Regolamento aziendale in materia di protezione dei dati personali attuativo del Regolamento UE 2016/679 e del Decreto Legislativo n. 101/2018.

IL CONSIGLIO DI AMMINISTRAZIONE
DEL CENTRO DI RIABILITAZIONE VACLAV VOJTA SOCIETÀ COOPERATIVA

Visto

- il Regolamento (UE) 2016/679 del Parlamento Europeo e dl Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), entrato in vigore il 25 maggio 2018;

- il Decreto Legislativo n. 101 del 10 agosto 2018, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), entrato il vigore il 19 settembre 2018;

Ravvisata

la necessità di fornire al Centro di Riabilitazione Vaclav Vojta, in applicazione del principio di accountability (che prevede la responsabilizzazione in capo al Titolare del trattamento circa gli adempimenti in materia di protezione dei dati personali), un valido strumento di lavoro finalizzato a garantire l'applicazione della normativa sopra richiamata;

Delibera

1. di adottare il "Regolamento aziendale privacy ai sensi del Regolamento UE 2016/679 e del Codice in materia di protezione dei dati personali come modificato dal D.lgs. n. 101/2018. che si allega (di seguito "Regolamento Aziendale Privacy");
2. di rassegnare copia del presente Regolamento a tutte le Unità Riabilitative, Dipartimenti e Uffici del Centro Vojta;

Roma, 14/11/2018

Il Responsabile per la Protezione dei dati Personali _____

Il Referente Aziendale Privacy
Dott.ssa Stefania Cruciani

Il Presidente
Dott. Carlo Marotta

REGOLAMENTO AZIENDALE PRIVACY AI SENSI DEL REGOLAMENTO UE 2016/679 E DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI COME MODIFICATO DAL D.LGS N. 101/2018.

INDICE

Allegati

Articolo 1 – OGGETTO

1. Il presente Regolamento contiene disposizioni attuative del D.lgs. n. 196/2003 ("Codice in materia di protezione dei dati personali") e s.m.i., di seguito "Codice" – per la parte ancora in vigore a seguito del Decreto Legislativo n. 101/2018 – e del Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "GDPR") nell'ambito delle strutture del Centro di Riabilitazione Vaclav Vojta (di seguito: Centro Vojta o Azienda), con lo scopo 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 il Centro Vojta.
2. Il Centro Vojta adotta in materia di sicurezza, 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.
3. 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 GDPR.

Articolo 2 – DATI PERSONALI

Ai sensi dell'art. 4 GDPR si riportano le seguenti definizioni:

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta. la registrazione, l'organizzazione. la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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

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

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

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri

determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

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

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

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

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

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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

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

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

«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;

«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 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a nonna del presente regolamento;

«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;

«gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

«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;

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

«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;

«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;

«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;

«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;
«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.

Articolo 3 – TRATTAMENTO DEI 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. È possibile effettuare trattamenti relativi a dati diversi da quelli sensibili e giudiziari anche in mancanza di una norma di legge o di Regolamento che lo preveda espressamente, fermo restando l'esercizio di funzioni istituzionali.
3. Il trattamento di dati sensibili è invece consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
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. Il trattamento dei dati personali è comunque effettuato dal Centro Vojta nel rispetto dei principi previsti dal GDPR agli articoli 5 e 6, nonché in ambito sanitario, per le finalità connesse alla tutela della salute dell'interessato, di terzi o della collettività.
7. I trattamenti effettuati dall'Azienda, concernenti i dati personali degli utenti, sono finalizzati prevalentemente all'erogazione delle prestazioni sanitarie, nonché all'espletamento dei compiti riconosciuti nell'ambito regionale ed agli adempimenti amministrativi e contabili di organizzazione e di controllo preordinati alla predetta erogazione, con particolare riguardo alle seguenti Unità di Riabilitazione:
   a) Unità di Riabilitazione Adulti e dimorfismi
   b) Unità di Riabilitazione dell'Età Evolutiva
   c) Unità di Riabilitazione SemiResidenziale
   d) Unità di Riabilitazione Vascolare/Oncologica

Sono altresì effettuati nell'ambito dell'Azienda i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti:

a) la gestione del personale dipendente, ivi comprese le procedure di assunzione;
b) la gestione dei soggetti che intrattengono rapporti giuridici con l'Azienda, 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;
c) la gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni e servizi (anche di natura informatica e clinica), nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;

d) la gestione dei rapporti con i soggetti accreditati o convenzionati, associazioni anche di volontariato ed altri Enti ed Organismi Pubblici;

e) 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.

