversamente da specifica disposizione di legge o, nei casi previsti dalla legge, di regolamento o in generale a livello normativo.
6. I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi dell'atto di designazione sono, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Titolare, terzi incaricati, a qualunque titolo, dal Titolare, pazienti, controparti contrattuali del Titolare e, in generale, terze parti rispetto alle quali l'Azienda agisce come Titolare del trattamento dei dati personali ai sensi del Regolamento UE. I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute.
7. Il Responsabile dovrà effettuare il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite dovrà essere indicato nello specifico allegato all'atto di designazione. L'atto di designazione e il Contratto Principale costituiscono parte delle istruzioni dell'Azienda per il trattamento dei dati personali da parte del 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. Tali istruzioni dovranno essere fornite dal Titolare anche in caso di necessità 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 dovrà informare 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.
8. Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nel Contratto e nell'atto di nomina dovrà essere trasmessa dall'Azienda al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

9. Il Responsabile dovrà garantire che i soggetti da lui autorizzati al trattamento dei dati personali si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.
10. Il Responsabile dovrà impegnarsi ad adottare le misure richieste dall'art. 32 del GDPR.
11. 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 Responsabile dovrà impegnarsi a mettere in atto le misure tecniche e organizzative adeguate, indicate negli allegati all'atto di designazione di cui si dovrà richiedere la compilazione per la descrizione delle modalità di implementazione. Il Responsabile dovrà impegnarsi a comunicare le indicazioni applicabili ai prodotti e/o servizi forniti secondo quanto previsto dall'Atto di designazione (tale obbligo vige solo per i Responsabili fornitori di servizi tecnici/tecnologici o per specifici requisiti).
12. Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Atto di designazione, in considerazione del progresso e sviluppo tecnologico, dovrà effettuare una preventiva comunicazione al Titolare, fermo restando che tali modifiche non dovranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Atto di designazione.
13. Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nel Contratto, il Responsabile dovrà impegnarsi 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 Regolamento UE.
14. Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli artt. da 15 a 22 del regolamento UE nell'ambito delle attività di trattamento di dati personali svolti per conto del Titolare.
15. Tenendo conto della natura del trattamento, come descritto nel Contratto e nell'atto di designazione, e delle informazioni di volta in volta messe a disposizione, il Responsabile dovrà impegnarsi ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del Regolamento UE.
16. I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dal Contratto e nell'atto di designazione, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, dovranno essere periodicamente cancellati ove ne ricorra il termine in base a quanto previsto dal Massimario di Conservazione della ASL 01 Abruzzo. Alla cessazione del Contratto, i dati oggetto di Trattamento da parte del Responsabile dovranno essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.
17. In mancanza di diverse istruzioni successive, il Titolare dovrà chiedere 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 (diritto dell'Unione o degli Stati membri) obblighi il Responsabile alla conservazione dei dati personali trattati.
18. Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo e comunque entro 48 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.
19. Oltre a quanto già previsto dal precedente comma 15, il Responsabile dovrà, ai sensi dell'art. 28.3, lett. f) del Regolamento UE, 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 Regolamento UE o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR. Secondo quanto previsto dalla Procedura di Gestione delle Violazioni di Dati Personali, allegata al presente Regolamento, la

comunicazione delle suddette violazioni dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi protocollogenerale@pec.asl1abruzzo.it e databreach@asl1abruzzo.it.

20. Oltre a quanto già previsto dal precedente comma 15, il Responsabile, ai sensi dell'art. 28.3, lett. f) del GDPR, dovrà, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, 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 UE, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento UE.
21. Fatta salva la possibilità di nominare un Sub Responsabile, il Responsabile deve garantire che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi oggetto del Contratto.
22. Il Responsabile deve impegnarsi 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 svolte per conto del Titolare, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.
23. Il Responsabile, su richiesta del Titolare, dovrà 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.
24. Il Responsabile dovrà mettere 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 contenute nell'atto di designazione e dovrà consentire 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.
25. Il Titolare dovrà dare comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.
26. Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.
27. Il Responsabile dovrà impegnarsi 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 e Sub-Responsabili, 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 l'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.
28. Qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento, in violazione delle istruzioni impartite dal Titolare, in base a quanto previsto

dall'art. 28.10 del Regolamento UE, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

29. La designazione in qualità di Responsabile non dovrà comportare alcun diritto per questi 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 stipulato con il Titolare.
30. Il Responsabile dovrà tenere ed aggiornare costantemente il Registro dei Trattamenti svolti per conto del Titolare, secondo quanto previsto dall'art. 30.2 del Regolamento UE.
31. Il Titolare dovrà poter chiedere copia del Registro dei Trattamenti del Responsabile per i trattamenti svolti per conto del Titolare e di copia della documentazione relativa agli adempimenti privacy attuati dal Responsabile nell'ambito del servizio svolto per conto del Titolare.
32. Eventuali modifiche e/o integrazioni all'atto di designazione del Responsabile, previamente concordate con il Titolare, dovranno essere poste in atto in uno specifico articolo dell'atto stesso denominato "Accordi Specifici".
33. Ulteriori dettagli relativi alla designazione dei Responsabili del Trattamento sono specificati nella Procedura di Gestione delle Nomine e Designazioni allegata al presente Regolamento.

ART. 14 SUB-RESPONSABILI DEL TRATTAMENTO

1. Per l'esecuzione di specifiche attività per conto del Titolare, il Responsabile potrà avvalersi di sub-responsabili del trattamento ai sensi del Regolamento UE. 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 dovranno essere 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 nell'accordo di designazione 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 UE. Secondo quanto previsto dall'art. 28.4 del Regolamento UE, qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserverà nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.
2. L'accordo di designazione tra il Responsabile ed il Sub-responsabile dovrà essere fornito in copia al Titolare in maniera che esso possa verificarne la conformità rispetto ai requisiti definiti per il Responsabile; tale accordo potrà essere anche pre-esistente all'accordo di designazione del Responsabile del Trattamento da parte del Titolare. Nell'accordo di designazione tra il Responsabile ed il Sub-responsabile, dovrà essere previsto un ruolo di sub-responsabilità da parte del sub-responsabile.
3. L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto e all'atto di designazione dovrà essere previamente fornito al Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco. Alla richiesta di autorizzazione da parte del Responsabile, dovrà essere allegato l'accordo di designazione del Sub-responsabile.
4. Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 11 del presente Regolamento), laddove intenda:
   a) includere un nuovo Sub-responsabile del Trattamento nell'elenco,
   b) sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente.

   La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 30 giorni dalla ricezione della comunicazione da parte del Responsabile.

5. Qualora il Titolare sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare dovrà dare darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà: proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; oppure adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
6. Il Responsabile assume la responsabilità nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.
7. Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile 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.
8. Ulteriori dettagli relativi alla designazione dei Sub-Responsabili del Trattamento sono specificati nella Procedura di Gestione delle Nomine e Designazioni allegata al presente Regolamento.

ART. 15 AMMINISTRATORI DI SISTEMA

1. In base a quanto previsto dal Provvedimento del Garante Privacy del 27 novembre 2008 e ss.mm.ii., *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*, con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
2. Il Titolare dovrà conformarsi a quanto previsto dal provvedimento di cui al comma 1 e ad ogni altro pertinente provvedimento dell'Autorità Garante.
3. In fase di individuazione delle figure professionali dovrà essere posta particolare attenzione all'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministratore di base di dati (database administrator) o amministratore di rete (network administrator), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.
4. In riferimento ai sistemi informatici di trattamento dei dati del Titolare, il Soggetto Autorizzato al Trattamento con Delega competente (in riferimento ai sistemi informatici o sistemi di tecnologia sanitaria aziendali) 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) aggiornare periodicamente l'elenco 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 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.

5. Nel caso in cui il Titolare affidi in outsourcing servizi di amministrazione di sistema, le prescrizioni e gli adempimenti di cui al Provvedimento del 27 novembre 2008 del Garante per la Protezione dei dati personali sono posti in capo al soggetto esterno individuato dall'Azienda quale Responsabile del trattamento.
6. Il Responsabile, in particolare, è tenuto a:
   a) procedere all'attribuzione delle funzioni di Amministratore di sistema mediante designazione individuale previa valutazione dell'esperienza, capacità e affidabilità del soggetto designato;
   b) precisare analiticamente per ciascun soggetto designato l'ambito di operatività consentito in base al profilo autorizzativo assegnato;
   c) conservare e aggiornare periodicamente gli estremi identificativi delle persone fisiche preposte quali Amministratori di sistema;
   d) procedere alla verifica, almeno annuale, dell'operato degli Amministratori individuati;
   e) adottare sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori;
7. Ogni qualvolta l'Azienda intende esternalizzare servizi di amministrazione di sistema, l'atto di designazione a Responsabile di cui all'art 13 del presente Regolamento deve essere integrato con l'esplicitazione delle puntuali prescrizioni di cui al precedente comma.
8. Per i servizi già esternalizzati, i Soggetti Autorizzati al Trattamento con Delega (SATD) si attivano - ciascuno per le banche dati di propria competenza - nei confronti del Responsabile provvedendo a integrare le istruzioni/indicazioni già impartite.

ART. 16 SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI CON DELEGA (SATD).

1. Il titolare provvede alla nomina dei Soggetti Autorizzati al Trattamento dei Dati Personali con Delega (SATD) i quali compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni contenute nel GDPR oltre che nella normativa di settore in tema di protezione dei dati personali; in particolare hanno il dovere di osservare e la delega a fare osservare le precauzioni e le disposizioni individuate dal Titolare in tema di sicurezza dei dati personali.
2. Sono nominati SATD il Direttore Amministrativo, il Direttore Sanitario, i Direttori di Dipartimento, i Direttori/Responsabili di UOC e di UOSD che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.
3. Il SATD deve essere designato per iscritto dal Titolare mediante atto formale e i compiti a lui affidati devono essere analiticamente specificati da parte del Titolare nell'atto di nomina e potranno essere integrati, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.
4. Il SATD, nell'espletamento della sua funzione, collabora con il Titolare, il DPO e con l'Ufficio Privacy e, in particolare:
   a) comunica ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE riguardanti l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio;
   b) comunica eventuali variazioni da apportare al Registro dei Trattamenti;
   c) utilizza – per competenza - il modello di Informativa e Consenso approvato con il presente Regolamento e quelli eventualmente successivamente approvati dal Titolare, verificandone il rispetto;
   d) collabora nella gestione delle istanze degli interessati;

e) contribuisce a far sì che tutte le misure di sicurezza riguardanti i dati dell'Azienda siano applicate all'interno dell'Azienda stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
f) informa il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

5. La funzione di SATD, attribuita personalmente, non è suscettibile di delega.
6. Il SATD tratta i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte dall'Unità Operativa di cui è Direttore/Responsabile. Le attività di trattamento sono correlate allo svolgimento dell'incarico ricevuto.
7. Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto dalla designazione deve essere fornita dal Titolare al SATD per iscritto.
8. I soggetti i cui dati personali sono oggetto del trattamento da parte del SATD sono, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Titolare, terzi incaricati, a qualunque titolo, dal Titolare, pazienti, controparti contrattuali del Titolare e, in generale, terze parti rispetto alle quali l'Azienda agisce come titolare del trattamento dei dati personali ai sensi del regolamento UE.
9. Il SATD nomina le persone fisiche autorizzate al trattamento dei dati personali (SAT) con previsione dell'impegno alla riservatezza dei dati trattati.
10. I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute.
11. Il SATD dovrà impegnarsi, per i trattamenti sotto la propria responsabilità, a richiedere ed adottare le misure richieste dall'art. 32 del GDPR, tenendo conto 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.
12. Come indicato all'art. 13 del presente Regolamento aziendale, per l'esecuzione di specifiche attività, il Titolare può avvalersi di Responsabili del trattamento esterni all'organizzazione secondo quanto previsto dall'art. 28 del Regolamento UE. 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 al SATD ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Titolare o il SATD, secondo quanto disciplinato dalla "Procedura per la gestione di Accordi, Nomine e Designazioni", designeranno Responsabili del Trattamento, questi ultimi dovranno essere 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 nella lettera di nomina del SATD, 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 UE. Il SATD designante o, in caso di designazione del Responsabile da parte del Titolare, il SATD deputato al controllo (o SATD referente), avrà l'obbligo di controllare il rispetto degli adempimenti privacy da parte del Responsabile.
13. Negli accordi/convenzioni con terze parti e nei contratti di affidamento di attività o di servizi all'esterno della struttura del Titolare, i trattamenti di dati effettuati in forza del rapporto contrattuale dovranno essere sottoposti all'osservanza delle norme di legge sulla protezione dei dati personali e delle disposizioni dell'Azienda in materia.
14. In caso di acquisizione da parte dell'Azienda di forniture che prevedono l'utilizzo di infrastrutture ad alta complessità (es.: servizi Cloud, telecontrollo remoto di attrezzature sanitarie, telemedicina, laboratorio analisi, Videosorveglianza), al fine di verificare l'attuazione delle misure di sicurezza da parte del Responsabile del Trattamento, la UOSD Sistemi Informativi c/o la UOC Ingegneria Clinica possono fornire il necessario supporto al SATD designante o referente.
15. Il SATD, per la verifica di adozione ed attuazione, da parte dei Responsabili del Trattamento, di misure tecniche e organizzative che garantiscano un livello di sicurezza dei dati adeguato e conforme a quanto previsto dal regolamento UE e, in particolare, che forniscano sufficienti garanzie per la protezione dei

dati personali dei Terzi Interessati, dovranno utilizzare gli allegati all'atto di designazione in qualità di Responsabile del Trattamento.

16. Qualora il SATD intendesse apportare modifiche alle misure tecniche e organizzative rispetto a quelle previste nei documenti indicati al comma precedente, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione al Titolare, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto indicato dalle misure previste.
17. Il SATD cui compete l'istruttoria dei rapporti contrattuali e/o convenzionali a vario titolo (es.: UOC Acquisizione Beni e Servizi, UOC Patrimonio, UOC Ingegneria Clinica, UOSD Sistemi Informativi, UOC Affari Generali e Legali, ecc...), effettua una costante ricognizione dei contratti/convenzioni in essere di cui è il referente, al fine di provvedere:
    a) agli adempimenti di legge in materia di trattamento dei dati personali,
    b) all'inserimento nei contratti/convenzioni medesimi della clausola di garanzia.
18. L'elenco di tali contratti/convenzioni deve essere inviato, per competenza, all'UOSD Sistemi Informativi e/o alla UOC Ingegneria Clinica e/o alla UOC Servizio Tecnico Patrimoniale oltre che all'Ufficio aziendale Privacy.
19. Tenendo conto della natura del trattamento dei dati personali svolto dal SATD, come descritto nel Registro dei Trattamenti, questi si impegna ad assistere il Titolare al fine di adempiere al proprio obbligo di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli artt. da 15 a 22 del GDPR.
20. Tenendo conto della natura del trattamento come descritto nel Registro dei Trattamenti, nella lettera di nomina del SATD e delle informazioni di volta in volta messe a disposizione, il SATD si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del GDPR
21. I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del SATD, 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 secondo modalità conformi alle normative applicabili.
22. Il SATD si impegna a mettere a disposizione del Titolare, su richiesta scritta di quest'ultimo, tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dall'atto della sua nomina.
23. Il SATD dovrà consentire al Titolare e al DPO di eseguire verifiche e ispezioni (congiuntamente "Audit") sulle informazioni di cui al comma precedente, e si impegna ad assistere il Titolare, al fine di dimostrare, con riferimento al trattamento di dati svolto per compiti istituzionali, l'adempimento degli obblighi previsti dall'atto della sua nomina. Gli Audit potranno anche essere condotti direttamente da personale del Titolare o da un revisore terzo indipendente da esso incaricato.
24. Il SATD si fa carico di assicurare, in accordo con il Titolare, la dovuta formazione in materia di trattamento dei dati del personale da lui autorizzato.
25. Ulteriori dettagli relativi alla designazione dei Soggetti Autorizzati al Trattamento con Delega (SATD) sono specificati nella Procedura per la Gestione di Accordi, Nomine e Designazioni allegata al presente Regolamento.

ART. 17 SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI (SAT)

1. Il SATD deve nominare Soggetti Autorizzati al Trattamento dei Dati Personali (SAT) le persone fisiche che svolgono trattamenti di dati personali nell'ambito dell'Unità Operativa o Struttura da lui diretta.
2. Il Soggetto Autorizzato (SAT) può trattare i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte dall'Unità Operativa di appartenenza. Le attività di trattamento di dati personali sono correlate allo svolgimento delle proprie funzioni.
3. Il trattamento dei dati personali da parte dei SAT dovrà avvenire secondo le istruzioni impartite dal SATD. I soggetti i cui dati personali sono oggetto del trattamento da parte del SAT possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Titolare, terzi incaricati, a qualunque titolo, dal Titolare, pazienti, controparti contrattuali del Titolare e, in generale, terze parti

rispetto alle quali l'Azienda agisce come Titolare del trattamento dei dati personali ai sensi del GDPR. I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

4. Il SAT dovrà effettuare il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare e/o dal Soggetto autorizzato con delega in forma scritta. L'atto di nomina costituisce parte delle istruzioni del Titolare e/o del SATD per il trattamento dei dati personali da parte del Soggetto Autorizzato e potrà essere integrato, 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 del SATD.
5. Il SAT si impegna a mantenere la riservatezza dei dati trattati e si assoggetta a tale obbligo.
6. Il SAT si impegna ad adottare le misure richieste dall'Art. 32 del GDPR secondo le istruzioni impartite
7. Tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito delle strutture del Titolare, pur non essendo dipendenti o titolari di incarichi conferiti dall'Azienda (es.: consulenti, tirocinanti, borsisti, collaboratori in genere), devono essere autorizzati al trattamento dei dati personali: in base a quanto previsto dallo specifico rapporto giuridico (contratto, convenzione o altro), tali autorizzazioni potranno essere concesse dal soggetto esterno (es.: Responsabile del Trattamento) o dal Titolare o da suoi delegati (SATD). A titolo esemplificativo, ci si riferisce al personale tirocinante o al personale volontario che opera temporaneamente all'interno della struttura del Titolare in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato (es. Associazione di volontariato o Ente universitario) per lo svolgimento di tirocini formativi/ attività di volontariato a sostegno dei pazienti ricoverati nei reparti ospedalieri.
8. Detto personale è soggetto agli stessi obblighi cui sono sottoposti tutti i SAT, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
9. Ulteriori dettagli relativi alla designazione dei Soggetti Autorizzati al Trattamento (SAT) sono specificati nella Procedura di Gestione delle Nomine e Designazioni allegata al presente Regolamento.

ART. 18 PERSONA FISICA ESTERNA ALLA STRUTTURA DEL TITOLARE AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI

1. Tutto il personale non dipendente dell'Azienda che presta comunque attività all'interno dell'Azienda stessa a qualsiasi titolo (es.: personale addetto alle pulizie), con o senza retribuzione, qualora in ragione della propria attività venga a conoscenza di dati personali trattati dall'Azienda o possa accedere ai locali di trattamento dati è tenuto al rispetto del presente Regolamento e, in particolare:
   a) deve mantenere la massima riservatezza sulle notizie e le informazioni di cui venga a conoscenza;
   b) deve astenersi dall'effettuare operazioni di trattamento dei dati salvo che non sia individuato quale SAT.

ART. 19 DIRITTI DELL'INTERESSATO

1. La materia in oggetto viene regolamentata dall'Azienda attraverso la procedura per l'esercizio dei Diritti in Materia di Protezione dei Dati Personali dell'interessato ai Sensi degli Artt. 15 - 22 del Regolamento UE 679/2016", allegata al presente Regolamento.

ART. 20 UFFICIO PRIVACY

1. L'Azienda individua al proprio interno un Ufficio Privacy, garantendogli le risorse umane e strumentali necessarie per l'efficace ed ottimale assolvimento dei compiti assegnati.
2. L'Ufficio Privacy viene istituito con atto del Direttore Generale, su proposta del Direttore Amministrativo, ed è composto da soggetti di ruolo amministrativo/tecnico (scelti tra i dirigenti o i funzionari) che garantiscano, per la loro elevata esperienza e alta capacità professionale il pieno rispetto delle disposizioni in materia di riservatezza.

3. L'Ufficio Privacy svolge i seguenti compiti:
   a) Supporta il Titolare ed il Responsabile della Protezione Dati per la gestione di tutti gli adempimenti amministrativi relativi alla normativa in materia di Protezione dei Dati Personali;
   b) coadiuva il Titolare e il DPO nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali
   c) promuove l'osservanza del Regolamento aziendale sulla privacy fornendo la necessaria consulenza in ordine alle problematiche in tema di protezione dei dati;
   d) provvede alla gestione della produzione regolamentare interna in materia di trattamento dati;
   e) su richiesta del Titolare e/o proposta del DPO propone, svolge e coordina l'attività di formazione in tema di normativa sulla protezione dei dati, assicurando la promozione della cultura della privacy a livello aziendale;
   f) provvede all'adeguamento dei percorsi e delle procedure aziendali per quanto attiene l'aspetto della protezione dei dati;
   g) collabora con il DPO nella gestione delle istanze dell'interessato e delle controversie sui dati personali e, più in generale, in tema di protezione, avanzate dall'interessato al Titolare del trattamento;
   h) provvede alla redazione e tenuta del Registro dei Trattamenti, secondo quanto previsto dall'art. ART. 10.4, avvalendosi della collaborazione con le seguenti figure: i Soggetti Autorizzati al Trattamento dei Dati Personali con Delega, il Dirigente responsabile dell'UOSD Sistemi Informativi e gli Amministratori di sistema;
4. Nell'esercizio delle competenze di cui ai punti precedenti deve essere garantito all'Ufficio Privacy l'apporto di tutte le articolazioni organizzative dell'Azienda.

ART. 21 STRATEGIA PER LA TENUTA IN SICUREZZA DEI DATI

1. L'Azienda persegue l'obiettivo strategico del mantenimento di adeguate condizioni di sicurezza dei dati trattati attraverso:
   a) la predisposizione del Piano Aziendale per la Sicurezza Informatica;
   b) il sistematico raccordo del Responsabile della Transizione Digitale con il DPO per la definizione delle modalità di intervento informativo rivolte ai SATD e ai Responsabili del trattamento
   c) la sistematica verifica da parte dei SATD in collaborazione con il Responsabile della Transizione Digitale - che agirà di concerto con il Dirigente responsabile UOSD Sistemi Informativi e gli Amministratori di Sistema - dell'applicazione delle misure di sicurezza individuate nel Piano Aziendale per la Sicurezza Informatica e nelle indicazioni/direttive ulteriormente impartite.
2. Le misure di sicurezza previste nel Piano di cui al comma 1 devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1, del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso") da integrare e/o attuare in funzione delle condizioni previste dall'articolo stesso e dal contesto aziendale.

ART. 22 MISURE DI SICUREZZA INFORMATICHE GENERALI

1. Il trattamento di dati personali a mezzo di strumenti elettronici è consentito ai SAT dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione possono consistere in:
   a) un codice per l'identificazione del SAT associato a una parola chiave riservata conosciuta solamente dal medesimo;
   b) un dispositivo di autenticazione in possesso e uso esclusivo del SAT, eventualmente associato a un codice identificativo o a una parola chiave;

c) una caratteristica biometrica del SAT, eventualmente associata a un codice identificativo o a una parola chiave.

