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

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 e/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