Articolo 4 - 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 statutarie del Centro Vojta.

3. I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati.

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.

5. È compito delle persone fisiche autorizzate al trattamento dei dati personali con delega ("SATD"), ai sensi dell'art. 28 GDPR, verificare periodicamente la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisca di propria iniziativa.

6. I dati che, anche a seguito di verifiche, risultassero eccedenti, non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a nonna di legge, dell'atto che li contiene.

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 GDPR, i dati personali appartenenti a determinate categorie sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

9. In ogni caso devono essere adottate misure tecniche tali da garantire che i dati personali siano accessibili alle sole persone fisiche autorizzate al trattamento dei dati personali ("SAT") e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

Articolo 5 - 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 GDPR 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;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Articolo 6 - COMUNICAZIONE DEI DATI

1. La comunicazione di dati personali da parte dell'Azienda a soggetti pubblici è ammessa solo quando sia prevista da una norma di legge o di Regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali del Centro Vojta 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.
2. La comunicazione da parte dell'Azienda di dati personali a privati e la diffusione sono ammesse unicamente quando siano previste da una norma di legge o di regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.
3. I dati idonei a rivelare lo stato di salute non possono essere diffusi.
4. 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.
5. 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.
6. 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.

Articolo 7 - INFORMAZIONI ALL'INTERESSATO

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 dovuta a prescindere dall'obbligo di acquisizione del consenso. Essa deve contenere gli elementi tassativamente indicati dagli artt. 13e 14 GDPR 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 Incaricati e l'ambito di diffusione dei dati medesimi;
   e) i diritti di cui all'art. 17 del presente Regolamento;

f) gli estremi identificativi del Titolare e del Responsabile al trattamento.

3. Le predette informazioni all'interessato possono essere rese anche tramite affissione di appositi manifesti nei locali di accesso all'utenza, secondo procedure e attraverso modelli concordati con il Referente Aziendale Privacy ("RAP"), e loro pubblicazione sul sito aziendale www.centrovojta.com all'interno della sezione Privacy).
4. Ai sensi dell'art. 13 GDPR, 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 (di seguito anche "RPD/DPO");
   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) GDPR, 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 GDPR.
5. Qualora i dati personali non siano stati ottenuti presso l'interessato, 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) GDPR, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
   f) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4 GDPR, 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. Nella Sezione Allegati, in calce al presente Regolamento sono inserite le informative ed i Consensi al trattamento dei dati personali elaborate dal Centro Vojta (che potranno essere aggiornati).

Articolo 8 - REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

1. L'Azienda redige, conserva ed aggiorna il Registro dei trattamenti che contiene 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:
   a) Condizioni di Liceità, ai sensi dell'art. 6 par. 1 GDPR;
   b) la Base Giuridica;
   c) la Verifica della compatibilità dell'ulteriore Finalità (art. 6 par. 4);
   d) la descrizione Estesa del Trattamento.
2. È tenuto a cura del Referente Aziendale Privacy ("RAP") in collaborazione con i Soggetti Autorizzati al Trattamento dei Dati Personali con Delega ("SATD") che dovranno comunicare l'elenco dei trattamenti effettuati nell'ambito della propria struttura/unità operativa. Esso viene aggiornato periodicamente o qualora vengano comunicati da parte dei SATD casi di attivazione di un nuovo trattamento – che deve, comunque, essere preventivamente autorizzato dal RAP – o cessazione di un trattamento in essere. Il RPD/DPO si occuperà di verificare la corretta tenuta del Registro dei trattamenti.