3. Il SATD richiede all'Amministratore di Sistema l'attivazione della credenziale di autenticazione informatica per i propri SAT, specificando a quali dati e tipi di operazioni ciascun SAT deve poter accedere in relazione ai propri compiti (c.d. profilo di autorizzazione). Periodicamente e comunque almeno annualmente il SATD verifica la sussistenza per la conservazione dei profili di autorizzazione, dandone formale comunicazione all'Amministratore di sistema.
4. Lo stesso codice per l'identificazione, quando tale misura venga adottata, non può essere assegnato ad altri SAT, neppure in tempi diversi.
5. Ove ricorrano le condizioni, il potere sostitutivo del SATD si esercita con le seguenti modalità:
   a) la funzione di custode delle copie delle credenziali di autenticazione (per i soli sistemi non associati al Dominio informatico interno e per i soli sistemi per i quali non sia prevista la figura di Amministratore di Sistema) è posta in capo al SATD di riferimento o a propri collaboratori formalmente individuati;
   b) il SATD provvede per iscritto all'attribuzione della funzione di cui al punto precedente;
   c) il custode utilizza le credenziali solo ove sussistano i presupposti tassativamente individuati dalla normativa di settore;
   d) il custode o l'Amministratore di Sistema – in base ai casi specificati al comma 5.a) del presente articolo – , previa redazione di un verbale, accedono al computer o all'applicativo informatico – es.: posta elettronica – del SAT e a conclusione delle operazioni necessarie provvedono ad immettere una nuova password provvisoria e a spegnere il computer;
   e) il SATD informa tempestivamente il SAT dell'effettuazione dell'intervento;
   f) il SAT ha l'obbligo di sostituire la precedente password.
6. La gestione delle misure di sicurezza adottate dall'Azienda è disciplinata dal Piano di Sicurezza, allegato al presente Regolamento, predisposto e conservato agli atti dall'UOSD Sistemi Informativi.

ART. 23 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

1. Ai sensi dell'art. 32.1 del Regolamento UE, le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento.
2. Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento.
3. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.
4. All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del Titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del Titolare fino alla limitazione o al divieto di procedere al trattamento.
5. Il Piano di Sicurezza allegato al presente Regolamento, in fase di prima attuazione, viene considerato dall'Azienda come Valutazione di Impatto sulla Protezione dei Dati Personali.

ART. 24 ACCORGIMENTI E SOLUZIONI PARTICOLARI IN AMBITO SANITARIO

1. Le comunicazioni e le informazioni sulle specifiche patologie dell'interessato possono essere rese a quest'ultimo solo tramite:
   a) il competente medico dell'Azienda;

b) un medico di fiducia dell'interessato da questi designato;
c) altro operatore sanitario dell'Azienda che abbia rapporti diretti con il paziente e che sia stato autorizzato per iscritto dal SATD a effettuare la comunicazione.

2. Nel caso di cui al precedente comma 1, lett c) l'autorizzazione è disposta all'atto della designazione dell'operatore quale SAT da parte del SATD che ne individua limiti, modalità e cautele ai sensi della vigente normativa di settore.
3. Nel caso in cui l'interessato si trovi in stato di impossibilità fisica, di incapacità di agire, di incapacità di intendere e di volere le comunicazioni e le informazioni di cui al comma 1 sono rese a chi dimostri di esercitare legalmente la potestà ovvero di essere un congiunto prossimo, un familiare, un convivente o, in assenza di questi, il Responsabile della struttura presso cui dimora l'interessato.
4. In costanza di ricovero, le informazioni di cui al comma 1 possono essere rese a familiari o a terzi soltanto previa autorizzazione scritta dell'interessato acquisita su apposito modulo di Consenso al trattamento dei dati da inserire in cartella clinica.
5. Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.
6. In ogni Presidio Ospedaliero/Strutture Residenziali e Semiresidenziali/Distretto/Ufficio dell'Azienda devono essere adottate soluzioni procedurali/organizzative atte a garantire la riservatezza degli utenti in occasione della richiesta o della fruizione di prestazioni sanitarie o di servizi amministrativi ad esse correlate.
7. I Direttori/Responsabili delle strutture di cui al cui punto che precede sono tenuti a porre in essere misure atte a garantire che le informazioni di natura sanitaria rese verbalmente (chiamata dei pazienti, indagine anamnestica, colloqui con familiari, etc..) o mediante supporto cartaceo (documentazione sanitaria) non siano accessibili da parte di soggetti terzi non espressamente autorizzati dagli interessati.
8. I SATD in ambito sanitario, devono inoltre:
   a) adottare soluzioni volte a rispettare un ordine di precedenza o di chiamata prescindendo dalla individuazione nominativa;
   b) assumere le dovute cautele volte ad evitare che le prestazioni sanitarie, comprese la raccolta delle anamnesi, avvengano in situazioni di promiscuità;
   c) rispettare la dignità dell'interessato durante la prestazione medica e in ogni operazione di raccolta dei dati;
   d) adottare accorgimenti opportuni per garantire che le informazioni sulle prestazioni di Pronto Soccorso e sulla dislocazione dell'interessato nell'ambito delle Unità Operative vengano fornite esclusivamente a terzi legittimati, rispettando comunque contrarie manifestazioni di volontà dell'interessato;
   e) attivare procedure dirette a prevenire che a terzi estranei possano essere forniti elementi di correlazioni fra reparti o strutture e l'interessato indicativi dell'esistenza di un particolare stato di salute;
   f) sottoporre i SAT che non siano tenuti per legge al segreto professionale a regole di condotte analoghe.
9. Le strutture ospedaliere/territoriali possono rilasciare anche telefonicamente informazioni sui degenti, limitatamente alla loro presenza e alla loro collocazione all'interno della struttura, solo previa autorizzazione scritta dell'interessato acquisita tramite il modulo di cui al precedente punto 4 (Consenso) indicato dalla Procedura di Gestione delle Informative e dei Consensi allegata al presente Regolamento.

ART. 25 TRATTAMENTI PER RICERCA SCIENTIFICA E PER FINI STATISTICI

1. Nella conduzione di sperimentazioni cliniche di medicinali di cui al D. lgs 24 giugno 2003, n. 211, al D. Lgs. 6 novembre 2007, n.200 o riferibili ad altra normativa specifica di settore, l'Azienda, fatte salve le ipotesi espressamente previste dalla normativa, può effettuare la comunicazione dei dati personali dei partecipanti allo studio, o consentirne comunque l'accessibilità, unicamente nei confronti del Promotore

e dei collaboratori esterni di cui questi si avvalga in qualità di Responsabili o SAT per lo svolgimento delle attività, o parti di attività, inerenti lo studio stesso, previo consenso dell'interessato.

2. I trattamenti di dati relativi a ricerca medica, biomedica ed epidemiologica dovranno essere conformi a quanto previsto dall'art. 110 del Codice
3. I trattamenti di dati personali ulteriori da parte di terzi a fini di ricerca scientifica o a fini statistici dovranno essere conformi a quanto previsto dall'art. 110-bis del codice

ART. 26 FORMAZIONE

1. L'Azienda individua nella specifica formazione del personale un elemento strategico della propria politica in materia di protezione dei dati personali. La formazione può essere erogata sia ricorrendo a risorse interne che avvalendosi dell'intervento di risorse esterne e può avvenire sia attraverso la presenza in aula che in modalità e.learning.
2. Nell'ambito della programmazione degli interventi di formazione del personale, sono garantiti a tutti i dipendenti, in relazione ai distinti ruoli privacy, interventi di formazione in materia di tutela della riservatezza e protezione dei dati finalizzati alla conoscenza della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza dei rischi e delle misure di sicurezza per prevenirli.
3. Alla formazione di base e programmata di cui al punto 2 si affiancano ulteriori interventi formativi da realizzarsi ove intervengano:
   a) innovazioni legislative (modifiche/integrazioni della normativa in materia di privacy o disposizioni normative comunque di impatto sul trattamento dei dati);
   b) rilevanti posizioni giurisprudenziali o interpretative di impatto su determinati trattamenti;
   c) introduzione di nuove tecnologie o modalità di trattamento.
4. L'offerta formativa viene definita dal Titolare in collaborazione con il DPO, l'Ufficio Privacy, la struttura deputata alla formazione aziendale ed i SATD. Devono essere tenute in considerazione anche le proposte che perverranno dal Responsabile della UOSD Sistemi Informativi/Responsabile della Transizione Digitale.

ART. 27 NOTIFICA DI UNA VIOLAZIONE DI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

1. L'Azienda, in qualità di Titolare del trattamento di dati personali ha l'obbligo di notificare all'Autorità di controllo le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritenga probabile che da tale violazione derivi rischi per i diritti e le libertà degli interessati (cd. "Data Breach").
2. La notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Titolare.
3. Se la probabilità del rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34 del Regolamento UE. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del Regolamento UE.
4. Il Titolare del trattamento, sentito il D.P.O. aziendale, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.
5. Ulteriori dettagli e le modalità sono indicate nella Procedura per la Gestione delle Violazioni di Dati Personali allegata al presente Regolamento.

ART. 28 RINVIO

1. Per quanto non espressamente previsto dal presente Regolamento trovano applicazione le seguenti disposizioni:

a) Regolamento UE 2016/679;
b) D. lgs 196/2003 "Codice in materia di protezione dei dati personali" così come modificato dal D.lgs. n. 101/2018;
c) Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

ART. 29 ABROGAZIONI

1. Si intendono, revocate tutte le disposizioni aziendali difformi da quelle del presente Regolamento

ART. 30 NOTE FINALI

1) Il testo del presente Regolamento (composto di 31 articoli) potrà essere aggiornato con atto deliberativo del Direttore Generale, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa in materia di protezione dati.
2) I n.7 (sette) allegati al presente Regolamento, inclusivi della relativa modulistica, data la loro caratteristica di essere strumenti di lavoro dinamici, potranno essere soggetti a modifiche e revisioni che non necessitano dell'adozione di un nuovo atto deliberativo; esse avverranno attraverso il ricorso a note – assunte al Registro di Protocollo Informatico generale della Asl di Avezzano – Sulmona – L'Aquila - a firma del Direttore Generale e saranno pubblicate sul sito aziendale alla voce Protezione dei Dati Personali.

ART. 31 ALLEGATI

Allegato	Descrizione
A	PRY-REG-001 - Registro dei Trattamenti di riepilogo
B	PRY-DOC-002 - Piano di Sicurezza
C	PRY-PRD-001 - Procedura di Gestione delle Violazioni di Dati Personali e Modelli Allegati
D	PRY-PRD-002 - Procedura per l'esercizio dei diritti degli interessati e Modelli Allegati
E	PRY-PRD-003 - Procedura per la Gestione delle Informative e Consensi e Modelli Allegati
F	PRY-PRD-004 - Procedura di Gestione di Accordi, Nomine e Designazioni e Modelli Allegati
G	PRY-MOD-017 - Clausola di Garanzia da inserire nei contratti con Terzi

Allegato C

al Regolamento Aziendale per la protezione dei dati personali della ASL 01 Abruzzo

Procedura di Gestione delle Violazioni di Dati Personali e Modelli Allegati

Procedura

per la Gestione delle

Violazioni di Dati Personali (Data Breach)

della Asl di Avezzano – Sulmona L'Aquila

in base a quanto previsto dal

Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) e D.Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali e ss.mm.ii.

Allegato 3 – Regolamento Aziendale per la Protezione dei Dati Personali

Sommario

1 Introduzione ... 3
2 Scopo ... 3
3 Campo di Applicazione ... 3
4 Definizioni ... 4
5 Normativa di Riferimento ... 6
5.1 Articolo 33 – Notifica di una violazione dei dati personali all'autorità di controllo ... 6
5.2 Articolo 34 – Comunicazione di una violazione dei dati personali all'interessato ... 6
6 Team di Risposta alle Violazioni ed elementi di valutazione ... 8
6.1 Team di Risposta alle Violazioni (Data Breach Response Team – DBRT) ... 8
6.2 Informazioni preliminari per la valutazione delle violazioni ... 9
7 Descrizione del Processo ... 10
7.1 Rilevazione della Violazione di Dati Personali ... 10
7.2 Gestione della violazione (Valutazione e Decisione) ... 11
7.3 Documentazione della violazione ... 14
7.4 Analisi post violazione ... 14
8 Flusso operativo ... 16
9 Data Breach presso l'Azienda quando opera in qualità di Responsabile del Trattamento ... 17
10 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) che da "particolari categorie di dati personali" quali i dati relativi alla salute.
La ASL n.01 di Avezzano - Sulmona - L'Aquila (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, per poter rispettare quanto previsto dagli artt. 33 e 34 del Regolamento: in particolare viene definito un flusso di attività da attivarsi nel caso in cui dovesse manifestarsi un evento di violazione dei dati personali rispetto a quanto definito esplicitamente dalla normativa vigente o dalle regolamentazioni interne dell'Azienda Sanitaria.

L'obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle Violazioni di Dati Personali e delle relative indicazioni operative immediate per poter procedere con la rilevazione, la valutazione ed il contenimento della violazione; viene inoltre valutata la necessità di dover procedere con la comunicazione all'Autorità Garante per la Protezione dei Dati Personali ed eventualmente all'interessato.

3 Campo di Applicazione

Per Violazione di Dati Personali (cd. "Data Breach") si intende *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.*

Il presente documento determina il processo di gestione delle violazioni di dati personali che possono accadere al manifestarsi di eventi come i seguenti (a titolo esemplificativo e non esaustivo):

- accesso non autorizzato ai dati personali;
- azioni accidentali o deliberate da parte dei soggetti autorizzati al trattamento;
- invio dei dati a un destinatario errato;
- perdita o furto di dispositivi di memoria o computer portatili che contengono dati personali;
- alterazione non autorizzata dei dati personali;
- perdita della disponibilità dei dati personali.

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;

«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;

«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;

«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;

«SATD»: Soggetto Autorizzato al Trattamento di dati personali con Delega da parte del titolare;

«SAT»: Soggetto Autorizzato al Trattamento di dati personali.

5 Normativa di Riferimento

Il processo contenuto nel presente documento descrive i passi da seguire nel caso si verifichi un evento di Violazione del Dati Personali in conformità con quanto indicato dagli artt. 33 e 34 del Regolamento che stabiliscono i seguenti obblighi:

- obbligo di notifica all'Autorità Garante "senza ingiustificato ritardo" e, ove possibile, entro 72 ore (art. 33 del Regolamento);
- obbligo di comunicazione agli interessati quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 34 del Regolamento).

5.1 Articolo 33 – Notifica di una violazione dei dati personali all'autorità di controllo

*1. In caso di **violazione dei dati personali**, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 (del Regolamento) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

5.2 Articolo 34 – Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33 (del Regolamento), *paragrafo 3, lettere b), c) e d).*

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

6 Team di Risposta alle Violazioni ed elementi di valutazione

6.1 Team di Risposta alle Violazioni (Data Breach Response Team – DBRT)

Il Team di Risposta alle Violazioni è una entità multidisciplinare composta da soggetti che presentano conoscenze e competenze tali da assumersi la responsabilità per valutare e porre in essere le misure di contenimento delle conseguenze negative della violazione.

La composizione del Team è costituita in maniera fissa da referenti delle strutture organizzative direttamente coinvolte nella gestione della Protezione dei Dati Personali e opzionalmente, su richiesta da parte dei componenti di base del Team, da ulteriori eventuali funzioni che verranno interessate in base alle specifiche necessità (es.: UOC Affari Generali e Legali, UOC Ingegneria Clinica, UOC Personale, UOC Beni e Servizi).

Team di Risposta alle Violazioni		
Funzione	**Competenza**	**Partecipazione**
UOSD Sistemi Informativi / Responsabile della Transizione Digitale	Conoscenza dell'infrastruttura di rete, delle misure di sicurezza idonee adottate e delle infrastrutture tecnico-applicative impiegate per il trattamento dei dati	Coordinatore e Componente di base
Data Protection Officer	Responsabile della Protezione dei Dati Personali.	Componente di base
Ufficio Privacy	Ufficio competente per il mantenimento della compliance alle normative privacy nazionali ed europee	Componente di base
Direttore/Responsabile della struttura organizzativa in cui si è verificato l'evento (SATD)	Può fornire ulteriori informazioni e supporto per un efficace risposta all'incidente	Componente di base

In caso di violazioni di dati personali che presentino una particolare gravità (tali da richiedere la comunicazione al Garante per la Protezione dei Dati Personali ed eventuale comunicazione agli interessati) deve essere coinvolto anche il Legale Rappresentante della ASL.

Il Team deve assicurare un'adeguata tempestività nella risposta alle violazioni, oltre a fornire tutte le risorse per il contrasto dell'evento e la preparazione per la risposta.

Se necessario, i membri del Team possono farsi aiutare da team esterni, come ad esempio società che si occupano di sicurezza informatica, società di analisi forense dei dati etc.

Opzionalmente, in base alle necessità, il coordinatore può integrare ulteriore personale (interno o esterno) nel team se utile al contrasto di una specifica violazione

Il Team di Risposta alle Violazioni (Data Breach Response Team) deve essere preparato alla risposta di presunte o accertate violazioni; di seguito vengono riportati i dati di contatto di ogni membro facente parte del Team.

Funzione	**Nome**	**Telefono**	**Mail**
UOSD Sistemi Informativi / Responsabile della	Ing. Maurizio Di Stefano	0862-368754	databreach@asl1abruzzo.it

Transizione Digitale		
Data Protection Officer	Ing. Nicola Barberini	328-3607738
Ufficio Privacy	Dott.ssa Emanuela Modestini Dott. Marco Di Girolamo	0864-499319 0863-499563

I dipendenti della ASL sono comunque tenuti a dare tempestivamente notizia della possibile violazione anche al Direttore/Responsabile della struttura organizzativa in cui si è verificato l'evento.

6.1.1 Compiti del Team

A valle della segnalazione della violazione, il Team dovrà:

- validare/rispondere alla violazione;
- predisporre un'appropriata e imparziale investigazione, documentandola correttamente;
- identificare gli eventuali asset da bonificare e tenere traccia delle misure da porre in essere per risolvere le vulnerabilità;
- coordinarsi con le autorità se necessario;
- coordinarsi per la comunicazione verso l'interno e verso l'esterno;
- preoccuparsi di rispettare gli obblighi di notifica e comunicazione;
- analizzare ogni incidente e tenere traccia della Violazione nel registro.

6.2 Informazioni preliminari per la valutazione delle violazioni

Nell'ambito delle valutazioni relative alla gravità (*severity*) delle violazioni dovranno essere tenuti in considerazione i seguenti fattori di rischio per i diritti e le libertà dei soggetti interessati:

a) tipologia violazione: la tipologia di violazione si configura come parametro per la valutazione del rischio. (es. la violazione dei dati sanitari di tutti i pazienti è più grave della perdita dei dati sanitari di un paziente);
b) natura, numero e grado di sensibilità dei dati personali violati;
c) facilità di associazione dei dati violati all'interessato: facilità di associazione dei dati violati ad una determinata persona fisica;
d) gravità delle conseguenze per gli interessati: valutazione relativa al rischio che i dati personali violati rappresentino un rischio immediato per gli interessati, tale da porre in essere frodi o sostituzioni di persona;
e) numero di interessati esposti al rischio;
f) caratteristiche del titolare del trattamento (in base al contesto dell'Azienda).

In particolare per "Tipologie di Violazioni" si intende:

- Violazione sulla Riservatezza (cd. *Confidentiality Breach*) accesso accidentale o illecito ai dati personali o divulgazione degli stessi;
- Violazione sulla Disponibilità (cd *Availibility Breach*) perdita o distruzione accidentale o illecita del dato personale;
- Violazione sull'Integrità (cd *Integrity Breach*) quando vi è una modifica accidentale o non autorizzata del dato personale.

7 Descrizione del Processo

Il processo contenuto nel presente documento descrive i passi da seguire nel caso si verifichi un evento di Violazione dei Dati Personali in conformità con quanto stabilito dagli Artt.33, 34 del Regolamento.

Il processo si articola nelle seguenti fasi:

- Rilevazione di una Violazione di Dati Personali;
- Gestione della Violazione (Valutazione e Decisione);
- Risposta all'evento;
- Notifica all'Autorità Garante;
- Comunicazione agli Interessati;
- Documentazione della Violazione.

7.1 Rilevazione della Violazione di Dati Personali

Le segnalazioni di eventi che portano a violazioni sui dati personali possono avvenire per canali interni ed esterni:

1) Canali interni

Le segnalazioni di eventi anomali possono provenire internamente da:

- Personale dell'organizzazione: le violazioni di dati personali sono gestite dall'Ufficio Privacy per conto del Titolare del trattamento, con il coordinamento del Responsabile dell'UOSD Sistemi Informativi e con il supporto del Responsabile della Protezione Dati (DPO). In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenirne il ripetersi.
  Nel caso in cui un Soggetto Autorizzato al Trattamento dei Dati si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il proprio responsabile (Soggetto Autorizzato al Trattamento con Delega) della possibile violazione. Quest'ultimo dovrà quindi informare l'Ufficio Privacy, l'UOSD Sistemi Informativi ed il Responsabile Protezione Dati (DPO) mediante la compilazione dell'Allegato 1 Modulo di documentazione interna della Violazione da inviare all'indirizzo databreach@asl1abruzzo.it .
- UOSD Sistemi Informativi mediante opportuni strumenti di monitoraggio di eventi di natura Software e ICT: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dai sistemi di security ICT aziendale. Tali eventi relativi ai sistemi ICT sono sotto responsabilità e conseguentemente monitorati e gestiti dall'UOSD Sistemi Informativi e da Amministratori di Sistema opportunamente incaricati. In caso di rilievo di concreta, sospetta e/o avvenuta violazione dei dati personali relativi ai sistemi ICT aziendali, l'Amministratore di Sistema, o il Soggetto Autorizzato al Trattamento dei Dati Personali autorizzato al monitoraggio degli eventi informatici, deve immediatamente informare il proprio responsabile (Responsabile dell'UOSD Sistemi Informativi), l'Ufficio Privacy ed il Responsabile Protezione Dati (DPO) mediante la compilazione dell'Allegato 1 – Modulo di documentazione interna della Violazione da inviare all'indirizzo databreach@asl1abruzzo.it.

2) Canali esterni

Le segnalazioni di eventi anomali possono pervenire anche dell'esterno:

- Segnalazione dall'interessato: il soggetto interessato dal trattamento può effettuare una segnalazione anche in caso di semplice sospetto che i propri dati personali siano stati utilizzati in maniera fraudolenta da terzi o in generale che siano stati oggetto di violazione. In questi casi, l'interessato

dovrà rivolgersi al Titolare per la verifica di eventuali violazioni inviando l'Allegato 5 alla presente procedura all'indirizzo databreach@asl1abruzzo.it . Tale modulo è reso disponibile sul sito istituzionale http://www.asl1abruzzo.it/ nella sezione "Protezione Dati Personali".

- Segnalazione dal Responsabile del Trattamento: il Responsabile del Trattamento, in caso si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il proprio referente (Soggetto Autorizzato al Trattamento con Delega – SATD Referente) della possibile violazione; il Responsabile è tenuto ad assistere il SATD nell'informare l'Ufficio Privacy, l'UOSD Sistemi Informativi ed il Responsabile Protezione Dati (DPO) mediante la compilazione dell'Allegato 1 – Modulo di documentazione interna della Violazione da inviare all'indirizzo email databreach@asl1abruzzo.it ed all'indirizzo PEC protocollogenerale@pec.asl1abruzzo.it.