Articolo 9 – IL TITOLARE DELTRATTAMENTO DEI DATI PERSONALI

1. Ai sensi del GDPR, il Titolare del trattamento è il Centro di Riabilitazione Vaclav Vojta Società Cooperativa, con sede in via via Salvatore Pincherle, 186 – 00146 Roma 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: PEC: centrovojta@pec.centrovojta.com Email: RPD@centrovojta.com;
2. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti posti in essere sono conformi al GDPR;
3. Il Titolare, avvalendosi della supervisione e collaborazione del RPD/DPO aziendale, 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 obbligo di notificazione e comunicazione;
   b) a nominare il RAP determinandone le relative funzioni aziendali, tra cui il potere di nominare con successivo atto i 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 dall'art. 12 GDPR, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
   c) ad individuare e nominare il RPD/DPO;
   d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
   e) 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.

4. I Responsabili sono nominati sia dal Titolare che dal RAP, il quale potrà esercitare le prerogative concesse al Titolare nei confronti dei Responsabili e dei Sub-Responsabili ai sensi degli artt. 11 e 12; colui che predispone la nomina ne cura la conservazione degli originali. Copia della lettera di nomina munita di firma per accettazione del Responsabile va trasmessa comunque al RPD/DPO (al seguente indirizzo: RPD@centrovojta.com) che detiene ed aggiorna il relativo elenco e lo trasmette, in copia, ogni semestre al Titolare.

Articolo 10 – REFERENTE AZIENDALE PRIVACY (RAP)

1. L'Azienda individua al proprio interno un Referente Aziendale Privacy che assolva le funzioni di responsabile interno aziendale, garantendogli le risorse umane e strumentali necessarie per l'efficace ed ottimale assolvimento dei compiti assegnati.
2. Il Referente Aziendale Privacy viene nominato con atto del Consiglio di Amministrazione, ed individuato generalmente nel Direttore Sanitario dell'Azienda o tra le risorse del ruolo amministrativo (scelto 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. Il Referente Aziendale Privacy svolge i seguenti compiti:

a) Nomina i SATD e i SAT;

b) Nomina, di concerto con il Titolare, i Responsabili;

c) Monitora periodicamente l'accesso e il trattamento dei dati da parte di SATD e SAT;

d) garantisce al Titolare e al RPD/DPO il necessario supporto per lo svolgimento dei compiti a lui assegnati;

e) coadiuva il Titolare e il RPD/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

f) concorre a promuovere l'osservanza del Regolamento aziendale sulla privacy fornendo la necessaria consulenza in ordine alle problematiche in tema di protezione dei dati;

g) mantiene in modo corretto la produzione normativa interna in materia di trattamento dati;

h) su richiesta del RPD/DPO propone, svolge e/o coordina l'attività di formazione in tema di normativa sulla riservatezza dei dati, assicurando la promozione della cultura della privacy a livello aziendale;

i)provvede all'adeguamento dei percorsi e delle procedure aziendali per quanto attiene l'aspetto della riservatezza dei dati;

j) si occupa – unitamente ai dipartimenti aziendali preposta all'amministrazione dei conflitti tra diritto alla riservatezza dei dati e dovere di garantire la trasparenza dell'attività amministrativa e di good governance;

k) collabora con il RPD/DPO e con il Titolare nella gestione delle istanze dell'interessato e delle controversie sui dati personali e, più in generale, in tema di riservatezza, avanzate dall'interessato al Titolare del trattamento di cui all'art. 23 del presente Regolamento Aziendale Privacy;

l) si occupa della redazione e tenuta del Registro dei Trattamenti;

m) verifica periodicamente che l'attuazione delle misure tecniche e organizzative del Centro Vojta garantiscano un livello di sicurezza dei dati adeguato e conforme a quanto

previsto dal GDPR e, in particolare, fornisca sufficienti garanzie per la protezione dei dati personali dei Terzi Interessati.

4. Nell'esercizio delle competenze di cui ai punti precedenti deve essere garantito al Referente Aziendale Privacy l'apporto di tutte le articolazioni organizzative dell'Azienda, in aggiunta ad eventuali servizi specialistici di consulenza.

16. Qualora il RAP intendesse apportare modifiche alle misure tecniche e organizzative del Centro Vojta, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione al Titolare.

17. Per l'esecuzione di specifiche attività per conto del Titolare, il RAP potrà avvalersi – previa richiesta di autorizzazione rivolta al Titolare e formale assenso di questi – di Responsabili del trattamento esterni all'organizzazione del Titolare – Centro Vojta – ai sensi del GDPR. I Responsabili del, Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al RAP ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il RAP nominerà Responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nella lettera di nomina del RAP, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento. Qualora il Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il RAP conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi attribuiti al Responsabile.