7.2 Gestione della violazione (Valutazione e Decisione)

La gestione di una violazione dei dati personali è stata standardizzata in un processo suddiviso nelle seguenti quattro fasi:

1) Analisi preliminare delle segnalazioni;
2) Risk assessment, individuazione misure e contenimento della violazione;
3) Notifica all'Autorità Garante;
4) Comunicazione agli interessati;

7.2.1 Analisi preliminare delle segnalazioni

Il gruppo di lavoro incaricato della valutazione delle segnalazioni di Violazioni di Dati Personali è il cosiddetto Team di Risposta alle Violazioni che effettuerà una analisi preliminare delle informazioni relative alla presunta violazione, avendo in tal modo un quadro strutturato dell'anomalia segnalata.
A seguito della ricezione della segnalazione, il Titolare del trattamento, per il tramite del Responsabile dell'UOSD Sistemi Informativi, effettua la registrazione e l'identificazione univoca della segnalazione, utilizzando l'apposito registro allegato alla presente procedura (Allegato 2). Il Team, con la partecipazione di tutti i suoi componenti, procede ad effettuare una valutazione preliminare riguardante la possibile violazione occorsa, al fine di stabilire se si sia effettivamente verificata un'ipotesi di Violazione (Data Breach) e se sia necessaria un'indagine più approfondita dell'accaduto.
Nel caso in cui l'evento venga accertato come "falso positivo", la procedura di verifica viene chiusa e l'evento viene classificato opportunamente all'interno del registro delle Violazioni.
Nel caso in cui la violazione venga accertata, il Team procede al recupero di tutte le informazioni disponibili relative alla violazione ed informa, tramite il suo coordinatore, il Titolare del trattamento senza ingiustificato ritardo.

NB: per eseguire una migliore valutazione della violazione e dei suoi impatti per i soggetti interessati, devono essere tenuti in considerazione i seguenti aspetti:

a) la presenza di:
   - dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale,
   - dati genetici,
   - dati biometrici intesi a identificare in modo univoco una persona fisica,
   - dati relativi alla salute o dati relativi alla vita sessuale
   - dati relativi a condanne penali e a reati o
   - dati relativi alle misure di sicurezza utilizzate per la protezione;
b) la presenza, altresì, di:

- dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- dati di persone fisiche vulnerabili, in particolare minori;

c) il trattamento di notevoli quantità di dati personali;
d) il trattamento di dati personali di un vasto numero di Interessati.

Nel caso in cui si individuasse una possibile violazione di dati contenuti in un sistema informatico (ICT), il Responsabile dell'UOSD Sistemi Informativi inoltrerà la segnalazione, oltre al Responsabile della Protezione dei Dati, anche all'Amministratore di Sistema di competenza per effettuare una istruttoria e le valutazioni in merito all'accaduto.
Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato 1, quali:

- la data di scoperta della violazione (tempestività);
- il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

7.2.1.1 Azioni di Contenimento

Nel caso di eventi che coinvolgano sistemi ICT, alcune best practices da attuare come primo approccio alle violazioni sono elencate nei punti che seguono:

1. contenimento dei dispositivi compromessi inettendoli *offline* distaccandoli dalla rete aziendale;
2. censimento delle macchine che sono state violate;
3. individuazione di quali vulnerabilità siano state sfruttate per violare i dispositivi ed eventualmente gli apparati di rete coinvolti;
4. raccolta delle evidenze per il Garante in modo tale da dimostrare quali misure siano state impiegate e quali azioni siano state attuate durante l'evento;
5. ripristino dei sistemi e delle reti;
6. integrazione delle informazioni raccolte per l'individuazione di nuove misure per far si che l'incidente non avvenga in futuro.

7.2.2 Risk assessment e individuazione delle misure

A termine della fase di valutazione preliminare, nel caso si stabilisca che una possibile violazione sia effettivamente avvenuta, il Team (in caso di *violazioni informatiche* unitamente all'Amministratore di sistema di competenza), stabilisce:

- le opportune misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- le modalità e le tempistiche di suddette misure, individuando gli attori e i compiti per limitare la violazione;
- la necessità di notifica dell'evento all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- la necessità di comunicazione dell'evento agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notifica all'Autorità Garante e di comunicazione agli interessati, il Team valuta la gravità della violazione utilizzando un modello standardizzato, come da Modulo di valutazione del Rischio connesso al Data Breach (Allegato 3), secondo le indicazioni di cui all'art. 33 GDPR.

Si precisa che gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio tale da essere *non trascurabile* (Rischio Alto – Allegato 3); l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato (Rischio Critico – Allegato 3).

7.2.3 Notifica all'Autorità Garante competente

Se a seguito delle valutazioni preliminari e del risk assessment effettuato nel rispetto della presente procedura, si rileva la necessità di effettuare la notifica della *violazione dei dati*, secondo quanto prescritto dal Regolamento UE, il Titolare del trattamento, con il supporto del Responsabile Protezione Dati e dell'Ufficio Privacy, provvederà alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore (48 ore nel caso di violazione dei dati relativi al Dossier Sanitario) dal momento in cui ne è venuto a conoscenza.

La notifica al Garante, come di seguito strutturata, deve essere inviata a mezzo PEC al seguente indirizzo protocollo@pec.gpdp.it. Essa deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le stesse saranno fornite in fasi successive non appena disponibili e senza ritardo.

Per effettuare la notifica all'autorità Garante della Violazione deve essere utilizzato l'allegato n.4 alla presente procedura.

7.2.4 Comunicazione agli interessati

Se a seguito delle valutazioni preliminari e del risk assessment effettuato nel rispetto della presente procedura, si rileva la necessità di effettuare la comunicazione della violazione dei dati agli interessati, in quanto riscontrato un rischio elevato per i diritti e le libertà delle persone fisiche, secondo quanto prescritto dal Regolamento UE, il Titolare del trattamento, con il supporto del Responsabile Protezione Dati e dell'Ufficio Privacy, provvederà alla comunicazione all'Interessato senza ingiustificato ritardo.

Il contenuto della comunicazione prevede:

- il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Secondo quanto previsto dall'art. 34.3 del Regolamento UE, nei seguenti casi non è richiesta la comunicazione all'interessato:

a) *il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
b) *il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;*
c) *detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*

Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato – punto c) del precedente elenco –, si potrà utilizzare una comunicazione pubblica (es.: pubblicazione sul sito istituzionale), che dovrà essere ugualmente efficace nel contatto diretto con l'interessato

Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui all'art. 34.3 sia soddisfatta.

7.3 Documentazione della violazione

Indipendentemente dalla valutazione della necessità di procedere alla notifica e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un evento (es.: incidente sulla sicurezza delle informazioni) la ASL è tenuta a documentarlo.

Tale documentazione sarà conservata presso l'Ufficio Privacy per opportuna consultazione da parte del Responsabile della Protezione dei Dati e del Responsabile dell'UOSD Sistemi Informativi.

La registrazione degli eventi, come precedentemente indicato, dovrà essere effettuata, da parte del Responsabile dell'UOSD Sistemi Informativi, nell'apposito Registro delle Violazioni, in cui saranno riportate le seguenti informazioni:

- numero registrazione segnalazione;
- data segnalazione;
- segnalatore e Unità Operativa di appartenenza;
- valutazione;
- notifica all'Autorità Garante Privacy;
- comunicazione agli interessati.

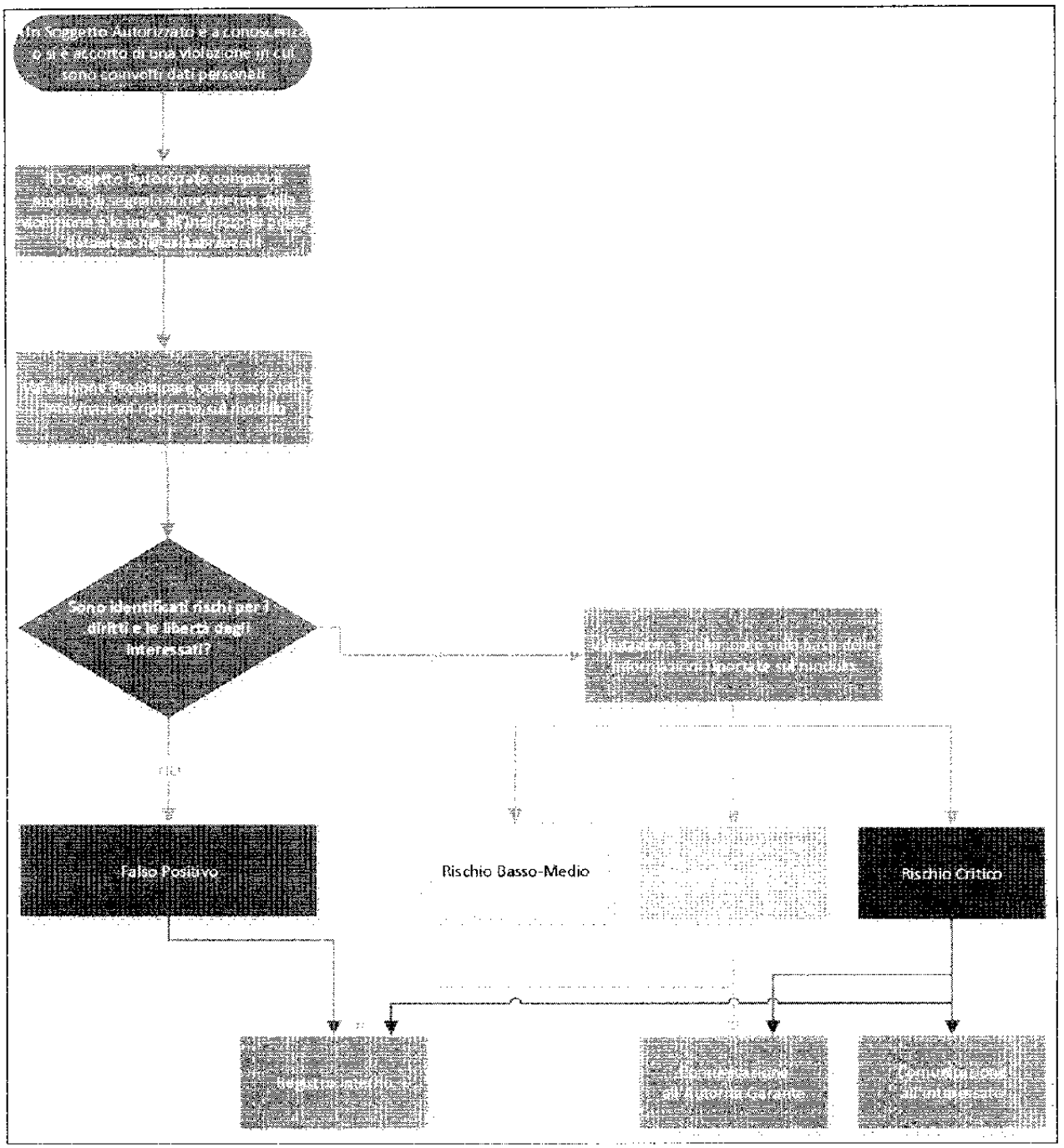
Il Registro delle Violazioni (il cui modello è indicato nell'allegato 2 al presente documento) sarà continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

7.4 Analisi post violazione

Al fine di verificare l'efficacia delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento, dopo aver posto in essere i precedenti adempimenti, è necessario procedere alla

raccolta finale delle evidenze, all'analisi delle informazioni giunte sul contesto di violazione osservato e alla valutazione delle stesse.

8 Flusso operativo



9 Data Breach presso l'Azienda quando opera in qualità di Responsabile del Trattamento

Qualora la ASL agisca in qualità Responsabile del Trattamento, in caso di Violazione dei Dati Personali, sarà tenuta ad informare il Titolare del trattamento senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo.

10 Allegati

Alla presente procedura sono allegati i seguenti moduli:

- Allegato 1 - PRY-MOD-002 – Segnalazione Interna della Violazione
- Allegato 2 - PRY-MOD-003 – Registro Segnalazioni delle Violazioni
- Allegato 3 - PRY-MOD-004 – Modulo di Valutazione della Segnalazione di Dati Personali
- Allegato 4 - PRY-MOD-005 – Modello notifica Data Breach
- Allegato 5 - PRY-MOD-006 – Segnalazione della Violazione da parte dell'Interessato

Azienda Sanitaria Locale Avezzano, Sulmona, L'Aquila

REGIONE ABRUZZO – ASL 1 AVEZZANO SULMONA L'AQUILA

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI
ALLEGATO 1 – MODULO DI DOCUMENTAZIONE INTERNA DELLA VIOLAZIONE DI DATI PERSONALI
ai sensi dell'art. 33 del Regolamento UE 679/2016 (GDPR)

Modulo di documentazione interna della Violazione di Dati Personali

Nome soggetto che riporta l'incidente	
Unità Operativa di appartenenza	
Numero di contatto del soggetto che riporta l'incidente ed indirizzo di posta elettronica	
Data dell'evento ed orario (anche approssimativo)	
Data e ora in cui si è venuti a conoscenza della violazione	
Fonte della segnalazione	
Tipologia di anomalia riscontrata	
Descrizione dell'anomalia	
Numero di soggetti coinvolti	

Numero dei dati personali di cui si presume il coinvolgimento	
Tipologia di dati personali che si ritiene essere stati coinvolti	**Basso Rischio**: **Alto Rischio**: i dati identificano *(barrare con X)* • razza o origine etnica • opinioni politiche, religiose o filosofiche • appartenenza a sindacati • dati genetici • dati biometrici • dati che identificano orientamento sessuale • dati che riguardano la salute
Modalità in cui è avvenuta la violazione (es. avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	
Azioni poste in essere (Contenimento)	

ESTREMI SEGNALAZIONE				ESITO		NOTIFICA GARANTE		COMUNICAZIONE AGLI INTERESSATI	
Numero Registrazione	Da ta	Segnalatore	Unità Operativa	Valutazione	Falso Positivo	Effettuata	Data Notifica	Effettuata	Data Comunicazione

Azienda Sanitaria Locale Avezzano, Sulmona, L'Aquila	**REGIONE ABRUZZO – ASL 1 AVEZZANO SULMONA L'AQUILA**
	PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI **ALLEGATO 3 - MODULO DI VALUTAZIONE DELLA SEGNALAZIONE DI DATI PERSONALI** **ai sensi dell'art. 33 del Regolamento UE 679/2016 (GDPR)**

N. Segnalazione (da registro delle segnalazioni) _____

Data _____

	Tipologia di violazione		Rischio			
Tip. Operaz.	**Accidentale**	**Illecito**	**Basso**	**Medio**	**Alto**	**Critico**
Accesso						
Modifica						
Perdita						
Distruzione						
Divulgazione						

Nel modello sopra indicato, è necessario indicare con una "X" la tipologia di operazione eseguita in relazione alla tipologia di violazione; successivamente deve essere indicato, in maniera corrispondente il livello di rischio dell'evento verificatosi considerando i seguenti criteri di valutazione/gravità:

- **1 - Rischio Basso**: 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 – Rischio Medio**: 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 – Rischio Alto**: 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 – Rischio Critico**: 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)

Una volta individuato il livello di rischio dell'evento verificatosi, dovranno essere attuate le seguenti istruzioni:

- Nel caso di livello di **rischio basso o medio**, la violazione non rientra tra quelle soggette a comunicazione al Garante Privacy.
- Nel caso di livello di **rischio alto**, la violazione deve essere comunicata al Garante Privacy ma non all'interessato
- Nel caso di livello di **rischio critico**, la violazione deve essere comunicata sia al Garante Privacy che all'interessato.

ALLEGATO n. 4
PRY-MOD005

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.

2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)

3 Indicare nome e cognome nel caso di persona fisica

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**
   - (•) Il
   - ( ) Dal (la violazione è ancora in corso)
   - ( ) Dal al
   - ( ) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**
   Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**
   - ( ) Il titolare è stato informato dal responsabile del trattamento
   - ( ) Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?**[9]

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro...)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

◯ N.
◯ Circa n.
◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

☐ Dipendenti/Consulenti
☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
☐ Associati,soci, aderenti, simpatizzanti, sostenitori
☐ Soggetti che ricoprono cariche sociali
☐ Beneficiari o assistiti
☐ Pazienti
☐ Minori
☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
☐ Categorie ancora non determinate
☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

◯ N. interessati
◯ Circa n. interessati
◯ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. **Possibili conseguenze della violazione sugli interessati**

a) In caso di perdita di confidenzialità: [17]

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

b) In caso di perdita di integrità: [18]

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

c) In caso di perdita di disponibilità: [19]

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. **Potenziali effetti negativi per gli interessati**

- ☐ Perdita del controllo dei dati personali
- ☐ Limitazione dei diritti
- ☐ Discriminazione
- ☐ Furto o usurpazione d'identità
- ☐ Frodi
- ☐ Perdite finanziarie
- ☐ Decifratura non autorizzata della pseudonimizzazione
- ☐ Pregiudizio alla reputazione
- ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ☐ Conoscenza da parte di terzi non autorizzati

Qualsiasi altro danno economico o sociale significativo (specificare)

3. **Stima della gravità della violazione**

- ○ Trascurabile
- ○ Basso
- ○ Medio
- ○ Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati**

2. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

- ◯ Sì, è stata comunicata il
- ◯ No, sarà comunicata
  - il
  - in una data da definire
- ◯ No, sono tuttora in corso le dovute valutazioni[21]
- ◉ No e non sarà comunicata perché:
  - a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
    Spiegare le motivazioni
  - b) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;

    Descrivere le misure applicate
  - ■ c) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

    Descrivere le misure adottate
  - d) detta comunicazione richiederebbe sforzi sproporzionati.
    Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia

[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679

[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

1058

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

MODULO DI SEGNALAZIONE DELLA VIOLAZIONE DI DATI PERSONALI DA PARTE DELL'INTERESSATO

NOME SOGGETTO CHE RIPORTA L'INCIDENTE	
NUMERO DI CONTATTO DEL SOGGETTO CHE RIPORTA L'INCIDENTE ED INDIRIZZO DI POSTA ELETTRONICA	
DATA DELL'EVENTO ED ORARIO (ANCHE APPROSSIMATIVO)	
DATA E ORA IN CUI SI È VENUTI A CONOSCENZA DELLA VIOLAZIONE	
TIPOLOGIA DI ANOMALIA RISCONTRATA	
DESCRIZIONE DELL'ANOMALIA	
NUMERO DI SOGGETTI COINVOLTI	
NUMERO DEI DATI PERSONALI DI CUI SI PRESUME IL COINVOLGIMENTO	
MODALITÀ IN CUI È AVVENUTA LA VIOLAZIONE	

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

ALLEGATO 5 – MODULO DI SEGNALAZIONE DELLA VIOLAZIONE DI DATI PERSONALI DA PARTE DELL'INTERESSATO

ai sensi dell'art. 33 del Regolamento UE 679/2016 (GDPR)

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI

ART. 13 DEL REGOLAMENTO UE 679/2016

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che la ASL 1 Avezzano Sulmona L'Aquila, in qualità di Titolare del trattamento dei dati, con sede in Via Saragat - località Campo di Pile - 67100 L'Aquila (Italia), E-mail: direzionegenerale@asl1abruzzo.it; PEC: protocollogenerale@pec.asl1abruzzo.it, centralino tel. 0862-3681), tratterà i dati personali conferiti con il presente modulo, con modalità cartacee, informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n.196 e s.m.i.), in particolare per l'obbligo legale del Titolare derivante dagli artt. 33-34 del Regolamento UE 679/2016.

Il conferimento dei dati, è necessario per poter avviare il processo di gestione delle violazioni di dati personali da parte del Titolare, ai sensi degli artt. 33 e 34 del Reg. UE 679/2016: la loro mancata indicazione non consente l'avviamento di tale procedura da parte del Titolare. I dati acquisiti nell'ambito del processo di gestione delle violazioni saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Dopo la fase di valutazione da parte del Titolare, come previsto dagli artt. 33 e 34 del Reg. UE 679/2016, tali dati potranno essere comunicati al Garante per la protezione dei dati personali. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Titolare (ASL 1 Avezzano Sulmona L'Aquila - Responsabile della Protezione dei dati personali, Via Saragat - località Campo di Pile - 67100 L'Aquila (Italia), dpo@asl1abruzzo.it; PEC: dpo@pec.asl1abruzzo.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato

1562

Allegato D

al Regolamento Aziendale per la protezione dei dati personali della ASL 01 Abruzzo

Procedura per l'esercizio dei diritti degli interessati e Modelli Allegati

Procedura per l'esercizio dei diritti in materia di protezione dei dati personali dell'interessato ai sensi degli artt. 15 - 22 del Regolamento UE 679/2016

della Asl di Avezzano – Sulmona – L'Aquila

in base a quanto previsto dal

Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali

Allegato 4 – Regolamento Aziendale per la Protezione dei Dati Personali

Sommario

1 Premessa 3
2 Definizioni 3
3 Obblighi del titolare del trattamento (ai sensi dell'art. 12 del Regolamento (UE) 2016/679) 5
4 Diritto di Accesso ai dati personali (art. 15 del Regolamento (UE) 2016/679) 5
5 Richiesta di intervento sui dati (artt. 16-18 del Regolamento (UE) 2016/679) 5
5.1 Diritto di rettifica (ai sensi dell'art. 16 del Regolamento (UE) 2016/679) 6
5.2 Diritto alla cancellazione e all'oblio (art. 17 del Regolamento (UE) 2016/679) 6
5.3 Diritto di limitazione del trattamento (ai sensi dell'art. 18 del Regolamento (UE) 2016/679) 6
6 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19 del Regolamento (UE) 2016/679) 6
7 Diritto alla Portabilità dei dati (art. 20 del Regolamento (UE) 2016/679) 6
8 Diritto di Opposizione al trattamento (art. 21, paragrafo 1 del Regolamento (UE) 2016/679) 7
9 Diritto di Opposizione al trattamento per fini di marketing diretto (art. 21, paragrafo 2 del Regolamento (UE) 2016/679) 7
10 Limitazioni ai diritti dell'interessato 7
11 Diritti riguardanti le persone decedute 8
12 Coordinamento degli adempimenti 8
13 Percorso di gestione della richiesta 8
14 Allegato 1 10

1 Premessa

L'Asl di Avezzano - Sulmona - L'Aquila (di seguito, ASL) adotta la presente procedura sull'esercizio dei diritti dell'interessato, di seguito denominata "Procedura", ai sensi degli artt. 15 e ss del Regolamento (UE) n. 679/2016 – di seguito Regolamento – e di quanto previsto dal D. Lgs. 196/03 come mod. dal D.Lgs. 101/2018 – di seguito Codice.

Il fine della presente procedura è di consentire all'interessato l'esercizio dei diritti che gli sono riconosciuti dalla normativa comunitaria, attraverso la predisposizione di un "percorso", ad uso dell'utenza.

2 Definizioni

«**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;

«**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;

«**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;

«**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;

3 Obblighi del titolare del trattamento (ai sensi dell'art. 12 del Regolamento (UE) 2016/679)

1. Il titolare del trattamento deve fornire all'interessato le informazioni relative all'azione intrapresa riguardo ad una richiesta di accesso, ai sensi degli articoli da 15 a 22, senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato per un massimo di altri due mesi, se necessario, tenuto conto della complessità della richiesta e del numero di richieste.
2. Qualora si applichi la proroga, l'interessato è informato dei motivi del ritardo entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta in formato elettronico, le informazioni sono fornite, ove possibile, in formato elettronico, salvo indicazione diversa dell'interessato.
3. Se non *ottempera* alla richiesta dell'interessato, il Titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di:
    a) proporre reclamo a un'autorità di controllo
    b) proporre ricorso giurisdizionale

4 Diritto di Accesso ai dati personali (art. 15 del Regolamento (UE) 2016/679)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso ai dati e alle seguenti informazioni:
    a) le finalità del trattamento;
    b) le categorie di dati personali in questione;
    c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se i destinatari appartengono a paesi terzi o organizzazioni internazionali;
    d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
    e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
    f) il diritto di proporre reclamo ad un'autorità di controllo;
    g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
    h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. L'interessato può rivolgere suddetta richiesta in qualsiasi momento utilizzando i canali di comunicazioni resi disponibili utilizzando l'apposito modello allegato alla presente procedura.

5 Richiesta di intervento sui dati (artt. 16-18 del Regolamento (UE) 2016/679)

1. L'interessato ha il diritto di ottenere dal titolare:
    a) la rettifica dei dati personali inesatti (art. 16),
    b) la cancellazione dei dati personali che lo riguardano (art. 17),
    c) la limitazione del trattamento (art. 18).

5.1 Diritto di rettifica (ai sensi dell'art. 16 del Regolamento (UE) 2016/679)

1. Con il diritto di rettifica l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

5.2 Diritto alla cancellazione e all'oblio (art. 17 del Regolamento (UE) 2016/679)

1. Non è consentita la cancellazione di referti e di cartelle cliniche in quanto questi rappresentano un atto medico-legale che deve essere conservato a tutela degli operatori sanitari che hanno gestito tali dati secondo le tempistiche definite dalla specifica normativa applicabile.
2. Tale diritto, quindi, non è esercitabile per motivi di interesse pubblico nel settore della sanità pubblica (art. 17.3.c)

5.3 Diritto di limitazione del trattamento (ai sensi dell'art. 18 del Regolamento (UE) 2016/679)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
   b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21.1 del Regolamento UE, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

6 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19 del Regolamento (UE) 2016/679)

1. Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18 del Regolamento UE, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda

7 Diritto alla Portabilità dei dati (art. 20 del Regolamento (UE) 2016/679)

1. È riconosciuto in capo all'interessato del trattamento dei dati personali il diritto alla portabilità dei dati per cui egli ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di

trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

2. Inoltre, nell'esercitare i propri diritti relativamente alla portabilità dei dati l'interessato ha il diritto di ottenere la trasmissione diretta dei dati da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. Questo diritto non è esercitabile nell'esercizio di compiti di interesse pubblico, connesso all'esercizio di pubblici poteri, quale quello sanitario (art. 20.3) mentre può essere esercitato per il trattamento avente ad oggetto la seguente finalità: "Gestione Selezione Risorse Umane".
4. Tale diritto è esercitabile nei casi in cui i dati personali riguardanti l'interessato siano stati forniti consapevolmente ed in modo attivo dall'interessato anche attraverso l'utilizzo di un dispositivo o servizio (ad esempio glucometri con invio dati al medico tramite app, dati forniti dall'assistito tramite portali di telemedicina, ecc...)

8 Diritto di Opposizione al trattamento (art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del Regolamento, compresa la profilazione sulla base di tali disposizioni.
2. Il titolare del trattamento non tratta più i dati personali salvo che egli dimostri l'esistenza di motivi legittimi preminenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

9 Diritto di Opposizione al trattamento per fini di marketing diretto (art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

1. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
2. Tale fattispecie non si applica al trattamento dei dati personali da parte della ASL.

10 Limitazioni ai diritti dell'interessato

1. In base a quanto disposto dall'art. 2-undecies del Codice i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:
   a) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria (art. 2-undecies c.1 lett. e) del Codice);
   b) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio (art. 2-undecies c.1 lett. f) del Codice).
2. Nei casi di cui al comma 1, lettere *a*), *b*) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei

diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere *a*), *b*). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160 del Codice.

11 Diritti riguardanti le persone decedute

1. In base a quanto disposto dall'art. 2-terdecies del D. Lgs.196/03 modificato dal D.Lgs. 101/2018, i diritti riguardanti le persone decedute sono regolamentati secondo le seguenti disposizioni:
   a) I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
   b) L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge.
   c) La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.
   d) L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.
   e) In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

12 Coordinamento degli adempimenti

1. Per quanto non disciplinato nella presente Procedura aziendale si rinvia al Regolamento (UE) 2016/679.
2. Il coordinamento degli adempimenti, in capo al Titolare del trattamento, è demandato al Responsabile per la Protezione dei Dati che avrà, altresì, il compito di:
   a) redigere e conservare un registro sull'esercizio dei diritti in materia di protezione dei dati personali dell'interessato;
   b) relazionare (almeno su base annua) al titolare in merito alla corretta e attuale attuazione della presente Procedura.

13 Percorso di gestione della richiesta

1. Arrivo della richiesta dell'interessato ad uno dei seguenti recapiti:
   a) Responsabile della protezione dei dati:
      - e-mail: dpo@asl1abruzzo.it
      - PEC: dpo@pec.asl1abruzzo.it
      - Asl di Avezzano – Sulmona – L'Aquila, con sede in via Via Saragat - località Campo di Pile - 67100 L'Aquila
   b) Direzione Generale
      - e-mail: direzionegenerale@asl1abruzzo.it
      - PEC: protocollogenerale@pec.asl1abruzzo.it
      - Direzione Generale Asl di Avezzano – Sulmona – L'Aquila, con sede in via Via Saragat - località Campo di Pile - 67100 L'Aquila
2. La richiesta, se ricevuta dalla Direzione Generale, una volta protocollata, deve essere trasmessa all'Ufficio Privacy ed al DPO (a quest'ultimo solo nel caso in cui non sia stata ricevuta direttamente dal DPO) ai seguenti indirizzi: ufficioprivacy@asl1abruzzo.it e dpo@asl1abruzzo.it per la necessaria istruttoria. Qualora la richiesta venisse ricevuta dal DPO, questa deve essere trasmessa preliminarmente alla Direzione Generale per la necessaria protocollazione e, successivamente, seguire l'iter descritto in precedenza.
3. Richiesta generica: va inoltrata dal DPO ai Soggetti Autorizzati al Trattamento con Delega dal titolare (SATD), affinché accertino se tra i dati trattati nelle banche dati di loro competenza ci siano dati relativi

all'interessato. Una volta compiuta la verifica essi dovranno comunicarne le risultanze al DPO (al seguente indirizzo di posta elettronica, e-mail: dpo@asl1abruzzo.it) entro il termine di 7 (sette) giorni dalla data di inoltro dell'istanza, da parte del DPO.

4. Richiesta specifica: va inoltrata dal DPO al/ai Soggetto/i Autorizzato/i al Trattamento con Delega (SATD) che risultino essere competenti, i quali compiuta la verifica trasmetteranno le risultanze entro il termine di 7 (sette) giorni al Responsabile per la Protezione dei Dati (al seguente indirizzo di posta elettronica, e-mail: dpo@asl1abruzzo.it).
5. Il Responsabile per la Protezione dei Dati sulla scorta delle risultanze pervenute provvede a fornire riscontro all'interessato, oltre che ad adempiere ai compiti di cui all'art. 11, paragrafo 2, della presente Procedura.

14 Allegati

- Allegato 1 – PRY-MOD-001 – Modello di Esercizio dei Diritti dell'Interessato
- Allegato 2 – PRY-MOD-015 – Modello di Reclamo al Garante Privacy
- Allegato 3 – PRY-MOD-016 – Modello Registro di Esercizio dei Diritti

Azienda Sanitaria Locale Avezzano, Sulmona, L'Aquila	**REGIONE ABRUZZO – ASL 1 AVEZZANO SULMONA L'AQUILA**
	PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI ALLEGATO 1 – MODELLO DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI ai sensi degli artt. 15-22 del Regolamento UE 679/2016 (GDPR)

All'attenzione del Direttore Generale della Asl di Avezzano - Sulmona - L'Aquila

Per il tramite del Responsabile per la Protezione dei Dati

e-mail: dpo@asl1abruzzo.it

PEC: dpo@pec.asl1abruzzo.it

Il/La sottoscritto/a.....

nato/a a.....il..... C.F. .....esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. **Accesso ai dati personali** - *(art. 15 del Regolamento (UE) 2016/679)*

Il sottoscritto *(barrare solo le caselle che interessano)*:

- chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
- in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare:
  - le finalità del trattamento;
  - le categorie di dati personali trattate;
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
  - il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati - *(artt. 16-18 del Regolamento (UE) 2016/679)*

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

- ☐ rettifica e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
- ☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

  a)……

  ……;

  b)……

  ……;

  c)……

  ……;

- ☐ nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;
- ☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ contesta l'esattezza dei dati personali;
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

3. Portabilità dei dati - *(art. 20 del Regolamento (UE) 2016/679)*

Ove applicabile, con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

- ☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;
- ☐ trasmettere direttamente al seguente (diverso) titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare:*

  ..... *)* i seguenti dati:

  - ☐ tutti i dati personali forniti al titolare;
  - ☐ un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

4. Opposizione al trattamento - *(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)*

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1. lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____

_____

_____

_____

_____

_____

5. **Opposizione al trattamento per fini di marketing diretto**

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Ove applicabile, il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

- ☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.
- ☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[1]**:**

Estremi identificativi: _____

Via/Piazza _____

Comune _____ Provincia _____ Codice postale _____

oppure

e-mail/PEC: _____ _____

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____

_____

_____

_____

_____

_____

_____/ _____ _____

(Luogo e data)

[1] Allegare copia di un documento di riconoscimento

CHE COS'E' IL RECLAMO E COME SI PRESENTA AL GARANTE

Il reclamo è lo strumento che consente all'interessato di rivolgersi al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del Regolamento Ue 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento) e di richiedere una verifica dell'Autorità

Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro. In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato e un recapito per l'invio di comunicazioni anche tramite posta elettronica, fax o telefono.

Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna, **consegnandolo a mano presso gli uffici del Garante** (all'indirizzo di seguito indicato) o mediante l'inoltro di:

a) **raccomandata A/R indirizzata a: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma**

b) **messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it**

In sede di prima applicazione, il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata, ovvero con firma digitale, ovvero con firma autografa (in tale ultimo caso, al reclamo dovrà essere allegata copia di un documento di riconoscimento dell'interessato/a in corso di validità).

MODELLO DI RECLAMO*

AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
P.ZZA VENEZIA, 11
00187 ROMA

Reclamo ex art. 77 del Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento

Il/La sottoscritto/a ..... nato/a a ..... il ..... residente in ..... CF..... ..... il/la quale ai fini del presente procedimento dichiara di voler ricevere eventuali comunicazioni al seguente recapito (indicare uno o più recapiti, tra indirizzo fisico, telefono, e-mail, fax) espone quanto segue:

(in questa parte del reclamo dovranno essere forniti necessariamente i seguenti elementi:)

a) dichiarazione in relazione alla circostanza che la Repubblica italiana è lo Stato membro in cui risiede abitualmente, lavora oppure il luogo ove si è verificata la presunta violazione;

b) gli estremi identificativi del titolare del trattamento (cioè, 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 e che avrebbe commesso la violazione);

c) gli estremi identificativi del responsabile del trattamento (ove conosciuto);

d) un'indicazione, per quanto possibile dettagliata, dei fatti e delle circostanze su cui l'atto si fonda, ivi comprese eventuali richieste già rivolte sulla questione al Titolare del trattamento;

e) le disposizioni del Regolamento (Ue) 2016/679 e del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento che si presumono violate, specificando se siano stati già eventualmente esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento, e l'indicazione delle misure richieste.

Tutto ciò premesso, il/la sottoscritto/a:

CHIEDE

al Garante per la protezione dei dati personali, esaminato il reclamo che precede e ritenutane la fondatezza, di assumere nei confronti di .....(indicare il titolare del trattamento, recapito, ed ogni elemento utile alla sua individuazione) ogni opportuno provvedimento e, in particolare:

a) rivolgere a questi o al responsabile del trattamento avvertimenti o ammonimenti sul fatto che detti trattamenti possono verosimilmente violare, ovvero abbiano violato, le disposizioni vigenti in materia;

b) ingiungere al titolare del trattamento di soddisfare le richieste di esercizio dei diritti di cui agli artt. da 15 a 22 del Regolamento e/o di conformare i trattamenti alle disposizioni vigenti in materia anche nei confronti del responsabile del trattamento, ove previsto;

c) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento.

Elenco dei documenti allegati:

1;

2;

3;

Data

Firma

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Per le informazioni relative al trattamento dei dati personali effettuato dal Garante per la protezione dei dati personali a seguito della ricezione del presente modello, si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia n. 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, ivi incluse le finalità di trattazione delle istanze pervenute, nonché di archiviazione, di ricerca storica e di analisi per scopi statistici.

Il conferimento dei dati è obbligatorio e la loro mancata indicazione non consente di effettuare l'esame del reclamo. I dati acquisiti nell'ambito della procedura di esame del reclamo saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori dell'Autorità o delle imprese espressamente nominate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza all'Autorità è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia n. 11, 00187, Roma, email: rpd@gpdp.it).

PRY-MOD-016
31/10/2019
REV1.0

PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI
ALLEGATO 3 - REGISTRO DI ESERCIZIO DEI DIRITTI

Progressivo	Nome Interessato	Cognome Interessato	Data richiesta	Diritto esercitato	Riferimento protocollo richiesta	Note	Data chiusura

Allegato E

al Regolamento Aziendale per la protezione dei dati personali della ASL 01 Abruzzo

Procedura per la Gestione delle Informative e Consensi e Modelli Allegati

Procedura
per la Gestione delle
Informative e Consensi

della Asl 01 Abruzzo

in base a quanto previsto dal

Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) – artt. 7, 13 e 14 e dal D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali

Allegato 5 – Regolamento Aziendale per la Protezione dei Dati Personali

Sommario

1 Introduzione 3
2 Scopo 3
3 Campo di Applicazione 3
4 Premesse 3
5 Definizioni 5
6 Normativa di Riferimento 7
6.1 Normativa di riferimento per la gestione delle informative 7
6.2 Normativa di riferimento per la gestione del consenso 12
7 Analisi del Contesto 13
7.1 Liceità del Trattamento 13
7.2 Informazioni da fornire all'interessato nel rispetto del Principio di Trasparenza 15
8 Descrizione del Processo 17
8.1 Approccio generale 17
8.2 Processo di gestione dell'informativa e del consenso 17
9 Aspetti conclusivi 22
10 Allegati 23

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.01 di Avezzano, Sulmona, L'Aquila (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.01 di Avezzano, Sulmona, L'Aquila, per il rispetto di quanto previsto dagli artt. 7, 13 e 14 del Regolamento e dall'art. 2-septies del D.Lgs. 196/03 – Codice in materia di Protezione dei Dati Personali – come modificato dal D. Lgs. 101/2018 riguardanti le modalità di raccolta del consenso e di somministrazione dell'informativa all'interessato con particolare riguardo sia all'informativa unica (iniziale) che alle informative di dettaglio fornite nell'ambito delle specifiche attività delle Unità Operative.

L'obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle Informative e dei Consensi e delle relative indicazioni operative al fine di poter consentire alle Unità Operative di garantire agli interessati il diritto all'informativa secondo quanto previsto dagli artt. 13 e 14 del Regolamento nel rispetto del principio di liceità, correttezza e trasparenza previsto dall'art. 5.1.a). Verranno inoltre indicate le casistiche riguardanti la raccolta del consenso dell'interessato ove richiesto dalla normativa sopra indicata.

3 Campo di Applicazione

Il presente documento regolamenta il processo di gestione delle informative e dei consensi nelle varie casistiche che possano presentarsi nelle strutture amministrative, ospedaliere e territoriali della ASL di Avezzano, Sulmona, L'Aquila.

4 Premesse

Nell'ambito del processo di gestione delle informative e consensi, è necessario specificare il contesto mediante opportune premesse:

- a decorrere dal 25 maggio 2018 è pienamente applicabile il Regolamento (UE) 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali (di seguito "Regolamento");

- ogni trattamento di dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato;
- in base al principio di liceità, correttezza e trasparenza – art. 5.1.a) del Regolamento – i dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi;
- in base al principio di limitazione delle finalità – art. 5.1.b) del Regolamento – i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali;
- Secondo il principio di minimizzazione – art. 5.1.c) del Regolamento – , oggetto di ogni tipo di trattamento dovranno essere i soli dati essenziali per lo svolgimento delle attività istituzionali: tali dati dovranno essere *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*,
- in base al principio di esattezza – art. 5.1.d) del Regolamento – i dati devono essere 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;
- Secondo quanto previsto dal principio di integrità e riservatezza – art. 5.1.e) del Regolamento – i dati personali dovranno essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Salvo quanto specificatamente indicato in regolamentazioni aziendali, è necessario quindi un "approccio alla sicurezza dei dati" da parte del personale che, laddove si presenti una situazione non prevista o non conosciuta, comunichi al proprio responsabile (SATD) la problematica in maniera da poter adottare le eventuali misure del caso specifico;
- Agli interessati deve essere garantito il diritto di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati: l'applicabilità di tali diritti dovrà essere verificata caso per caso secondo quanto previsto dagli artt. 15-22 del Regolamento;
- È compito dei Soggetti Autorizzati al Trattamento dei dati Personali con Delega verificare periodicamente il rispetto dei diritti e dei principi menzionati (la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi), anche con riferimento ai dati che l'interessato fornisca di propria iniziativa. Per la definizione dei soggetti autorizzati al trattamento dei dati personali si rinvia al Vademecum licenziato dalla Asl.

5 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;

«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;

«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;

«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;

«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;

6 Normativa di Riferimento

La normativa di riferimento per la gestione delle informative e dei consensi si compone di vari riferimenti, suddivisi per area di interesse:

- normativa di riferimento per la gestione delle informative
- normativa di riferimento per la gestione del consenso

Alla normativa principale (Regolamento UE 679/2016) indicata in maniera completa, verranno aggiunti i riferimenti relativi alla normativa nazionale in materia di protezione dei dati personali applicabile (D.Lgs. 196/2003 come mod. dal D. Lgs. 101/2018)

6.1 Normativa di riferimento per la gestione delle informative

Il processo contenuto nel presente documento descrive i passi da seguire per informare l'interessato sul trattamento dei dati personali effettuato dalla ASL 01 Abruzzo in conformità con quanto stabilito dagli Artt.13 e 14 del Regolamento UE 679/2016 come di seguito specificato.

6.1.1 Articolo 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

6.1.2 Articolo 14 Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) le categorie di dati personali in questione;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

e) il diritto di proporre reclamo a un'autorità di controllo;

f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.

5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

6.1.3 Articolo 6 Liceità del Trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

6.1.4 Articolo 9 Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3.I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

4.Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

6.1.5 Ulteriori riferimenti normativi

Ad integrazione di quanto indicato nel paragrafo precedente, i riferimenti normativi per la gestione dell'informativa sono costituiti dai seguenti punti:

- Art. 2-undecies del D. Lgs. 196/03 – Limitazioni ai diritti dell'interessato
- Art. 2-terdecies del D. Lgs. 196/03 – Diritti riguardanti le persone decedute
- Provvedimento del Garante Privacy n. 55 del 7 marzo 2019 – *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*

6.2 Normativa di riferimento per la gestione del consenso

6.2.1 Articolo 7 Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

6.2.2 Ulteriori riferimenti normativi

Ad integrazione di quanto indicato nel paragrafo precedente, i riferimenti normativi per la gestione del consenso sono costituiti dai seguenti punti:

- Art. 2-ter del D. Lgs. 196/03 Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
- Art. 2-sexies del D. Lgs. 196/03 – Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante
- Art. 2-septies del D. Lgs. 196/03 – Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute

7 Analisi del Contesto

7.1 Liceità del Trattamento

7.1.1 Casistica generale per il contesto sanitario

La seguente tabella sintetizza le casistiche al momento individuate per l'identificazione delle finalità e delle basi giuridiche per il trattamento di dati personali e di dati appartenenti a particolari categorie come indicato dall'art. 9 del Reg. UE 679/2016: tali basi giuridiche consentono di rispettare il principio di liceità richiesto dal Regolamento all'art. 5.1.a). Sono stati presi a riferimento anche gli artt. 2-ter e 2-sexies del D.Lgs. 196/03 (mod. dal D.Lgs. 101/2018) che regolamentano le casistiche relative al trattamento di dati personali e di dati appartenenti a categorie particolari nella normativa nazionale. In caso di trattamento di dati ex art. 10 del Regolamento (*Trattamento dei dati personali relativi a condanne penali e reati*), come previsto dall'articolo stesso, è necessario fare riferimento alla base giuridica già menzionata relativa all'art. 6.1.

Nella tabella, sono quindi indicate, per ogni tipologia di interessato (in base alle casistiche generali rilevate all'interno dell'Azienda), le basi giuridiche di trattamento sia dei dati personali che dei dati appartenenti a categorie particolari (tra cui sono annoverati anche i dati sanitari):

Cod.	Interessato	Finalità	Base Giuridica (dati personali) art. 6.1 – Reg. UE 679/2016 e art. 2-ter D. Lgs. 196/03	Base Giuridica (dati particolari) art. 9.2 Reg. UE 679/2016 e art. 2-sexies D. Lgs. 196/03
1	Pazienti (Assistiti/Assistibili)	Prestazione sanitaria o contatto (es.: screening, vaccinazioni, ecc…)	6.1.c)	9.2.h) 9.2.i) 9.2.g)
2	Paziente in emergenza Segnalatore (chiamata al 118)	Prestazione sanitaria di emergenza/urgenza	6.1.d)	9.2.c)
3	Paziente elettore	Votazioni presso strutture ospedaliere da ricoverato	6.1.e) 6.3.b) – leggi specifiche in materia di elezioni	
4	Genitore	Esercizio potestà genitoriale (obbligo di legge)	6.1.b) – contratto 6.1.c) – obbligo di legge a cui è soggetto il Titolare del Trattamento	
5	Tutore/Amministratore di Sostegno/Caregiver	Protezione delle persone prive in tutto od in parte di autonomia	6.1.b) – contratto 6.1.c) – obbligo di legge a cui è soggetto il Titolare del Trattamento Titolo XII - Codice civile Legge 9 gennaio 2004, n. 6	
6	Delegati	Ritiro referti, copie di cartella clinica o altro	6.1.b) 6.1.c)	
7	Gestore esercizi pubblici (Ispezioni)	Ispezione igienico-sanitaria	6.1.c) 6.1.c)	
8	Rappresentante legale imprese (Ispezioni)	Ispezione sicurezza sul lavoro	6.1.c) 6.1.c)	

Cod.	Interessato	Finalità	Base Giuridica (dati personali) art. 6.1 – Reg. UE 679/2016 e art. 2-ter D. Lgs. 196/03	Base Giuridica (dati particolari) art. 9.2 Reg. UE 679/2016 e art. 2-sexies D. Lgs. 196/03
9	Rappresentante legale imprese (Ispezioni)	Ispezione allevamenti	6.1.c)	
10	Dipendenti	Instaurazione e gestione del rapporto di lavoro	6.1.c) 6.1.b) 6.1.c)	9.2.b)
11	Personale dipendente o collaboratori di fornitori/personale somministrato	Gestione del rapporto contrattuale con il fornitore (datore di lavoro) Sicurezza sul lavoro (per i dipendenti e collaboratori del fornitore)	6.1.b) 6.1.c)	
12	Interlocutori non contrattualizzati (contatti commerciali o precontrattuali)	Invio di email o contatti per formulare richieste per finalità istituzionali (es.: riparazioni, ecc…)	6.1.e) – finalità istituzionali (interesse pubblico) – primo contatto da parte dell'Amministrazione 6.1.b) – nel caso in cui si attivassero misure precontrattuali e successivamente contrattuali	
13	Amministratori di società partecipanti a gare d'appalto	Appalti pubblici/ Acquisizioni	6.1.c) Codice degli Appalti (Decreto legislativo 18 aprile 2016, n. 50)	

Nota: Per i riferimenti normativi richiamati, si veda il capitolo 5 del presente documento.