18. Il RAP procedente ha l'obbligo, anche avvalendosi della consulenza del RPD/DPO, di predisporre lo schema dell'atto di nomina a Responsabile del trattamento, ed allegarlo quale parte integrante e sostanziale al provvedimento/accordo relativo all'affidamento dell'attività/servizio, integrando l'eventuale modello predisposto dalla Azienda (v. allegato), in relazione allo specifico trattamento di dati effettuato dai singoli Responsabili.

19. Il RAP, ove competente per la stipula e la conservazione dei contratti e in ogni caso negli ambiti della propria competenza funzionale, effettua una costante ricognizione dei contratti del Centro Vojta in essere, al fine di provvedere:

a) agli adempimenti di legge in materia di trattamento dei dati personali;

b) alla richiesta rivolta al Titolare del trattamento affinché lo autorizzi alla nomina a Responsabile del soggetto cui sia affidata l'attività o il servizio;

c) all'inserimento nei contratti medesimi di clausole di garanzia;

20. Il nominativo del singolo Responsabile del Trattamento che il RAP intenda designare per l'esecuzione di attività di trattamento dei dati, riguardanti le attività istituzionali svolte dalle Unità Riabilitative dal lui/lei dirette, dovrà essere previamente comunicato al Titolare per la necessaria autorizzazione scritta.

21. Il RAP si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (e-mail ordinaria e/o PEC), laddove il Responsabile (da lui designato) intenda, per l'erogazione dei servizi e/o delle forniture, avvalersi e, di conseguenza, nominare, sostituire o cessare il rapporto con un Sub-Responsabile del Trattamento. La nomina, sostituzione o cessazione si intenderà accettata dal Titolare esclusivamente a seguito di formale positivo riscontro.

22. Qualora il Titolare sollevi obiezioni su uno o più Responsabili o Sub-Responsabili del Trattamento, egli darà indicazioni al RAP sulle relative motivazioni. In tal caso, il RAP potrà:

a. proporre altro Sub-Responsabile del Trattamento in sostituzione del Sub-Responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni;

b. adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).

23. Il RAP è responsabile di verificare il puntuale assolvimento da parte dei SATD e SAT, nonché dei Responsabile/i e del/i Sub-responsabile/i del Trattamento degli adempimenti previsti dal GDPR.

24. Nel caso in cui il RAP abbia necessità di ricorrere a un Responsabile o un Sub-Responsabile del Trattamento situato in un Paese terzo (extra UE), egli 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 RAP 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.

25. Tenendo conto della natura del trattamento dei dati personali svolto dal RAP, come descritto nel Registro dei Trattamenti, questi si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, al fine di adempiere al proprio obbligo di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli artt. da 12 a 22 GDPR.

26. Il RAP dovrà informare il Titolare, senza ingiustificato ritardo, laddove un Terzo Interessato eserciti uno dei diritti di cui agli artt. da 12 a 22 del GDPR, con particolare riferimento a, a titolo esemplificativo e ove applicabile, il diritto di accesso ai dati personali, il diritto di chiedere la rettifica e cancellazione (c.d. "diritto all'oblio") dei dati personali, il diritto di limitare il trattamento dei dati personali o di opporvisi il diritto alla "portabilità" dei dati personali, il diritto di opporsi a una decisione basata unicamente sul trattamento automatizzato ai sensi dell'art. 22 GDPR.

27. Tenendo conto della natura del trattamento come descritto nel Registro dei Trattamenti, nella lettera di nomina del RAP e delle informazioni di volta in volta messe a disposizione, il RAP si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 GDPR.

28. I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del RAP, 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.

29. Il RAP 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.

30. Il RAP dovrà consentire al Titolare di eseguire verifiche su tali informazioni e ispezioni (congiuntamente "Audit"), 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. Il Titolare darà comunicazione al RAP della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

31. Il Titolare potrà successivamente fornire al RAP una relazione scritta di natura

confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

32. Il RAP si fa carico di assicurare la dovuta formazione del personale da lui diretto e/o autorizzato diretto al trattamento dei dati personali in materia di trattamento dei dati.