7.1.2 Consenso al trattamento dei dati personali

Oltre alle basi giuridiche sopra richiamate, tra le condizioni richieste perché il trattamento dei dati personali sia da considerarsi lecito si annovera l'acquisizione di un consenso (artt. 6.1.a) e 9.2.a) del Regolamento), che, per le particolari categorie di dati personali (in particolare per quelli sanitari), deve essere: informato, esplicito e specifico.

In particolare, le casistiche identificate per la richiesta del consenso all'interessato sono le seguenti:

a) dati genetici,
b) se il trattamento dei dati personali e relativi alla salute è finalizzato alla:
   i. costituzione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico (FSE);
   ii. attività di medicina predittiva;
   iii. teleassistenza/telemedicina,
   iv. trasmissione dei referti on line, ecc.
   v. fornitura di altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;
   vi. finalità didattiche
   vii. dati personali relativi alla salute, il cui trattamento avviene a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, in assenza di una disposizione di legge o di regolamento che lo autorizzi

viii. dati personali relativi alla salute, il cui trattamento avviene a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, in presenza di una disposizione di legge o di regolamento che lo autorizzi ma in assenza di anonimizzazione dei dati

c) Ambito di comunicazione del proprio stato di salute a:
   i. Medico curante (MMG, PLS)
   ii. Familiari
   iii. Altri
d) Ambito di comunicazione della propria presenza all'interno delle strutture dell'Azienda
e) Eventuali richieste di pareri di esperti esterni (c.d. *2nd opinion*)
f) Richiesta di ulteriori dati personali per finalità organizzative (es.: contatto paziente e conferma appuntamenti)
g) Trattamento dei dati personali e sanitari da parte di figure quali, ad esempio, quelle indicate nell'elenco che segue, previamente autorizzate (con obbligo di riservatezza) da parte del Titolare o di suoi delegati (Soggetti Autorizzati al Trattamento con Delega – SATD) secondo quanto previsto dall'art. 2-quaterdecies del D.Lgs. 196/03 mod. dal D.Lgs. 101/2018:
   i. Tirocinanti
   ii. Specializzandi
   iii. Volontari
   iv. Borsisti

Nei casi sopra indicati, il trattamento dei dati personali ed appartenenti a particolari categorie è consentito solo se l'interessato ha prestato il proprio consenso, autonomo e specifico, al relativo trattamento;

7.2 Informazioni da fornire all'interessato nel rispetto del Principio di Trasparenza

Al fine di rispettare il principio di Trasparenza – art. 5.1.a) del Regolamento – secondo quanto previsto dagli artt. 13 e 14 del Regolamento, è previsto il diritto al **rilascio della Informativa** sia in caso di raccolta dei dati direttamente presso l'interessato che in caso di raccolta di dati da terzi.

Tale adempimento (rilascio di tali informazioni) è propedeutico al trattamento dai dati personali, di conseguenza in mancanza dell'informativa applicabile al contesto definito, non è possibile procedere al trattamento di dati personali.

Secondo le indicazioni normative previste dagli articoli 13 e 14 del Regolamento l'informativa per il trattamento dei dati personali raccolti sia presso l'interessato che presso terzi deve contenere le seguenti indicazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale (nel caso in cui si manifestasse la necessità, è un'esigenza da approfondire con il Responsabile della Protezione dei Dati – RPD/DPO)
g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
i) qualora il trattamento sia basato sul consenso, l'esistenza del diritto di poterlo revocare in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) il diritto di proporre reclamo a un'autorità di controllo;
k) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
m) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano
n) da fonti accessibili al pubblico;
o) le categorie di dati personali in questione;

Nel caso in cui il titolare del trattamento (o un suo soggetto delegato) intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato informazioni (mediante una nuova informativa) che indichino tale diversa finalità e le informazioni elencate in precedenza.

Inoltre, in base a quanto previsto dagli artt. 78-79 del Codice in materia di Protezione dei Dati Personali le strutture sanitarie e socio-sanitarie possono fornire le informazioni relative al complessivo trattamento dei dati personali necessario per attività di diagnosi, assistenza e terapia sanitaria a tutela della salute o dell'incolumità fisica dell'interessato in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.

8 Descrizione del Processo

8.1 Approccio generale

Al fine di rispettare i principi di trattamento e tutelare i diritti degli interessati, specificati rispettivamente nell'art. 5 e nel Capo III del Regolamento, è stata stabilita una specifica strategia di gestione delle informative e relative richieste di consenso da sottoporre nei punti di "accesso" ai servizi da parte degli interessati: un elenco generale di categorie di interessati è stato indicato nel capitolo precedente.

In linea generale sono identificati due distinti livelli di gestione del principio di trasparenza (art. 5.1.a del Regolamento) indicati nei punti seguenti:

a) Informativa generale
b) Informativa per lo specifico trattamento con eventuale consenso

Di conseguenza le opzioni possono essere riepilogate nella seguente tabella:

Opzione	Informativa	Consenso
A	Informativa Generale	NO
B	Informativa Specifica	NO
C	Informativa Specifica	SI

La fornitura delle informazioni riguardanti la protezione dei dati personali all'interessato (artt. 13 e 14 del Regolamento) potrà essere effettuata mediante una delle possibili strategie di seguito indicate:

1) Opzione A (Informativa Generale)
2) Opzione A (Informativa Generale) + Opzione B (Informativa Specifica)
3) Opzione A (Informativa Generale) + Opzione C (Informativa Specifica + Consenso).

Ad esempio, nell'ambito della fase di accesso alle cure (es.: prenotazione), preliminarmente verrà fornita l'informativa generale all'interessato e successivamente, in base ad eventuali specifiche esigenze (es.: in caso di necessità di chiedere all'interessato dati di ricontatto quali numero di telefono o indirizzo di posta elettronica), verrà fornita l'informativa specifica con relativo consenso laddove ritenuto necessario.

Nel caso in cui l'informativa generale sia già stata fornita all'interessato (es.: prenotazione ed esecuzione di prestazioni di 2° livello, prenotabili direttamente nel CUP di 2° livello) verranno adottate direttamente le strategie 2 o 3.

8.2 Processo di gestione dell'informativa e del consenso

Il processo di gestione dell'informativa e del consenso si compone delle seguenti fasi:

1. Identificazione/rilevazione o modifica di un trattamento di dati personali
2. Valutazione del trattamento e della necessità di sviluppare una informativa specifica ed eventuale formula di consenso
3. Predisposizione dell'informativa e della formula di consenso
4. Definizione della fase di somministrazione dell'informativa
5. Gestione del Tempo di conservazione dell'informativa e del consenso

8.2.1 Identificazione/rilevazione o modifica di un trattamento di dati personali

L'input al processo viene fornito dalla fase di identificazione/rilevazione di un trattamento di dati personali o da una modifica allo stesso. È possibile distinguere i seguenti casi:

- Identificazione di un trattamento: il SATD, nell'ambito dell'Unità Operativa da lui diretta, identifica i nuovi trattamenti di dati personali (in caso di nuove modalità di trattamento per processi esistenti o in caso di definizione di nuovi processi organizzativi)
- Rilevazione di un trattamento: la rilevazione di un trattamento può avvenire nei seguenti casi:
  - in fase di censimento (es.: tramite la somministrazione di appositi questionari),
  - audit interno all'UO (condotto da parte del SATD o da parte di personale da lui incaricato) o
  - audit da parte del Responsabile della Protezione dei Dati o dell'Ufficio Privacy;
- Modifica di un trattamento: la modifica di un trattamento di dati personali può avvenire, in generale, nei seguenti casi:
  - Variazioni nella finalità di trattamento (es.: trattamento per ulteriori finalità)
  - Variazioni organizzative (es.: esternalizzazione di un servizio);
  - Variazioni nelle modalità di trattamento e gestione delle informazioni (es.: da modalità cartacea a modalità informatizzata o cambio di sistema informatico);
  - Variazione nella tipologia di dati trattati
  - Variazione nei soggetti destinatari di comunicazione delle informazioni trattate
  - Variazione normativa applicabile allo specifico trattamento
  - Trasferimento di dati in paesi extra-UE

8.2.2 Valutazione del Trattamento

Una volta identificato il trattamento di dati personali, è necessario analizzarne le specificità e valutare la possibilità di utilizzo di una informativa generale (o comunque esistente) o la necessità di sviluppo di una specifica informativa e relativa formula di consenso: tale valutazione dovrà essere effettuata dai SATD al fine di poter rispettare il principio di Trasparenza di cui all'art. 5.1.a) del Regolamento UE 679/2016.

Secondo quanto indicato nel paragrafo 8.1 il SATD, in base al trattamento di dati personali rilevato/modificato nell'ambito della propria UO, dovrà proporre il possibile utilizzo di un'informativa esistente o un nuovo documento dedicato da lui predisposto sulla base di un modello (*template*) reso disponibile dall'Ufficio Privacy (in allegato alla presente procedura), seguendo una delle strategie (1, 2 e/o 3) indicate nel paragrafo 8.1 (in allegato anche il modello per il consenso). Tali proposte dovranno essere successivamente comunicate all'Ufficio Privacy e validate dal Responsabile della Protezione dei Dati.

Generalmente, secondo quanto previsto dal Garante Privacy nel Provvedimento 55/2019, i casi per i quali non viene previsto il consenso in ambito sanitario sono generalmente riconducibili alle seguenti basi giuridiche:

a) **motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice;

b) **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);

c) **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** (anche indicata come "finalità di cura") **sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità**, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

Al fine di poter effettuare una corretta valutazione in merito alla necessità della predisposizione del modulo di consenso per lo specifico trattamento, il Garante indica che **i trattamenti "necessari"** (di cui all'art. 9, par. 2, lett. h) del Regolamento UE) **al perseguimento delle specifiche "finalità di cura"** previste dalla norma sono quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (ad esempio l'esecuzione di una visita specialistica o di un ricovero).

Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari (ad esempio, il trattamento di dati personali per il ricontatto paziente che non sono strettamente indispensabili per l'erogazione della prestazione sanitaria) , richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del Regolamento).

8.2.3 Predisposizione dell'informativa e della formula di consenso

Il Processo di predisposizione dell'informativa è articolato nelle seguenti fasi:

Fase Preliminare:

Cod.	Descrizione Fase	Responsabilità
1	Predisposizione dei modelli (template) generale e specifico di informativa e relativo consenso per i trattamenti	Ufficio Privacy
2	Validazione dei moduli predisposti	Responsabile della Protezione dei Dati
3	Messa a disposizione dei moduli così predisposti per poter essere utilizzati dai vari SATD	Ufficio Privacy

Fase Operativa:

Cod.	Descrizione Fase	Responsabilità
1	Recepimento da parte dei SATD delle singole UO dei modelli (template) resi disponibili dall'Ufficio Privacy.	SATD di riferimento delle singole UO
2	Utilizzo dei modelli (template) e creazione di specifica informativa ed eventuale consenso	SATD di riferimento delle singole UO
3	In caso di modifiche sostanziali ai modelli (template) o per richiesta di validazione delle informative e consensi così redatte dai SATD è possibile richiedere un parere del Responsabile della Protezione dei Dati	Responsabile della Protezione dei Dati

8.2.4 Definizione della fase di somministrazione dell'informativa agli interessati

Le casistiche per la somministrazione delle informative agli interessati individuate in precedenza (par. 7.1.1) possono essere così classificate:

Prog.	Interessati	Casistica	Classe

1	Pazienti (Assistiti/Assistibili)	Prestazione sanitaria o contatto (es.: screening, vaccinazioni, ecc…)	Utente
2	Paziente in emergenza Segnalatore (chiamata al 118)	Prestazione sanitaria di emergenza/urgenza	Utente
3	Paziente elettore	Votazioni presso strutture ospedaliere da ricoverato	Utente
4	Genitore	Esercizio potestà genitoriale (obbligo di legge)	Utente
5	Tutore/Amministratore di Sostegno/Caregiver	Protezione delle persone prive in tutto od in parte di autonomia	Utente
6	Delegati	Ritiro referti, copie di cartella clinica o altro	Utente
7	Gestore esercizi pubblici (Ispezioni)	Ispezione igienico-sanitaria	Utente
8	Rappresentante legale imprese (Ispezioni)	Ispezione sicurezza sul lavoro	Utente
9	Rappresentante legale imprese (Ispezioni)	Ispezione allevamenti	Utente
10	Dipendenti	Instaurazione e gestione del rapporto di lavoro	Dipendente
11	Personale dipendente o collaboratori di fornitori/personale somministrato	Gestione del rapporto contrattuale con il fornitore (datore di lavoro) Sicurezza sul lavoro (per i dipendenti e collaboratori del fornitore)	Fornitore
12	Interlocutori non contrattualizzati (contatti commerciali o precontrattuali)	Invio di email o contatti per formulare richieste per finalità istituzionali (es.: riparazioni, ecc…)	Fornitore
13	Amministratori di società partecipanti a gare d'appalto	Appalti pubblici/ Acquisizioni	Fornitore

Le modalità di somministrazione delle informative, in relazione alla classe individuata sono le seguenti:

- Classe Utente (paziente, delegato o soggetto di sostegno): l'informativa generale viene sempre rilasciata in fase di prenotazione, mentre l'informativa specialistica con relativo consenso (ove previsto) viene rilasciata in fase di regolarizzazione dell'impegnativa o accettazione ove necessario.
- Classe Dipendente: l'informativa viene rilasciata in fase di stipula del contratto di assunzione
- Classe Fornitore: l'informativa viene rilasciata al momento della raccolta dei dati personali.

8.2.4.1 Canali di comunicazione/Punti di contatto degli interessati (somministrazione dell'informativa)

I canali di comunicazione previsti con l'utenza possono essere elencati nei seguenti punti:

- Sito Web istituzionale
- Canale telefonico (call center)
- Sportello – Accesso ai locali
- Posta elettronica

8.2.4.1.1 Sito Web Istituzionale

Nel sito internet aziendale, all'interno della sezione Privacy, devono essere pubblicate, da parte dell'Ufficio Privacy, le informative generali e specifiche relative ai trattamenti di dati personali effettuati dalla ASL 01 Abruzzo.

Al fine di poter garantire la tutela dei dati personali degli interessati che inviino proprie richieste e-mail agli indirizzi di posta elettronica pubblicati sul sito web istituzionale, il messaggio di posta elettronica in risposta dovrà contenere l'indicazione prevista al successivo paragrafo 8.2.4.1.4 – "Posta Elettronica".

8.2.4.1.2 Canale telefonico

In generale, nell'ambito delle comunicazioni telefoniche, gli operatori della ASL dovranno dare comunicazione agli interessati che i dati personali eventualmente raccolti nel corso del colloquio telefonico verranno trattati in maniera conforme alla vigente normativa sulla Protezione dei Dati Personali e che potranno visionare l'informativa disponibile nella specifica sezione del sito istituzionale all'URL:

http://www.asl1abruzzo.it/pagina276_privacy.html

Nello specifico caso del servizio CUP (Centro Unico di Prenotazione) telefonico, nella fase iniziale della risposta alla chiamata da parte dell'utente, deve essere comunicato all'interessato, mediante una opportuna registrazione vocale, la conformità, alle normative vigenti in materia di Protezione dei Dati Personali, del trattamento effettuato dagli operatori telefonici a fini di prenotazione della prestazione sanitaria.

8.2.4.1.3 Sportello – Accesso ai locali

Come approccio generale, nell'ambito della comunicazione con gli interessati nelle operazioni di sportello, deve essere contestualmente consegnata l'informativa richiesta dal trattamento di dati personali previsto dall'operazione stessa.

Come ulteriore modalità di rispetto del principio di trasparenza, nell'ambito specifico dell'erogazione dei servizi sanitari, copia dell'informativa deve essere affissa sia nei locali presso cui avviene il primo contatto con gli interessati che nelle sale di attesa.

Nel caso specifico degli sportelli del servizio CUP (Centro Unico di Prenotazione), l'informativa dovrà essere somministrata agli interessati ad ogni operazione di prenotazione.

8.2.4.1.4 Posta Elettronica

Al fine di poter garantire la tutela dei dati personali raccolti tramite il canale della posta elettronica, per finalità di interlocuzione con terze parti, è necessario specificare, in fondo ad ogni messaggio inviato, un link che rinvii all'informativa specificatamente predisposta e pubblicata sul sito internet istituzionale.

In caso di comunicazione tramite posta elettronica con degli specifici interessati nell'ambito di particolari servizi, è necessario indicare, in fondo ai messaggi, un link che rinvii ad una informativa specificatamente predisposta per il servizio e pubblicata sul sito internet istituzionale.

8.2.4.2 Verifica del rilascio dell'informativa

Al fine di poter verificare il rilascio dell'informativa generale all'interessato (con particolare riguardo al caso del paziente), l'art. 79 del D. Lgs. 196/03 come mod. dal D. Lgs. 101/2018, indica quanto segue:

1. Le strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie possono avvalersi delle modalità particolari di cui all'articolo 78 del D. Lgs. 196/03 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.

Omissis...

...la struttura o le sue articolazioni annotano l'avvenuta informazione con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

Al fine di poter garantire l'avvenuta annotazione, la modalità di somministrazione dell'informativa generale prevede (come indicato in precedenza) il rilascio di una copia dell'informativa contestualmente alla prenotazione di ogni singola prestazione, unitamente alla ricevuta emessa dall'operatore di sportello: tale emissione unica (della ricevuta e dell'informativa) prevista dalla procedura informatica in uso, è completamente automatizzata e non è modificabile dall'operatore, con conseguenti garanzie di consegna all'interessato. Di conseguenza, essendo l'intera struttura aziendale a conoscenza che, per poter accedere alla prestazione sanitaria richiesta, l'informativa sia già stata somministrata all'interessato, tale modalità di somministrazione viene considerata quale "annotazione" prevista dall'art. 79.2 del D.Lgs. 196/03 sopra indicato.

Il caso di informativa specialistica senza necessità di specifico consenso è assimilabile al caso appena esposto.

Negli altri casi riguardanti i pazienti, in caso di somministrazione di informativa specialistica con consenso, il rilascio dell'informativa viene attestato dalla sottoscrizione del consenso ed i documenti sono conservati (archiviati) all'interno della cartella prevista dal percorso assistenziale prescelto.

Negli altri casi, classificati come Dipendente e Fornitore, il rilascio dell'informativa viene attestato da una sottoscrizione dell'interessato per "presa visione".

8.2.5 Tempo di conservazione dell'informativa e del relativo consenso

In base alle casistiche individuate i tempi di conservazione dei documenti indicati possono essere sintetizzati secondo il seguente elenco:

- Informativa di 1° livello: tale documento viene consegnato direttamente al paziente e non è soggetto a conservazione da parte dell'Azienda
- Informativa di 2° livello (o specialistica) senza consenso: come il precedente caso;
- Informativa di 2° livello (o specialistica) con necessità di consenso: il tempo di conservazione di questi documenti (informativa e consenso) è da individuarsi all'interno del Massimario di Conservazione dell'Azienda allegato alla Deliberazione della ASL n. 1732 del 12/10/2015 in cui è presente il prontuario di selezione degli archivi con indicazione delle tipologie di documenti trattati dall'Ente (ad esempio nel caso delle cartelle cliniche, tale tempo risulta essere illimitato).

9 Aspetti conclusivi

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

10 Allegati

- Allegato 1 – PRY-MOD-007 – Template Informativa Specialistica (II livello)
- Allegato 2 – PRY-MOD-008 – Template Modulo Consenso

1605

Azienda Sanitaria Locale
Avezzano, Sulmona, L'Aquila

REGIONE ABRUZZO – ASL 1 AVEZZANO SULMONA L'AQUILA

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
inerenti attività _____
ai sensi degli artt. 13 e 14 del Regolamento UE 679/2016 (GDPR)

"Attività _____"

Gentile utente,
al fine di fornirLe tutte le informazioni di cui agli articoli 13 e 14, le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del Regolamento UE 679/2016 (Regolamento Generale sulla Protezione dei Dati di seguito Regolamento) di cui potrà prendere visione al sito del Garante per la Protezione dei Dati Personali http://www.garanteprivacy.it/regolamentoue ,
ai sensi dell'art. 13 del Regolamento. La informiamo che i dati personali e quelli appartenenti a categorie particolari (rispettivamente artt. 4.1 e art. 9 del Regolamento) che La riguardano e da Lei forniti, o acquisiti attraverso _____, saranno trattati nel rispetto del Regolamento e degli obblighi di riservatezza a cui è tenuta la ASL di Avezzano – Sulmona – L'Aquila.

FINALITÀ DEL TRATTAMENTO
Alla luce degli Artt. 2-ter, 2-sexies, 2-septies e 75 del Codice in materia di protezione dei dati personali (di seguito Codice) e dell'art.9, paragrafo 2, lettere g), h) ed i) del Regolamento, i trattamenti dei Suoi dati personali (comprensivi di quelli appartenenti a categorie particolari di dati, ad esempio, quelli riguardanti lo stato di salute) non rendono necessario il Suo consenso, quando vengono effettuati dalla ASL di Avezzano – Sulmona – L'Aquila nell'esercizio delle proprie funzioni istituzionali nell'ambito delle attività svolte per "_____", relativamente alle seguenti finalità:

- Finalità 1: _____(es.: Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione).
- Finalità 2: _____(es.: Adempimenti amministrativi, gestionali e contabili, correlati ai compiti istituzionali della ASL 1 Avezzano Sulmona L'Aquila e/o connessi ad obblighi di legge);
- Finalità 3: _____(es.: Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, svolte anche tramite attività di ricontatto).

BASE GIURIDICA DEL TRATTAMENTO.
Il trattamento necessario per i seguenti motivi richiede la sola somministrazione delle Informazioni all'interessato:

Dati personali (art. 6 del Regolamento, riferimento art. 6 paragrafo 1) – es.: dati anagrafici

a. **BASE GIURIDICA 1** – l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (sopra indicate, inserire i riferimenti _____);
b. **BASE GIURIDICA 2** – il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c. **BASE GIURIDICA 3** – il trattamento è necessario per adempiere un obbligo legale al quale è soggetta la Asl di Avezzano – Sulmona – L'Aquila, in qualità di Titolare del trattamento (art. 6.1.c del Regolamento));
d. **BASE GIURIDICA 4** – il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e. **BASE GIURIDICA 5** – il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri al quale è soggetta la Asl di Avezzano – Sulmona – L'Aquila, in qualità di Titolare del trattamento (art. 6.1.e del Regolamento));

Dati particolari (art. 9 del Regolamento, riferimento art. 9 paragrafo 2) – es.: dati sanitari

a. **BASE GIURIDICA 6** – (art. 9, par. 2, lett. a del Regolamento) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui all'art. 9 paragrafo 1 del Regolamento UE 679/2016

163

b. **BASE GIURIDICA 7** – (art. 9, par. 2, lett. b del Regolamento) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c. **BASE GIURIDICA 8** – il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d. (art. 9, par. 2, lett. e del Regolamento) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

e. **BASE GIURIDICA 9 – motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice);

f **BASE GIURIDICA 10 – motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) e considerando n. 54 del Regolamento) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare));

g. **BASE GIURIDICA 11 – finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza);

h. **BASE GIURIDICA 12** – (art. 9, par. 2, lett. j del Regolamento) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

NEL CASO IN CUI SIANO SELEZIONATE LE BASI GIURIDICHE 1 o 6 (CONSENSO DELL'INTERESSATO)

Si invita a leggere il modello allegato ove sono riportate le finalità di trattamento per le quali è richiesto il Consenso. (artt. 6.1.a e 9.2.a del Regolamento). Da tenere presente che Lei ha il diritto di revocare in qualsiasi momento il consenso prestato senza che ciò pregiudichi la liceità del trattamento basata sul consenso prestato prima della revoca.

PERIODO DI CONSERVAZIONE O CRITERI PER DETERMINARE TALE PERIODO.

I Suoi dati saranno conservati solo per il tempo necessario al raggiungimento delle finalità per cui sono raccolti, rispettando il principio di limitazione della conservazione di cui all'Art. 5, paragrafo 1, lettera c) del Regolamento, nonché gli obblighi di legge cui è tenuto il Titolare.

La tempistica di conservazione della documentazione contenente dati personali è regolamentata dall'allegato D – Massimario di Selezione del Manuale di Gestione del Sistema Documentale approvato con Deliberazione della ASL n. 1732 del 12/10/2015 e pubblicato sul sito aziendale http://www.asl1abruzzo.it nell'area "Amministrazione Trasparente".

CATEGORIE DI DATI PERSONALI

- Dati personali: dati anagrafici. _____
- Particolari categorie di dati personali
  - Categoria 1: _____ (es.: Dati relativi alla salute dell'interessato)
  - Categoria 2: _____ (es.: Dati relativi alle convinzioni religiose o filosofiche)
  - Categoria 3: _____ (es.: Dati genetici)

AMBITO DI COMUNICAZIONE DEI DATI (DESTINATARI)

I Suoi dati saranno trattati nei modi previsti dalla legge e nel rispetto del segreto professionale e d'ufficio.

I suoi dati personali all'interno dell'ASL sono trattati esclusivamente da personale specificatamente nominato quale "soggetto autorizzato al trattamento dei dati personali, con delega o meno a compiere adempimenti specificatamente indicati dal Titolare del trattamento".

I Suoi dati potranno essere comunicati, solo se necessario, a soggetti espressamente previsti dalla normativa vigente; ulteriori comunicazioni potranno essere effettuate a soggetti che eseguano delle attività di trattamento per conto del Titolare, o con finalità e mezzi concordati e con cui siano stati stipulati specifici accordi (es.: Responsabili del Trattamento, Contitolari o Titolati autonomi).

- Destinatario 1: _____ (es.: Regione/Agenzia regionale di sanità, altra Azienda Sanitaria, Direzione Provinciale Lavoro, Autorità Sanitaria (Sindaco));
- Destinatario 2: _____ (es.: ai professionisti interni o esterni coinvolti nella gestione clinico assistenziale);
- Destinatario 3: _____ (es.: alla compagnia assicurativa dell'Azienda per la tutela della stessa e dei suoi operatori, per l'ipotesi di responsabilità);
- Destinatario 4: _____ (es.: ad altri soggetti pubblici o privati (che svolgono attività istituzionale per conto della Azienda));
- Destinatario 5: _____ (es.: all'Autorità Giudiziaria e/o di Pubblica Sicurezza, nei casi espressamente previsti dalla legge);

MODALITA' DI TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati avverrà mediante l'utilizzo di strumenti automatizzati e non: i suoi dati personali saranno, altresì, trattati dal personale sanitario e amministrativo dell'Azienda, nominato "soggetto autorizzato al trattamento dei dati personali, con delega o senza delega a compiere adempimenti specificatamente indicati dal Titolare del trattamento", nel rispetto del principio di minimizzazione dei dati, nei limiti dello scopo per cui sono stati raccolti.

I Suoi dati personali potranno essere trattati, se del caso, anche mediante sistemi di ripresa qualora ritenuto utile per le cure.

I Suoi dati personali e relativi a particolari categorie di dati (art 9 del Regolamento), saranno inoltre trattati al fine di adempiere agli obblighi previsti da leggi, regolamenti e dalla normativa comunitaria nonché alle disposizioni impartite dalle autorità a ciò legittimate dalla legge.

I dati relativi alla Sua persona sono registrati e conservati in banche dati cartacee, informatiche e miste (cartacee e informatiche).

Tutti i Suoi dati personali verranno trattati nel rispetto dei Principi applicabili al trattamento di dati personali secondo quanto previsto dall'art. 5 del Regolamento.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento è la ASL 1 Avezzano Sulmona L'Aquila, con sede in Via Saragat - località Campo di Pile - 67100 L'Aquila (Italia), E-mail: direzionegenerale@asl1abruzzo.it; PEC: protocollogenerale@pec.asl1abruzzo.it, tel. 0862.368931/368924

RESPONSABILE PER LA PROTEZIONE DATI – RDP (O DPO)

Il Responsabile della Protezione dei Dati (RPD) è raggiungibile al seguente indirizzo: ASL 1 Avezzano Sulmona L'Aquila, con sede in Via Saragat - località Campo di Pile - 67100 L'Aquila (Italia), E-mail: dpo@asl1abruzzo.it; PEC: dpo@pec.asl1abruzzo.it

DIRITTI DELL'INTERESSATO

Lei può esercitare i seguenti diritti sui Suoi dati personali, nella misura in cui è consentito dal Regolamento:

- Accesso (art. 15 del Regolamento)
- Rettifica (art. 16 del Regolamento)
- Cancellazione (oblio) (art. 17 del Regolamento): non esercitabile per motivi di interesse pubblico nel settore della sanità pubblica (art. 17.3.c del Regolamento)
- Limitazione del trattamento (art. 18 del Regolamento)
- Portabilità (art. 20 del Regolamento): non esercitabile nell'esercizio di compiti di interesse pubblico quale quello sanitario (art. 20.3)
- Opposizione al trattamento, (art. 21 del Regolamento)

Per l'esercizio dei diritti di cui sopra, e per eventuali ulteriori precisazioni, lei può rivolgersi al Responsabile della Protezione dei Dati contattabile al seguente riferimento: dpo@asl1abruzzo.it e all'Ufficio Privacy aziendale: ufficio.privacy@asl1abruzzo.it

Il modello per richiedere l'esercizio dei diritti sui Suoi dati personali è scaricabile al seguente link: http://www.asl1abruzzo.it/pagina431_esercizio-dei-diritti.html

DIRITTO DI REVOCA DEL CONSENSO

Lei ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Lei può esercitare tale diritto mediante compilazione del modulo di consenso allegato alla presente informativa.

DIRITTO DI PROPORRE RECLAMO ALL'AUTORITÀ DI CONTROLLO

Lei, qualora ritenga che il trattamento che La riguarda violi il Regolamento, ha il diritto di proporre reclamo al Garante dei dati personali con sede in Piazza di Monte Citorio, n. 121, CAP 00186 Roma, come previsto dall'art. 77 del Regolamento, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

FONTE DA CUI HANNO ORIGINE I DATI PERSONALI
(da inserire manualmente a cura del soggetto autorizzato solo se i dati non sono raccolti presso l'interessato)

.....

.....

AGGIORNAMENTO

La versione sempre aggiornata della presente informativa è disponibile sul sito web istituzionale all'indirizzo http://www.asl1abruzzo.it/pagina276_privacy-policy.html nella sezione "Informative" raggiungibile tramite il QR Code indicato a lato.

Azienda Sanitaria Locale
Avezzano, Sulmona, L'Aquila

REGIONE ABRUZZO – ASL 1 AVEZZANO SULMONA L'AQUILA

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI
(Basi giuridiche di riferimento: artt. 6.1.a) e 9.2.a), 7 Regolamento UE 679/2016)

Premesso che il presente Modello integra il Modello di Informativa. di cui si dichiara di avere preso visione.

Il sottoscritto _____ _____ nato a _____ il / ____/____:residente a_____ in via _____ C.F._____

In qualità di diretto interessato o esercente la potestà genitoriale / la tutela / la curatela/ l'amministrazione di sostegno sul soggetto beneficiario della prestazione sanitaria richiesta.

_____ _____
(nome e cognome)

acquisite le informazioni di cui all'informativa fornita ai sensi degli artt. 13 e 14 del Reg. UE 679/2016, consapevole che il trattamento riguarderà i propri dati personali e appartenenti a particolari categorie (vedi informativa)

AUTORIZZA

- **che sia data comunicazione in ordine al proprio stato di salute alle sotto indicate persone:**
  - a nessuno
  - al proprio medico curante _____ _____
  - a _____

    SI (.....) NO (....) REVOCA (.....) (se precedentemente prestato)
- **che la sua presenza nella Struttura Sanitaria sia comunicata alle sotto indicate persone:**
  - a nessuno
  - a _____(indicazioni specifiche)

    SI (.....) NO (....) REVOCA (.....) (se precedentemente prestato)
- **che tali dati potranno essere trattati anche attraverso riprese visive qualora ritenuto utile per le cure o per finalità di studio:**

  SI (.....) NO (....) REVOCA (.....) (se precedentemente prestato)
- **che tali dati potranno essere trattati per finalità di ricerca scientifica in campo medico, biomedico ed epidemiologico:**

  SI (.....) NO (....) REVOCA (.....) (se precedentemente prestato)
- **a ricevere un messaggio per finalità organizzative contatto paziente e conferma appuntamenti;**
  - **a mezzo contatto telefonico e/o sms sul numero** _____:

    SI (.....) NO (....) REVOCA (.....) (se precedentemente prestato)
  - **a mezzo posta elettronica all'indirizzo** _____

    SI (.....) NO (....) REVOCA (.....) (se precedentemente prestato)

Firma (leggibile) dell'Interessato: _____

Documento di riconoscimento tipo _____

n. _____ rilasciato da _____ Data

_____/_____/_____

ovvero
Data ____ __ Firma _____ Doc. n _____ _____
(se esercente la potestà o il tutore)

Il genitore presente dichiara che l'altro genitore esercitante la patria potestà è informato e acconsente al trattamento dei dati personali del minore.

---

ovvero
Considerato che l'interessato/a Sig./Sig.ra
.....
non può prestare il proprio consenso per impossibilità psico fisica, per incapacità, anche temporanea, di agire o per incapacità di intendere o di volere, il sottoscritto (*in stampatello):*
.....

.....

n° documento identità .....rilasciato da

.....

il..... C.F.....

- o Familiare (indicare il rapporto di parentela) .....
- o Convivente
- o Responsabile della struttura presso cui dimora l'interessato
- o Amministratore di Sostegno

acconsente al trattamento dei dati sensibili sanitari dell'interessato nell'ambito e per le finalità indicate nell'informativa e si impegna, non appena il paziente sia in grado di prestare autonomamente il proprio consenso, a comunicargli di averlo prestato in sua vece e luogo e della possibilità di revocarlo.

Con la firma del presente Modello dichiaro esplicitamente di avere letto e compreso la INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI redatta ai sensi dell'art. 13/14 del Regolamento UE 679/2016 e di esprimere il mio libero e inequivocabile consenso al trattamento per le seguenti specifiche finalità, legate al trattamento dei dati personali.

Data .....Firma del dichiarante .....

1611

Allegato F

al Regolamento Aziendale per la protezione dei dati personali della ASL 01 Abruzzo

Procedura di Gestione di Accordi, Nomine e Designazioni e Modelli Allegati

Procedura

per la Gestione di Accordi, Nomine e Designazioni

e relativa attribuzione di responsabilità

della Asl 01 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)

Allegato 6 – Regolamento Aziendale per la Protezione dei Dati Personali

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 i Trattamenti sotto l'autorità del Titolare o del Responsabile del Trattamento 7
5.1.1 Articolo 29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento 7
5.1.2 Art. 2-quaterdecies – Attribuzione di funzioni e compiti a soggetti designati 7
5.2 Normativa di riferimento per la designazione di Responsabili del Trattamento 7
5.2.1 Articolo 28 Responsabile del trattamento 8
5.3 Normativa di riferimento per gli Accordi di Contitolarità 9
5.3.1 Articolo 26 Contitolari del trattamento 9
6 Premesse 11
6.1 Generalità 11
6.2 Struttura organizzativa dell'Azienda Sanitaria 11
6.3 Approccio metodologico agli accordi. nomine e designazioni 12
7 Descrizione del Processo 13
7.1 Soggetti Autorizzati al Trattamento con Delega 13
7.1.1 Identificazione 13
7.1.2 Designazione 13
7.2 Soggetti Autorizzati al Trattamento 14
7.2.1 Identificazione 14
7.2.2 Designazione 14
7.2.3 Gestione operativa 15
7.2.4 Archiviazione degli atti 15
7.3 Responsabili del Trattamento 15
7.3.1 Identificazione e Classificazione 15
7.3.2 Designazione 16
7.3.3 Impegno da parte del Responsabile 17

7.3.4 Monitoraggio del Responsabile del Trattamento 17
7.3.5 Conclusione del rapporto e revoca 17
7.3.6 Archiviazione dei documenti degli atti di designazione 18
7.4 Sub-Responsabili del Trattamento 18
7.5 Contitolari del Trattamento e Titolari autonomi 18
7.5.1 Identificazione e Classificazione 18
7.5.2 Stipula dell'Accordo 19
7.5.3 Conclusione del rapporto e revoca 19
7.5.4 Archiviazione dei documenti degli atti istituenti il rapporto 19
7.6 Amministratori di Sistema 19
7.6.1 Identificazione 19
7.6.2 Designazione 20
7.7 Conclusioni 21
8 Allegati 22

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.01 di Avezzano – Sulmona – L'Aquila (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.01 di Avezzano – Sulmona – L'Aquila, 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 regolamenta il processo di gestione delle nomine e designazioni nelle varie casistiche che possano presentarsi nelle strutture amministrative, ospedaliere e territoriali della ASL di Avezzano – Sulmona -L'Aquila.

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;

«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;

«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;

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

«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;

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

«SAT»: Soggetto Autorizzato al Trattamento dei dati personali

«RT»: Responsabile del Trattamento dei dati personali

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

«UOC»: Unità Operativa Complessa

«UOSD»: Unità Operativa Semplice Dipartimentale

«AdS»: Amministratore di Sistema

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 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

5.1.1 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.

5.1.2 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.

5.2 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.

5.2.1 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.

5.3 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

Al fine di consentire la definizione di un organigramma aziendale privacy all'interno di organizzazioni 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 possa ricorrere alla attribuzione di funzioni e compiti a soggetti designati.

Nello specifico, l'*art. 2 - quaterdiecies* stabilisce che il titolare o il responsabile del trattamento possano 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 (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.

Le ulteriori figure previste sono le seguenti:

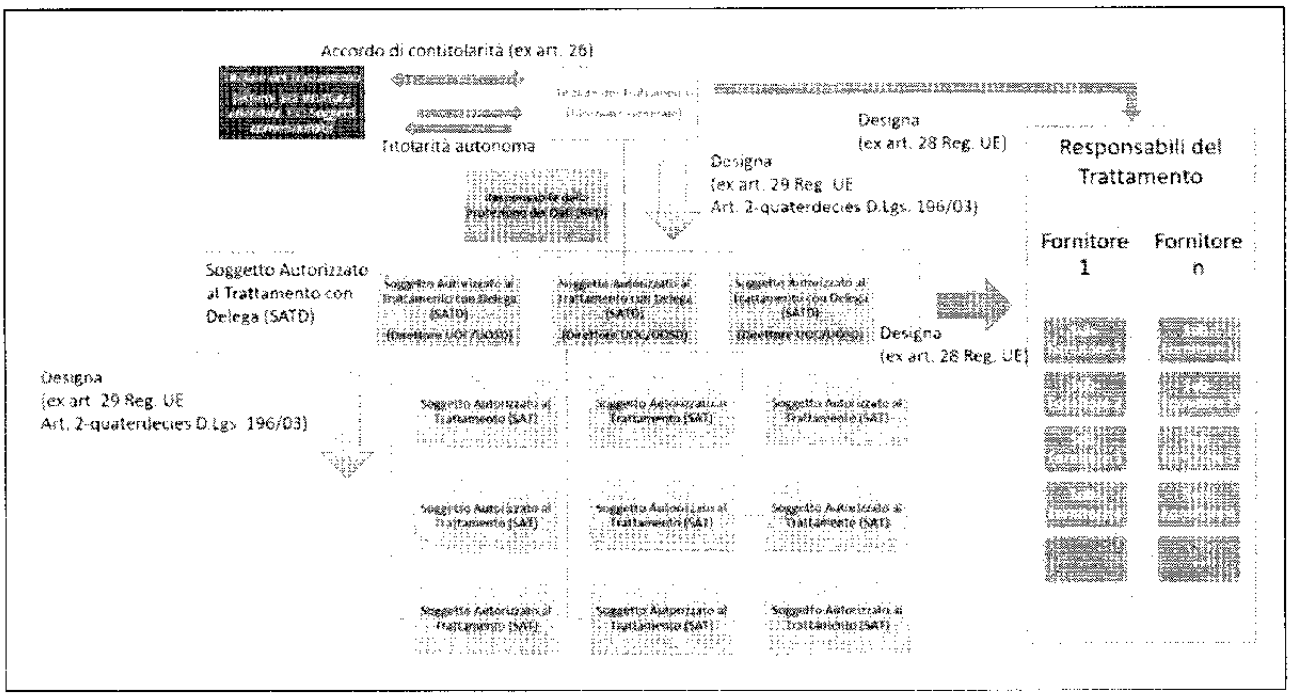
- Responsabile del Trattamento (ex art. 28 del Regolamento) ed eventuali sub-Responsabili
- Amministratori di Sistema (Provvedimento del Garante per la Protezione dei Dati Personali del 27 Novembre 2008)
- Contitolari del Trattamento (ex art. 26 del Regolamento)
- Titolari autonomi del Trattamento

6.2 Struttura organizzativa dell'Azienda Sanitaria

La struttura organizzativa dell'azienda è quella definita con atto aziendale approvato con Deliberazione n. 1207/18 e ss.mm.ii.

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
- Amministratori di Sistema

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 della normativa vigente in materia e garantisca la tutela dei diritti dell'interessato.

Il ruolo di Soggetto Autorizzato al Trattamento con Delega (SATD) viene identificato nelle funzioni di:

- Direttore Sanitario e Direttore Amministrativo,
- Direttore di Dipartimento,
- Direttore di UOC (Unità Operativa Complessa),
- Responsabile di UOSD (Unità Operativa Semplice Dipartimentale).

Il ruolo di Direttore/Responsabile delle strutture indicate costituisce 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 (es.: Attività libero professionale) 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.

La lettera di nomina, debitamente allegata al conferimento dell'incarico, dovrà essere compilata dall'UOC Personale[1] che ne curerà l'iter di sottoscrizione, protocollazione e conservazione nel fascicolo personale del dipendente. Copia della lettera dovrà essere trasmessa tramite il sistema di gestione documentale all'Ufficio Privacy per l'aggiornamento del Registro delle Nomine. Il Registro delle Nomine dovrà contenere almeno i seguenti campi:

- Numero di Registrazione (Progressivo)
- Nome
- Cognome

[1] Nelle more della piena operatività della presente procedura, la gestione delle nomine verrà condivisa con l'Ufficio Privacy

- Matricola
- Unità Operativa/Struttura
- Data Inizio
- Data Fine
- Motivazione di fine nomina
- Riferimento documento (protocollo) della lettera di incarico
- Riferimento documento (protocollo) dell'atto di designazione
- Eventuali Note

Il modello di tale registro è allegato alla presente procedura.

La vigenza della nomina si intenderà associata alla vigenza dell'incarico; di conseguenza, la cessazione dell'incarico comporterà la cessazione della validità della nomina.

In caso di assenza o impedimento del SATD (es.: in caso di ferie, malattia o altra temporanea assenza), il sostituto individuato ne assumerà temporaneamente le relative funzioni.

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 dipendenti e collaboratori del SATD che compiono attività di trattamento; l'elenco dei soggetti designati comprenderà, letteralmente, tutto il personale assegnato, anche parzialmente, alla struttura organizzativa 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 ricevuta); l'atto dovrà essere redatto utilizzando il Modello che si allega alla presente procedura, debitamente protocollato.

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 risulti 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.

A valle della designazione del Soggetto Autorizzato al Trattamento, il SATD dovrà predisporre ed aggiornare l'elenco dei propri SAT, tramite opportuno registro, il cui modello è allegato alla presente procedura. Esso dovrà contenere almeno i seguenti campi:

- Numero di Registrazione (Progressivo)
- Nome
- Cognome
- Matricola
- Data Inizio

- Data Fine
- Motivazione di fine nomina (ad es.: ordine di servizio, ecc...)
- Riferimento documento (es.: protocollo)
- Eventuali Note.

L'aggiornamento va compiuto ogni qual volta si proceda ad una nuova nomina o, comunque, sia abbia evidenza di variazioni nelle assegnazioni di personale (ad esempio a seguito di assegnazione temporanea, quiescenza, trasferimento).

Sarà comunque cura del SATD assicurarsi del puntuale aggiornamento dell'elenco dei Soggetti Autorizzati.

7.2.3 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 degli strumenti di supporto per il trattamento dei dati personali (es.: account posta elettronica, sistemi gestionali sanitari, sistemi gestionali contabili, ecc...), ed al contempo, in caso di variazione della designazione, tali credenziali siano conseguentemente modificate/ritirate; questo adempimento va espletato servendosi del supporto tecnico dell'UOSD Sistemi Informativi e Unità Operative che gestiscono le credenziali degli applicativi utilizzati.

7.2.4 Archiviazione degli atti

L'originale degli atti (Nomine SAT e relativi elenchi), dovranno essere conservati a cura del SATD designante in un proprio archivio opportunamente protetto.

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 due 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

I modelli di designazione, per le due tipologie indicate, sono allegati alla presente procedura.

7.3.2 Designazione

La designazione dei Responsabili del Trattamento, da effettuarsi in sede di sottoscrizione del contratto/convenzione/accordo con il soggetto Terzo, deve essere effettuata direttamente dai Direttori/Responsabili delle Strutture competenti che procedono all'affidamento dei servizi/incarichi professionali nel caso comportino il trattamento di dati personali.

In particolare, le Strutture interessate dovranno trasmettere all'Ufficio Privacy la seguente documentazione (in funzione del tipo di rapporto instaurato con il soggetto terzo – contratto/convenzione/accordo), al fine di fornire un supporto preliminare per la corretta predisposizione dei contratti di nomina dei Fornitori/soggetti Terzi (APD-Accordi sulla protezione dei dati), in qualità di Responsabili del trattamento dei dati, ai sensi dell'art. 28 del GDPR:

- provvedimento integrale di aggiudicazione del servizio/incarico (sono esclusi i lavori e le forniture)
- contratto/convenzione/accordo tra le parti
- offerta tecnica del Fornitore

Si evidenzia che l'accordo APD dovrà essere firmato (digitalmente) dal Fornitore, in qualità di Responsabile del trattamento dei dati e controfirmato dal Direttore/Responsabile (SATD) della Struttura interessata, su delega del Direttore Generale. L'accordo finale, sottoscritto per ciascun trattamento di dati personali effettuato da Terzi per conto dell'ASL 1 Abruzzo, dovrà essere custodito dal Direttore/Responsabile (SATD) per competenza, inoltrato all'Ufficio Privacy ed esibito su richiesta dell'Autorità Garante.

Per i casi di servizi che coinvolgano più Strutture (es.: servizio di conservazione di cartelle cliniche), la designazione dei Responsabili del Trattamento, da effettuarsi in sede di sottoscrizione del contratto/convenzione con il soggetto terzo, dovrà essere effettuata direttamente dal Titolare del Trattamento. Preliminarmente, in sede di redazione della delibera di aggiudicazione o della delibera di approvazione della convenzione, il Titolare dovrà indicare i competenti Soggetti Autorizzati al Trattamento di dati personali con Delega (SATD) delle strutture coinvolte, quali figure deputate al controllo del rispetto degli adempimenti privacy da parte del soggetto terzo.

In questo caso l'accordo APD dovrà essere firmato (digitalmente) dal Fornitore (come nel caso precedente), in qualità di Responsabile del trattamento dei dati e controfirmato dal Direttore Generale. L'accordo finale, sottoscritto per ciascun trattamento di dati personali effettuato da Terzi per conto dell'ASL 1 Abruzzo, dovrà essere custodito dal Titolare, inviato in copia ai Direttori/Responsabili (SATD) per competenza ed all'Ufficio Privacy ed esibito su richiesta dell'Autorità Garante.

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 ai soggetti terzi, in via preliminare, con specifico riferimento al caso di Società/Organizzazioni che erogano servizi presso le strutture o per conto dell'Azienda (punto 2 del paragrafo 7.3.1.1), 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 in sede alla sottoscrizione del contratto di fornitura al fine di poter garantire un corretto trattamento di dati personali da parte del soggetto terzo.

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

- 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 (Direttore Generale o SATD), essere corredata da ulteriori aspetti specifici riguardanti l'oggetto della fornitura (servizi o altro).

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 e di seguito elencati:

- Impegno a 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 del Trattamento

Il SATD deputato al controllo ha l'obbligo, in base a quanto previsto dal modulo di designazione, di monitorare l'operato dei Responsabili del Trattamento 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 validità della designazione è correlata alla durata del contratto/convenzione con il soggetto terzo.

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. Il registro dovrà contenere almeno i seguenti campi (il modello è allegato alla presente procedura):

- Numero di Registrazione (Progressivo)
- Soggetto Designato (ad es.: Ragione Sociale, Nome e Cognome nel caso di un professionista)
- Servizi (servizi previsti dal contratto di fornitura, convenzione, libera professione, ecc…)
- Data Inizio
- Data Fine
- Motivazione di fine designazione (ad es.: risoluzione anticipata, ecc…)
- Riferimento protocollo Contratto/Accordo/Convenzione
- Riferimento protocollo Documento di Designazione
- Eventuali Note (in cui è possibile indicare eventuali proroghe, risoluzioni anticipate dei contratti e relative motivazioni).

7.4 Sub-Responsabili del Trattamento

In virtù di quanto disposto dall'art. 28.2 del Regolamento, il soggetto designante il Responsabile del Trattamento (RT), si occupa di raccogliere e valutare, con il supporto 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 dal valutatore.

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 dal Titolare, o suoi delegati, con il supporto del Responsabile della Protezione dei Dati.

In caso di titolarità autonoma, il modello di riferimento per l'impegno da parte del Soggetto Terzo è allegato alla presente procedura.

In caso di Contitolarità, il contenuto del modello precedentemente menzionato deve essere preso quale riferimento nella definizione delle clausole per gli specifici accordi (ex Art. 26 Regolamento).

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 per l'aggiornamento del relativo Registro. Il registro dovrà contenere almeno i seguenti campi (il modello è allegato alla presente procedura):

- Numero di Registrazione (Progressivo)
- Soggetto Contitolare/Titolare autonomo (ad es.: Ragione Sociale, Nome e Cognome nel caso di un professionista)
- Servizi (Servizi previsti dalla convenzione, accordo, ecc...)
- Data Inizio
- Data Fine
- Motivazione di fine rapporto (ad es.: risoluzione anticipata, ecc...)
- Riferimento protocollo Contratto/Accordo/Convenzione
- Riferimento protocollo Documento di Accordo
- Eventuali Note (in cui è possibile indicare eventuali proroghe, risoluzioni anticipate e relative motivazioni).

7.6 Amministratori di Sistema

7.6.1 Identificazione

In relazione ai sistemi informatici e tecnologici, inclusi quelli relativi alla gestione della tecnologia sanitaria, il Titolare deve 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 Garante per la Protezione dei Dati Personali.

In riferimento ai sistemi informatici (anche relativi alla tecnologia sanitaria) interni alle strutture dell'Azienda Sanitaria, che effettuano trattamento dei dati personali, è necessario nominare uno o più Amministratori di Sistema in funzione dei relativi ambiti di operatività. L'esigenza consiste nel valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di:

- amministratore di Sistema (*System Administrator*);
- amministratore di Base di Dati (*Database Administrator*)
- amministratore di Rete (*Network Administrator*)

laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il Titolare, previa opportuna designazione dei terzi in qualità di Responsabili del Trattamento, con il supporto del SATD di riferimento (o SATD referente), per il tramite del SATD Delegato dell'UOSD Sistemi Informativi o del SATD Delegato dell'UOC Ingegneria Clinica, in base alle rispettive competenze, deve conservare, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema in relazione agli ambiti operativi e di responsabilità loro affidati.

7.6.2 Designazione

Per la nomina ad Amministratore di Sistema (AdS) deve essere utilizzato l'apposito modello allegato alla presente procedura.

La lettera di nomina dovrà essere compilata e sottoscritta dal SATD dell'UOSD Sistemi Informativi o dell'UOC Ingegneria Clinica, in base alle rispettive competenze, che ne curerà l'iter di sottoscrizione, protocollazione e conservazione. Copia della lettera dovrà essere trasmessa tramite il sistema di gestione documentale all'Ufficio Privacy per l'aggiornamento del Registro delle Nomine. Il registro dovrà contenere almeno i seguenti campi (il modello è allegato alla presente procedura):

- Numero di Registrazione (Progressivo)
- Soggetto Designato (ad es.: Ragione Sociale, Nome e Cognome nel caso di un professionista)
- Servizi (servizi previsti dal contratto di fornitura, convenzione, ecc…)
- Data Inizio
- Ambiti (indicazione degli ambiti per i quali viene svolta l'attività di Amministrazione di sistema, es.: Rete, Nome Applicativo, database, sistema di posta elettronica, ecc…)
- Data Fine
- Motivazione di fine designazione (ad es.: risoluzione anticipata, ecc…)
- Riferimento protocollo Contratto/Accordo/Convenzione
- Riferimento protocollo Documento di Designazione
- Eventuali Note (in cui è possibile indicare eventuali proroghe, risoluzioni anticipate dei contratti e relative motivazioni).

La nomina si intenderà vigente fino ad esplicita revoca da parte del Titolare o del SATD sottoscrittore.

In caso di assenza o impedimento dell'Amministratore di Sistema (es.: in caso di ferie, malattia o altra temporanea assenza), deve essere individuato un sostituto che ne assumerà temporaneamente le relative funzioni.

Ulteriori dettagli relativi alle modalità di gestione degli Amministratori di Sistema sono indicate nel modulo di nomina dei Soggetti Autorizzati al Trattamento con Delega allegato alla presente procedura.

7.7 Conclusioni

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

8 Allegati

Alla presente procedura sono allegati i seguenti documenti:

- Allegato 1 – PRY-SATD-001 – Modulo di nomina per Soggetto Autorizzato al Trattamento dei dati con Delega (SATD)
- Allegato 2 – PRY-MOD-010 – Modello di Registro di Soggetti Autorizzati al Trattamento con Delega (SATD)
- Allegato 3 – PRY-SAT-001 – Modulo di nomina per Soggetto Autorizzato al Trattamento dei dati (SAT)
- Allegato 4 – PRY-MOD-011 – Modello di Registro di Soggetti Autorizzati al Trattamento
- Allegato 5 – PRY-RT-001 – Modulo di designazione per Responsabile del Trattamento (Caso 1 Professionisti) da parte del Titolare
- Allegato 6 – PRY-RT-002 – Modulo di designazione per Responsabile del Trattamento (Caso 1 Professionisti) da parte del SATD
- Allegato 7 – PRY-RT-003 – Modulo di designazione per Responsabile del Trattamento (Caso 2 – Aziende/Organizzazioni) da parte del Titolare
- Allegato 8 – PRY-RT-004 – Modulo di designazione per Responsabile del Trattamento (Caso 2 – Aziende/Organizzazioni) da parte del SATD
- Allegato 9 – PRY-MOD-012 – Modello di Registro per Responsabili del Trattamento
- Allegato 10 – PRY-ADS-001 – Modulo di nomina per Amministratori di Sistema (AdS)
- Allegato 11 – PRY-MOD-013 – Modello di Registro per Amministratori di Sistema
- Allegato 12 – PRY-TA-001 – Modulo di impegno da parte del Titolare Autonomo
- Allegato 13 – PRY-MOD-014 – Modello di Registro per Contitolari e Titolari Autonomi

Azienda Sanitaria Locale
Avezzano, Sulmona, L'Aquila

Regione Abruzzo – ASL 01 Avezzano Sulmona L'Aquila

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)

Sede Legale:
Via Saragat – Località Campo di Pile
67100 L'Aquila
P. IVA 01792410662

IL DIRETTORE GENERALE

Prot. n. _____/ L'Aquila, lì _____

Preg.mo Dr./Sig./Dr.ssa/Sig.ra _____

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 Direttore Generale in qualità di rappresentante legale della ASL di Avezzano Sulmona L'Aquila – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano Sulmona L'Aquila – 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) 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 Avezzano Sulmona L'Aquila 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 Avezzano Sulmona L'Aquila (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 _____ (Ambito di Trattamento)

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), designate 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 (ufficioprivacy@asl1abruzzo.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) impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 della presente Lettera di Nomina;

   b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32, come previsto dall'art. 5 della presente Lettera di Nomina;

   c) ove competente (ved. Art. 6) designare i Responsabili ed 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. 6 della presente Lettera di Nomina;

   d) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'Art. 7 della presente Lettera di Nomina;

   e) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 8 della presente Lettera di Nomina;

   f) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'Art.9 della presente Lettera di Nomina;

   g) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'Art.10 della presente Lettera di Nomina;

   h) 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. 11 della presente Lettera di Nomina;

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

   j) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 della presente Lettera di Nomina;

   k) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 della presente Lettera di Nomina;

   l) redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e degli eventuali Responsabili e 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, se designati dal SATD, dai Responsabili e 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 dalla presente Lettera di Nomina.

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 designazione a Responsabile del Trattamento. Ove competente, il Delegato deve garantire l'adeguata compilazione da parte del fornitore dei sopracitati allegati relativi 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 designazione a Responsabile del Trattamento e a verificarne l'effettiva attuazione. Ove competente, il Delegato deve garantire l'adeguata compilazione da parte del fornitore dei sopracitati allegati relativi 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, quest'ultimo potrà avvalersi di Responsabili del trattamento esterni all'organizzazione del Titolare – ASL – (ciascuno un "Responsabile del Trattamento") ai sensi dell'art. 28 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 Titolare o da suo Delegato ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Titolare o suo Delegato, secondo quanto previsto dalla Procedura di Gestione di Accordi, Nomine e Designazioni, designerà 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 SATD**

deputato al controllo (detto SATD Referente), individuato per lo specifico contratto/convenzione secondo le modalità specificate nella Procedura sopra indicata, 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.

2) Il SATD, quando indicato come referente, si impegna a garantire il rispetto delle istruzioni impartite al Responsabile e a relazionare periodicamente al Titolare, in forma scritta, in merito alla corretta esecuzione del servizio. 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, il SATD referente agirà con il supporto dei dirigenti dell'UOSD Sistemi Informativi e/o della UOC Ingegneria Clinica (in base alle rispettive competenze). La periodicità di relazione da parte del SATD referente 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;

3) 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 SATD referente, potrà essere esaminata caso per caso con l'ausilio dell'Ufficio Privacy (competente struttura del Titolare) e del Responsabile della Protezione dei Dati (RPD).

4) Il SATD referente si impegna a informare anticipatamente il Titolare e il Responsabile della Protezione dei Dati, con mezzi elettronici (via PEC), laddove il Responsabile intenda, per l'erogazione dei servizi e/o delle forniture, avvalersi e, di conseguenza, designare, sostituire o cessare il rapporto con un Sub-responsabile del Trattamento che agisca in nome e per conto del Responsabile. La designazione, sostituzione o cessazione si intenderà accettata dal Titolare a seguito di formale positivo riscontro o in caso di mancato riscontro entro 30 giorni dalla comunicazione.

5) Qualora il Titolare sollevi obiezioni su uno o più Responsabili o sub-responsabili del Trattamento, egli darà indicazioni al SATD referente 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 SATD referente 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 e dalle normative vigenti in materia, e del rispetto delle istruzioni impartite (ved. Art. 3)**.

7) Nel caso in cui un Responsabile o un Sub-responsabile del Trattamento siano situati in un Paese terzo (extra UE), il SATD referente 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 SATD referente 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 15 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 15 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 all'indirizzo databreach@asl1abruzzo.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 dipendenti e collaboratori da lui diretti, deputati a trattare i Dati Personali del Titolare nell'ambito di trattamento dell'UO diretta dal SATD, 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 (a mezzo posta elettronica all'indirizzo sicurezzainformatica@asl1abruzzo.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, mediante opportuna annotazione nell'apposito registro come previsto dalla Procedura per la Gestione di Accordi, Nomine e Designazioni. Tale revoca dovrà essere opportunamente e tempestivamente comunicata all'UOSD Sistemi Informativi (a mezzo posta elettronica all'indirizzo sicurezzainformatica@asl1abruzzo.it) per le necessarie revoche 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, mediante opportuna annotazione nell'apposito registro come previsto dalla Procedura per la Gestione di Accordi, Nomine e Designazioni, ed a comunicare tempestivamente la sospensione all'UOSD Sistemi Informativi (a mezzo posta elettronica all'indirizzo sicurezzainformatica@asl1abruzzo.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 i SATD della UOSD Sistemi Informativi e dell'UOC Ingegneria Clinica) 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 esercitino 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 designati Responsabili del Trattamento dal Delegato) esercitino 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

Per ricezione ed integrale accettazione del Delegato

Dr./Dr.ssa

1660

1665

ALLEGATO 2-PRY MOD 010
MODELLO REGISTRO SATD

Progressivo	Nome	Cognome	Matricola	UO/Struttura	Data Inizio	Data Fine	Motivazione di fine nomina	Riferimento lettera di incarico (protocollo)	Riferimento atto di nomina (protocollo)	Note

1644

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)

Sede Legale:
Via Saragat – Località campo di Pile
67100 L'Aquila
P. IVA 01792410662

IL SOGGETTO AUTORIZZATO AL TRATTAMENTO CON DELEGA (SATD)

Dr./Dr.ssa _____
Ruolo: _____

Prot. n. _____/ L'Aquila, lì _____

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

Ruolo: _____

UO di assegnazione _____

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 Avezzano, Sulmona, L'Aquila (ASL n.1 Abruzzo di seguito anche la "ASL") – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano, Sulmona, L'Aquila – 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 Avezzano, Sulmona, L'Aquila e sul Soggetto Autorizzato al Trattamento di dati personali (di seguito "Soggetto Autorizzato" o SAT) 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
Soggetto Autorizzato al Trattamento di dati personali (SAT) e
dell'Art. 2-quaterdecies del D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018)

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

per i dati trattati dall'Unità Operativa _____ (Ambito di Trattamento)

La presente nomina si applica a tutte le attività svolte dal Soggetto Autorizzato (SAT) 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 la Lei svolto in qualità di 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 del profilo di autorizzazione a Lei attribuito.
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) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 della presente Lettera di Nomina;

   b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32, come previsto dall'art. 5 della presente Lettera di Nomina;

   c) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'Art. 6 della presente Lettera di Nomina;

   d) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'Art.7 della presente Lettera di Nomina;

   e) rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 8 e 9 della presente Lettera di Nomina;

   f) 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;

   g) conservare separatamente i dati appartenenti a particolari categorie di dati (Art. 9 GDPR);

   h) consultare esclusivamente i documenti contenenti dati personali necessari per lo svolgimento dell'attività lavorativa prestando particolare attenzione alla custodia ed archiviazione degli stessi;

   i) 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;

   j) custodire e tutelare l'accessibilità agli strumenti elettronici soprattutto mentre è in corso una sessione di lavoro;

   k) utilizzare gli strumenti ed i programmi in conformità ai regolamenti ("policies") aziendali al fine di proteggere i sistemi informativi e i dati ivi contenuti;

   l) utilizzare, custodire ed archiviare i supporti rimuovibili contenenti dati personali, in maniera da preservarne il contenuto, in conformità ai regolamenti aziendali.

m) 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;

n) 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;

o) accedere ai soli dati necessari all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;

p) comunicare solo i dati personali preventivamente autorizzati dal Titolare e/o dallo scrivente SATD;

q) informare prontamente il Titolare e/o lo scrivente SATD di ogni questione rilevante ai fini del rispetto della normativa in materia di protezione dei dati personali;

r) 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.

5) 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.

6) 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, utilizzando 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) 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 di lavoro 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) Quanto disposto nella presente nomina in termini di compiti e responsabilità e quanto applicato all'interno della struttura in materia di Protezione dei Dati Personali, come dettato dal Regolamento UE 679/2016 e dal D.Lgs. 196/03 mod. dal D. Lgs. 101/2018, è insito nel rapporto contrattuale di lavoro.

4) 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)

Dr./Dr.ssa _____

_____

Per ricevuta del Soggetto Autorizzato (SAT)

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

_____

ALLEGATO 4 - PRY - MOD 011
MODELLO REGISTRO SAT

Progressivo	Nome	Cognome	Matricola	Data Inizio	Data Fine	Motivazione di fine nomina	Riferimento documento (protocollo)	Note

Sede Legale:
Via Saragat – Località Campo di Pile
67100 L'Aquila
P. IVA 01792410662

Il DIRETTORE GENERALE

Prot. n. _____/ L'Aquila, lì _____

Spett.le _____

Indirizzo: _____

CF/P.IVA _____

Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali di _____ *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 AQ n. _____ del __/__/__.

Il sottoscritto Direttore Generale, Dott. Roberto Testa, in qualità di rappresentante legale della ASL di Avezzano Sulmona L'Aquila – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano - Sulmona - L'Aquila – 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) Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL AQ n. _____ del __/__/__ (di seguito la "Delibera") tra la ASL di Avezzano - Sulmona - L'Aquila (di seguito "ASL AQ" 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

il Dott./Dott.ssa _____

quale Responsabile del Trattamento

dei dati personali trattati per conto della ASL di Avezzano - Sulmona - L'Aquila nell'ambito del servizio

_____ (oggetto della Delibera)

16

Il Soggetto Autorizzato al Trattamento con Delega di Riferimento (SATD REFERENTE) è il Direttore/Responsabile della UOC/UOSD _____ Dott./Dott.ssa _____; a tale figura è affidato il compito di controllo del rispetto degli obblighi in materia di protezione dei dati da parte del Responsabile del Trattamento.

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 AQ).

Di seguito verranno intesi il Responsabile e la ASL di Avezzano - Sulmona - L'Aquila 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 Referente (email: _____@asl1abruzzo.it), all'Ufficio Privacy (email: ufficioprivacy@asl1abruzzo.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo@asl1abruzzo.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 Avezzano - Sulmona - L'Aquila, 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, 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 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 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 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 che verranno indicate dal Titolare.

3) Come ulteriore garanzia per la sicurezza del trattamento, il Responsabile si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti al Titolare o al Soggetto Autorizzato al Trattamento con Delega referente.

4) Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative previste dal Titolare, 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 Responsabile, come descritto nel Contratto allegato alla Delibera, il Responsabile 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 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 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, 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 48 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 Responsabile, 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 protocollogenerale@pec.asl1abruzzo.it e databreach@asl1abruzzo.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:
   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 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:
   1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli 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, 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 protocollogenerale@pec.asl1abruzzo.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 Direttore Generale ASL Avezzano Sulmona L'Aquila (TITOLARE)

Dott. Roberto Testa

Per ricezione ed integrale accettazione del Responsabile

Nome e Cognome del Soggetto Autorizzato al Trattamento con Delega (SATD) – (REFERENTE)

Dr./ssa

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 Avezzano - Sulmona - L'Aquila, 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	

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. _____
24. _____
25. _____
26. _____
27. _____
28. _____

Sede Legale:
Via Saragat – Località Campo di Pile
67100 L'Aquila
P. IVA 01792410662

Il SOGGETTO AUTORIZZATO AL TRATTAMENTO

Di DATI PERSONALI CON DELEGA (SATD)

Prot. n. _____/ L'Aquila, lì _____

Spett.le _____

Indirizzo: _____

CF/P.IVA _____

Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali di _____ *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 AQ n. _____ del __/__/__.

Il sottoscritto Dr. _____in qualità di Soggetto Autorizzato al Trattamento con Delega (di seguito anche SATD) della ASL di Avezzano Sulmona L'Aquila – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano - Sulmona - L'Aquila – 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) Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL AQ n. _____ del __/__/__ (di seguito la "Delibera") tra la ASL di Avezzano - Sulmona - L'Aquila (di seguito "ASL AQ" 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

il Dott./Dott.ssa _____

quale Responsabile del Trattamento

dei dati personali trattati per conto della ASL di Avezzano - Sulmona - L'Aquila nell'ambito del servizio

_____ (oggetto della Delibera)

Il Soggetto Autorizzato al Trattamento con Delega di Riferimento (SATD REFERENTE) è il Direttore/Responsabile della UOC/UOSD _____ Dott./Dott.ssa_____; a tale figura è affidato il compito di controllo del rispetto degli obblighi in materia di protezione dei dati da parte del Responsabile del Trattamento.

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 AQ).

Di seguito verranno intesi il Responsabile e la ASL di Avezzano - Sulmona - L'Aquila 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 e Referente (email: _____@asl1abruzzo.it), all'Ufficio Privacy (email: ufficioprivacy@asl1abruzzo.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo@asl1abruzzo.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 Avezzano - Sulmona - L'Aquila, 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, 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 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 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 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 che verranno indicate dal Titolare.

3) Come ulteriore garanzia per la sicurezza del trattamento, il Responsabile si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti al Titolare o al Soggetto Autorizzato al Trattamento con Delega referente.

4) Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative previste dal Titolare, 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 Responsabile, come descritto nel Contratto allegato alla Delibera, il Responsabile 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 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 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, 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 48 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 Responsabile, 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 protocollogenerale@pec.asl1abruzzo.it e databreach@asl1abruzzo.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:
   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 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:
   1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli 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, 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 protocollogenerale@pec.asl1abruzzo.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) – (REFERENTE)	Per ricezione ed integrale accettazione del Responsabile
Dr. _____	_____
_____	_____

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 Avezzano - Sulmona - L'Aquila, 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	

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. _____
24. _____
25. _____
26. _____
27. _____
28. _____

Azienda Sanitaria Locale Avezzano, Sulmona, L'Aquila	**Regione Abruzzo - ASL 01 Avezzano Sulmona L'Aquila**
	LETTERA DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI **Art. 28 Regolamento UE 679/2016**

Sede Legale:
Via Saragat – Località Campo di Pile
67100 L'Aquila
P. IVA 01792410662

Il DIRETTORE GENERALE

Prot. n. _____/ L'Aquila, lì _____

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 AQ n. _____ del __/__/__.

Il sottoscritto Direttore Generale in qualità di rappresentante legale della ASL di Avezzano Sulmona L'Aquila – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano - Sulmona - L'Aquila – 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) Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL AQ n. _____ del __/__/__ (di seguito la "Delibera") tra la ASL di Avezzano - Sulmona - L'Aquila (di seguito "ASL AQ" 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 Avezzano - Sulmona - L'Aquila nell'ambito del servizio

_____ (oggetto della Delibera)

Il Soggetto Autorizzato al Trattamento con Delega di Riferimento (SATD REFERENTE) è il Direttore/Responsabile della UOC/UOSD _____

Dott./Dott.ssa_____; a tale figura è affidato il compito di controllo del rispetto degli obblighi in materia di protezione dei dati da parte del Responsabile del Trattamento.

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 AQ).

Di seguito verranno intesi il Responsabile e la ASL di Avezzano - Sulmona - L'Aquila 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 anche al Soggetto Autorizzato con Delega Referente (email: _____@asl1abruzzo.it), all'Ufficio Privacy (email: ufficioprivacy@asl1abruzzo.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo@asl1abruzzo.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 Avezzano - Sulmona - L'Aquila, 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»).

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 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 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 del GDPR, 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 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 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 Responsabile si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti secondo quanto previsto dall'Allegato 3.

4) Qualora il Responsabile 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 Responsabile, come descritto nel Contratto allegato alla Delibera, il Responsabile 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 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 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, 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 48 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 Responsabile, 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 protocollogenerale@pec.asl1abruzzo.it e databreach@asl1abruzzo.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 all'atto 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.

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 allegato alla Delibera dovrà essere periodicamente (ogni anno entro il 31 gennaio) fornito al Titolare.

6) Il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'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) 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 31/01) 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;
    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 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 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:
   1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli 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, 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 protocollogenerale@pec.asl1abruzzo.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 protocollogenerale@pec.asl1abruzzo.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 Direttore Generale ASL Avezzano Sulmona L'Aquila (TITOLARE)

Per ricezione ed integrale accettazione del Responsabile

Il Soggetto Autorizzato al Trattamento con Delega (SATD) – (REFERENTE)

Dr./ssa

ALLEGATO 1 – Ambito di Trattamento e Categorie di attività

Scheda n. _____

Nella scheda seguente (una per ogni trattamento), nell'ambito dei servizi erogati per conto della ASL di Avezzano - Sulmona - L'Aquila, vengono definiti l'ambito di Trattamento e le categorie di attività svolte dal Responsabile; 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	

650

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 *(**A**dottata /**P**ianificata /**N**on Prevista)*	Descrizione
A.1	Art. 5.1.a – liceità	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.2	Art. 5.1.b – limitazione della finalità	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.3	Art. 5.1.c – minimizzazione dei dati	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.4	Art. 5.1.d – esattezza/qualità dei dati	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.5	Art. 5.1.e Limitazione della conservazione	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.6	Artt. 12, 13 e 14 – Informazioni per gli interessati	☐ SI ☐ NO	☐ A ☐ P ☐ 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. 7 – Gestione del Consenso al Trattamento	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.7	Art. 15 Diritto di Accesso dell'interessato	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.8	Art. 16 – Diritto di Rettifica	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione sia delle modalità operative per l'esercizio del diritto in questione*
A.9	Art. 17 – Diritto alla Cancellazione ("Oblio")	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione sia delle modalità operative per l'esercizio del diritto in questione*
A.10	Art. 18 – Diritto alla Limitazione del Trattamento	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione sia delle modalità operative per l'esercizio del diritto in questione*
A.11	Art. 19 – Obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione delle modalità operative per tenere traccia dei destinatari e garanzia dei diritti*
A.12	Art. 20 – Diritto alla portabilità dei dati	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione sia delle modalità operative per l'esercizio del diritto in questione*
A.13	Art. 21 – Diritto di Opposizione	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione sia delle modalità operative per l'esercizio del diritto in questione*
A.14	Art. 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la *profilazione*	☐ SI ☐ NO	☐ A ☐ P ☐ NP	*Indicazione delle modalità di gestione del processo decisionale automatizzato e delle modalità per garantire l'esercizio del diritto in oggetto.*

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.

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	

ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto

Fornire una descrizione del servizio fornito e dell'articolazione organizzativa finalizzata all'erogazione. È possibile allegare eventuali documenti descrittivi o schede tecniche.

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. _____
26. _____
27. _____
28. _____
29. _____
30. _____

Azienda Sanitaria Locale Avezzano Sulmona L'Aquila	**Regione Abruzzo – ASL 01 Avezzano Sulmona L'Aquila**
	LETTERA DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI
	Art. 28 Regolamento UE 679/2016

Sede Legale:
Via Saragat – Località Campo di Pile
67100 L'Aquila
P. IVA 01792410662

Il SOGGETTO AUTORIZZATO AL TRATTAMENTO Di DATI PERSONALI CON DELEGA (SATD)

Prot. n. _____/ L'Aquila, 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 AQ n. _____ del __/__/__.

Il sottoscritto Dr. _____in qualità di Soggetto Autorizzato al Trattamento con Delega (di seguito anche SATD) della ASL di Avezzano Sulmona L'Aquila – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano - Sulmona - L'Aquila – 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) Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL AQ n. _____ del __/__/__ (di seguito la "Delibera") tra la ASL di Avezzano - Sulmona - L'Aquila (di seguito "ASL AQ" 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 Avezzano - Sulmona - L'Aquila nell'ambito del servizio

_____ (oggetto della Delibera)

Il Soggetto Autorizzato al Trattamento con Delega di Riferimento (SATD REFERENTE) è il Direttore/Responsabile della UOC/UOSD _____
Dott./Dott.ssa_____; a tale figura è affidato il compito di controllo del rispetto degli obblighi in materia di protezione dei dati da parte del Responsabile del Trattamento.

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 AQ).

Di seguito verranno intesi il Responsabile e la ASL di Avezzano - Sulmona - L'Aquila 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 anche al Soggetto Autorizzato con Delega scrivente e Referente (email: _____@asl1abruzzo.it), all'Ufficio Privacy (email: ufficioprivacy@asl1abruzzo.it) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: dpo@asl1abruzzo.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 Avezzano - Sulmona - L'Aquila, 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»).

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 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 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 del GDPR, 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 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 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 Responsabile si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti secondo quanto previsto dall'Allegato 3.

4) Qualora il Responsabile 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 Responsabile, come descritto nel Contratto allegato alla Delibera, il Responsabile 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 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 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, 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 48 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 Responsabile, 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 protocollogenerale@pec.asl1abruzzo.it e databreach@asl1abruzzo.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 all'atto 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.

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 allegato alla Delibera dovrà essere periodicamente (ogni anno entro il 31 gennaio) fornito al Titolare.

6) Il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'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) 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 31/01) 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;
   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 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 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:
   1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli 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, 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 protocollogenerale@pec.asl1abruzzo.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 protocollogenerale@pec.asl1abruzzo.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) – (REFERENTE)	Per ricezione ed integrale accettazione del Responsabile
Dr./ssa	

ALLEGATO 1 – Ambito di Trattamento e Categorie di attività

Scheda n. _____

Nella scheda seguente (una per ogni trattamento), nell'ambito dei servizi erogati per conto della ASL di Avezzano - Sulmona - L'Aquila, vengono definiti l'ambito di Trattamento e le categorie di attività svolte dal Responsabile; 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	

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	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.2	Art. 5.1.b – limitazione della finalità	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.3	Art. 5.1.c – minimizzazione dei dati	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.4	Art. 5.1.d – esattezza/qualità dei dati	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.5	Art. 5.1.e Limitazione della conservazione	☐ SI ☐ NO	☐ A ☐ P ☐ NP	
A.6	Artt. 12, 13 e 14 – Informazioni per gli interessati	☐ SI ☐ NO	☐ A ☐ P ☐ NP	

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

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.

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	

ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto

Fornire una descrizione del servizio fornito e dell'articolazione organizzativa finalizzata all'erogazione. È possibile allegare eventuali documenti descrittivi o schede tecniche.

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. _____
26. _____
27. _____
28. _____
29. _____
30. _____

ALLEGATO 9 PRY-MOD 012

REGISTRO PER RESPONSABILI TRATTAMENTO

Progressivo	Soggetto Designato (società o esterno)	Servizi	Data Inizio	Data Fine	Motivazione di fine designazione	Riferimento protocollo Contratto/Convenzione	Riferimento protocollo Designazione	Note

Azienda Sanitaria Locale Avezzano, Sulmona, L'Aquila	**Regione Abruzzo – ASL 01 Avezzano Sulmona L'Aquila**
	LETTERA DI NOMINA DELL'AMMINISTRATORE DI SISTEMA **PROVVEDIMENTO DEL Garante Privacy del 27 Novembre 2008, Art. 29 Regolamento UE 679/2016,** **Art. 2-quaterdecies D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018)**

Sede Legale:
Via Saragat – Località Campo di Pile
67100 L'Aquila
P. IVA 01792410662

IL DIRETTORE GENERALE

Prot. n. _____/ L'Aquila, lì _____

Preg.mo Sig. /Sig.ra _____

Ruolo: _____

UO _____

Posta Elettronica _____

Oggetto: Lettera di Nomina ad Amministratore di Sistema ai sensi del Provvedimento del Garante Privacy del 27 Novembre 2008, 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 sottoscritto Dott. Roberto Testa in qualità di legale rappresentante della ASL di Avezzano Sulmona L'Aquila – Titolare del trattamento dei dati personali - considerato che:

a) La ASL di Avezzano Sulmona L'Aquila – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;
b) il Provvedimento a carattere generale del Garante per la Protezione dei Dati Personali del 27/11/2008 ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema") richiede una designazione individuale dei soggetti che svolgono le funzioni di Amministratore di Sistema ed un'elencazione analitica degli ambiti di operatività consentiti;
c) che il Sig. svolge alcune delle mansioni tipiche della figura di "Amministratore di Sistema" e possiede i requisiti di esperienza, capacità ed affidabilità prescritti dal citato provvedimento del Garante idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza;

con il presente atto nomina quale Amministratore di Sistema
ai sensi del citato Provvedimento del Garante per la Protezione dei Dati Personali ed 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)

Il/la Sig./Sig.ra _____

per il seguente ambito di operativo e di responsabilità

_____,

con il compito di sovrintendere ed amministrare gli strumenti informatici ad esso relativi.

1. COMPITI DELL'AMMINISTRATORE DI SISTEMA

I compiti affidati all'Amministratore di Sistema sono i seguenti:

1) assicurare il funzionamento del sistema informatico del titolare alla luce delle evoluzioni tecnologiche;
2) monitorare lo stato dei sistemi;
3) assicurare l'integrità, accessibilità e performance dei sistemi, realizzando periodiche manutenzioni, effettuando gli aggiornamenti necessari e definendo strategie di backup e restore dei dati per garantire il ripristino del sistema;
4) verificare costantemente che il titolare abbia adottato adeguate misure di sicurezza per il trattamento dei dati personali, previste dall'art. 32 del GDPR, provvedendo alla segnalazione di procedere con gli adeguamenti eventualmente necessari;
5) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, in merito all'efficacia delle misure di sicurezza adottate;
6) gestire il sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conformemente alle prassi e/o alle procedure aziendali sull'utilizzo degli strumenti informatici, di internet e della posta elettronica;
7) definire gli accessi al sistema attribuendo i profili di utilizzo per l'utente secondo le richieste del titolare o dei responsabili del trattamento nel rispetto delle misure di sicurezza;
8) attivare e aggiornare con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
9) aggiornare periodicamente, con frequenza almeno annuale, oppure semestrale se si trattano dati sensibili o giudiziari, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
10) distruggere i supporti di memorizzazione nel caso in cui non siano più riutilizzati in conformità al provvedimento del Garante del 13/10/2008 e s.m.i. ed alle procedure aziendali;
11) proporre al titolare ogni opportuna misura e ogni adeguata verifica, per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave se leggibili;
12) implementare i sistemi, individuati dal titolare del trattamento, idonei alla registrazione degli accessi logici (access log) ai sistemi di elaborazione ovvero ai sistemi di trasmissione dati o di sicurezza e agli archivi elettronici che vengono effettuati dagli Amministratori di Sistema in conformità al provvedimento a carattere generale del Garante per la protezione dei dati personali del 27/11/2008.

2. PUBBLICITÀ DELLA NOMINA

In conformità al punto 2.c) del dispositivo del citato provvedimento del Garante, gli estremi identificativi dell'Amministratore di Sistema, con l'elenco delle funzioni attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Gli estremi identificativi dell'Amministratore di Sistema ed i servizi informatici a cui è preposto saranno, inoltre, resi noti al personale del titolare nel caso di svolgimento di attività che, direttamente o indirettamente, consentono l'accesso a servizi o sistemi che trattano o permettono il trattamento di informazioni di carattere personale dei lavoratori.

3. VERIFICA DELLE ATTIVITÀ

In conformità punto 2.e) del dispositivo del citato provvedimento del Garante, il titolare del trattamento verifica, con cadenza almeno annuale, l'operato dell'Amministratore di Sistema, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

In conformità al punto 2.f) del dispositivo del citato provvedimento del Garante, saranno adottati sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione ed agli archivi elettronici da parte dell'Amministratore di Sistema.

4. DURATA

Il presente atto esplica i suoi effetti dalla data di sottoscrizione dello stesso da parte del titolare e dell'Amministratore di Sistema e cesserà i suoi effetti al momento della cessazione del rapporto di lavoro tra il titolare e l'Amministratore di Sistema, nonché in caso di modifica delle mansioni lavorative.

La sottoscrizione del presente atto non conferisce alcun diritto ad indennità posto che le attività oggetto dello stesso costituiscono un elemento delle mansioni lavorative assegnate in conformità al contratto di lavoro applicabile.

5. ISTRUZIONI

È tassativamente vietato qualsiasi trattamento effettuato con sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività dei dipendenti in rete informatica. In applicazione del principio di necessità, il Titolare del trattamento promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a minimizzare l'uso di dati riferibili ai dipendenti.

Per quanto attiene agli eventuali controlli sull'uso degli strumenti elettronici deve essere evitata ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei dipendenti, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. Infatti i controlli sono leciti solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'amministratore di sistema può adottare eventuali misure che consentano la verifica di comportamenti anomali, preferendo controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra-registrazione) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

La conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata solo da particolari esigenze tecniche o di sicurezza, o da una finalità specifica e comprovata e limitata al tempo necessario a raggiungerla.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziari o del Responsabile della Protezione dei dati personali.

Nei casi indicati, il trattamento dei dati personali e particolari (sensibili) deve essere limitato alle sole informazioni indispensabili per perseguire le finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Resta fermo l'obbligo del designato Amministratore di Sistema di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità legalmente previste, senza realizzare attività di controllo a distanza dei dipendenti.

All'atto della cessazione del rapporto con il Titolare, l'Amministratore di Sistema dovrà rendersi disponibile per il passaggio di consegne all'Amministratore di Sistema entrante.

IL DIRETTORE GENERALE

Dott. Roberto Testa

Per ricezione ed integrale accettazione del
l'Amministratore di Sistema

Sig./Sig.ra

ALLEGATO 11 PRY- MOD 013

REGISTRO PER AMMINITRATORI DI SISTEMA

Progressivo	Nome	Cognome	Matricola	UO/Struttura	Data Inizio	Ambiti	Data Fine	Motivazione di fine nomina	Riferimento lettera di incarico (protocollo)	Riferimento atto di nomina (protocollo)	Note

ATTESTAZIONE SUGLI ADEMPIMENTI PREVISTI DAL REGOLAMENTO UE 2016/679

Il/La sottoscritto/a .....in qualità di autonomo Titolare del trattamento dei dati personali, con riguardo al conferimento incarico di .....

PRESO ATTO

che le attività necessarie per l'espletamento dell'incarico comportano il trattamento di dati personali, nel caso anche appartenenti a categorie particolari (ex sensibili) e giudiziari, ai sensi degli artt. 6, 9 e 10 del Regolamento 2016/679, di cui l'ASL Avezzano-Sulmona-L'Aquila è Titolare;

SI IMPEGNA

al pieno rispetto della vigente disciplina in materia di protezione dei dati personali, garantendo l'osservanza del Regolamento Generale sulla protezione dei dati personali e del D.lgs 196/03, così come modificato dal D.lgs 101/18 ed in particolare:

a) Assicurerà che il trattamento dei dati avverrà solo ed esclusivamente in esecuzione del mandato conferitomi, nel più scrupoloso rispetto delle norme dettate dal D.lgs. 196/03 e s.m.i. con particolare riguardo alla riservatezza dei dati raccolti;
b) Predisporrà, nello svolgimento dell'incarico, tutte le misure di sicurezza (fisiche, logiche ed organizzative) di cui all'art. 32 del Regolamento UE 2016/679, idonee a garantire l'integrità e la riservatezza dei dati personali;
c) Provvederà ad adottare e garantire adeguate misure di sicurezza su dispositivi elettronici utilizzati per il trattamento dei dati di cui è titolare l'ASL Avezzano-Sulmona-L'Aquila, tra cui un idoneo sistema di autenticazione, autorizzazione e protezione da virus;
d) Assumerà l'obbligo di non comunicare, non divulgare e non utilizzare per altri fini, i dati e le informazioni di cui venga in possesso in ragione del conferimento dell'incarico;
e) Manterrà i dati personali in proprio archivio esclusivamente per il periodo di durata del conferimento dell'incarico e, successivamente, per obblighi di conservazione previsti da norme di legge o regolamento;
f) Garantirà l'esercizio dei diritti degli interessati, di cui agli artt. 15-22 del Regolamento UE 2016/679;

g) Segnalerà tempestivamente eventuali violazioni di dati (*data-breach*) al Titolare del trattamento e al suo Responsabile della protezione dei dati, per i conseguenti adempimenti.

Il Professionista incaricato in qualità di autonomo Titolare del trattamento

Data.....firma.....

Il Titolare del trattamento dei dati personali

Data.....firma.....

(per l'ASL Avezzano-Sulmona-L'Aquila)

Progressivo	Soggetto Esterno	Tipologia rapporto (CONTITOLARE/TITOLARE AUTONOMO)	Servizi	Data Inizio	Data Fine	Motivazione di fine accordo	Riferimento protocollo Contratto/Convenzione	Riferimento protocollo Designazione	Note

1706

ALLEGATO 13 PRY-MOD 014
REGISTRO PER CONTITOLARI E TITOLARI AUTONOMI

Allegato G

al Regolamento Aziendale per la protezione dei dati personali della ASL 01 Abruzzo

Clausola di Garanzia da inserire nei contratti con Terzi

Art. xx Responsabilità del trattamento dei dati personali

Per la corretta esecuzione dei Servizi/Prestazioni professionali oggetto del presente accordo/contratto/convenzione, [il FORNITORE] tratterà dati personali ed eventualmente particolari (sensibili) di persone fisiche la cui titolarità è in capo all'ASL Avezzano-Sulmona-L'Aquila, pertanto, in adempimento a quanto previsto dalla normativa vigente, alla data della stipula del citato contratto e per la durata dello stesso, si specifica che l'ASL Avezzano-Sulmona-L'Aquila è "Titolare del trattamento" dei dati sopra citati, mentre [il FORNITORE] sarà designato, ove applicabile, ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati personali (Reg. UE 679/2016), quale "RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI", tramite sottoscrizione dell'Accordo predisposto dal Titolare del trattamento (Accordo sulla protezione dei dati - APD) contestuale alla stipula del contratto (nomina i cui contenuti costituiranno parte integrante del contratto). In ragione di quanto sopra [il FORNITORE], in esecuzione dei servizi/prestazioni professionali previste nell' accordo, si impegna a:

- procedere al trattamento dei dati personali, nel pieno rispetto della vigente disciplina rilevante in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall' Autorità Garante per la Protezione dei Dati Personali, attenendosi ai principi di cui al capo II del nuovo Regolamento (UE) 2016/679;
- trattare 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;
- soddisfare quanto previsto e specificato nella nomina a RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI e nelle relative istruzioni.

Azienda Sanitaria Locale
Avezzano, Sulmona, L'Aquila

REGIONE ABRUZZO – ASL 1 AVEZZANO SULMONA L'AQUILA

Elenco Documenti

Data 31/10/2019

CODIFICA	TITOLO DOCUMENTO	REV	DATA
PRY-DOC-001	Regolamento Aziendale per la Protezione dei Dati Personali	1.3	31/10/2019
PRY-REG-001 (1/14)	Registro delle Attività di Trattamento	1.2	31/10/2019
PRY-DOC-002	Piano di Sicurezza	1.1	31/10/2019
PRY-PRD-001	**Procedura per la gestione delle Violazioni di Dati Personali**	**1.3**	**31/10/2019**
PRY-MOD-002	Allegato 1 – Modulo per la segnalazione Interna della Violazione	1.1	31/10/2019
PRY-MOD-003	Allegato 2 - Registro Segnalazioni delle Violazioni	1.0	31/10/2019
PRY-MOD-004	Allegato 3 - Documentazione Interna della Violazione	1.1	31/10/2019
PRY-MOD-005	Allegato 4 - Modello notifica Data Breach	1.0	31/10/2019
PRY-MOD-006	Allegato 5 - Segnalazione della Violazione da parte dell'Interessato	1.0	31/10/2019
PRY-PRD-002	**Procedura per l'esercizio dei diritti degli interessati**	**1.2**	**31/10/2019**
PRY-MOD-001	Allegato 1– Modello Esercizio Diritti dell'Interessato	1.0	31/10/2019
PRY-MOD-015	Allegato 2 – Modello di Reclamo al Garante	1.0	31/10/2019
PRY-MOD-016	Allegato 3 – Modello di Registro per l'esercizio dei Diritti degli Interessati	1.0	31/10/2019
PRY-PRD-003	**Procedura per la Gestione delle Informative e Consensi**	**1.2**	**31/10/2019**
PRY-INF-001	Allegato 1 – Informativa generale (I livello)	1.2	10/10/2019
PRY-MOD-007	Allegato 2 – Template Informativa Specialistica (II livello)	1.0	31/10/2019
PRY-MOD-008	Allegato 3 – Template Modulo Consenso	1.0	31/10/2019
PRY-PRD-004	**Procedura per la Gestione di Accordi, Nomine e Designazioni**	**1.2**	**31/10/2019**
PRY-SATD-001	Allegato 1 – Modulo di nomina per Soggetto Autorizzato al Trattamento dei dati con Delega (SATD)	1.4	31/10/2019
PRY-MOD-010	Allegato 2 – Modello di Registro di Soggetti Autorizzati al Trattamento con Delega (SATD)	1.0	31/10/2019
PRY-SAT-001	Allegato 3 --Modulo di nomina per Soggetto Autorizzato al Trattamento dei dati (SAT)	1.2	31/10/2019
PRY-MOD-011	Allegato 4 –Modello di Registro di Soggetti Autorizzati al Trattamento	1.0	31/10/2019
PRY-RT-001	Allegato 5 –Modulo di designazione per Responsabile del Trattamento (Caso 1 – Professionisti) da parte del Titolare	1.3	31/10/2019
PRY-RT-002	Allegato 6 –Modulo di designazione per Responsabile del Trattamento (Caso 1 – Professionisti) da parte del SATD	1.3	31/10/2019
PRY-RT-003	Allegato 7 –Modulo di designazione per Responsabile del Trattamento (Caso 2 – Aziende/Organizzazioni) da parte del Titolare	1.5	31/10/2019
PRY-RT-004	Allegato 8 –Modulo di designazione per Responsabile del Trattamento (Caso 2 – Aziende/Organizzazioni) da parte del SATD	1.5	31/10/2019
PRY-MOD-012	Allegato 9 –Modello di Registro per Responsabili del Trattamento	1.0	31/10/2019
PRY-ADS-001	Allegato 10 –Modulo di nomina per Amministratori di Sistema (AdS)	1.1	31/10/2019
PRY-MOD-013	Allegato 11 –Modello di Registro per Amministratori di Sistema	1.0	31/10/2019
PRY-TA-001	Allegato 12 –Modulo di impegno da parte del Titolare Autonomo	1.0	31/10/2019
PRY-MOD-014	Allegato 13 –Modello di Registro per Contitolari e Titolari Autonomi	1.0	31/10/2019
PRY-MOD -017	**Clausola di Garanzia da inserire nei contratti con terzi**	**1.3**	**31/10/2019**