Articolo 11 - RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD/DPO)

1. Il RPD/DPO provvede, ai sensi dell'art. 39 GDPR, a:

a) informare e fornire consulenza al titolare del trattamento, al RAP, ai SATD e ai SAT 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 GDPR, 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 GDPR;

d) cooperare con l'autorità di controllo;

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 GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il RPD/DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Articolo 12 – RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

1. Ai sensi dell'art. 28 GDPR, qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Suddetti Responsabili sono riconducibili alla categoria dei fornitori di beni e/o servizi per conto del Titolare del trattamento.

3. Il Responsabile tratta i dati personali nella misura necessaria a fornire i servizi di cui al contratto, alla convenzione, ai provvedimenti di nomina/aggiudicazione e agli altri accordi e norme che definiscono e regolano il rapporto con il Titolare (di seguito "Documenti"). I servizi che possono essere svolti dal Responsabile sono indicati nei documenti sopra richiamati ed, eventualmente, in altri documenti prodotti dal Titolare.

4. La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata indicata nei Documenti.

5. I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi dell'atto di nomina possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Centro Vojta, terzi incaricati, a qualunque titolo, dal Centro Vojta, pazienti, controparti contrattuali del Centro Vojta e, in generale, terze parti rispetto alle quali il Centro Vojta 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.

6. Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Centro Vojta in forma scritta: il dettaglio delle operazioni consentite è indicato nel relativo atto di nomina e/o nei Documenti. In particolare, l'atto di nomina e/o i Documenti costituiscono parte delle istruzioni del Centro Vojta 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.
7. Il Responsabile garantisce 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.
8. Il Responsabile si impegna ad adottare le misure richieste dall'art. 32 GDPR.
9. 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 si impegna a mettere in atto le misure tecniche e organizzative indicate nell'atto di nomina e/o nei Documenti di cui si richiede la compilazione per la descrizione delle modalità di implementazione. Il Responsabile si impegna a comunicare le indicazioni applicabili ai prodotti e/o servizi fomiti secondo quanto previsto dall'atto di nomina (tale obbligo vige solo per i Responsabili fornitori di servizi tecnici/tecnologici o per specifici requisiti).
10. Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'atto di nomina e/o nei Documenti, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione al Centro Vojta, fermo restando che tali modifiche non potranno comportare l'approntamento dì un livello di protezione inferiore rispetto a quanto previsto nell'atto di nomina e/o nei Documenti.
11. Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nell'Atto di nomina e/o nei Documenti, il Responsabile si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli artt. da 12 a 23 del GDPR.
12. 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 12 a 23 del GDPR.
13. Tenendo conto della natura del trattamento, come descritto nell'Atto di nomina e/o nei Documenti, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del GDPR.
14. I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dal nell'atto di

nomina e/o nei Documenti, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione dei rapporti contrattuali, i dati oggetto di Trattamento da parte del Responsabile devono 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.

15. In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

16. Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, In modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

17. Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. t) GDPR, 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 GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 GDPR.

18. La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi centrovojta@pec.centrovojta.com e RPD@centrovojta.com.

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

20. Fatta salva la possibilità di nominare un Sub-Responsabile, ove previsto nell'atto di nomina e/o nei Documenti, il Responsabile garantisce 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.

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

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

23. Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con Io scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

24. Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit (Verifica) comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

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

26. Il Responsabile, ove richiesto dal Centro Vojta, si impegna altresì a:

a) effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti} ed alle conseguenti risultanze;
b) collaborare con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
c) realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
d) informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dal Centro Vojta e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

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

30. La designazione a Responsabile non comporta 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 degli accordi stipulati con il Centro Vojta.

Articolo 13 – SUB-RESPONSABILI DEL TRATTAMENTO

1. Per l'esecuzione di specifiche attività per conto del Centro Vojta, ove previsto dall'atto di nomina e/o dai Documenti, il Responsabile potrà avvalersi di sub-responsabili del trattamento ai sensi del GDPR. I Sub-Responsabili del Trattamento

sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati fomiti al Responsabile ed è fotto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-Responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norna del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente Regolamento Aziendale Privacy, nell'atto di nomina e nei Documenti vincolanti 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 GDPR. Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile.

2. 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 all'atto di nomina e/o ai Documenti dovrà essere previamente fornito al Centro Vojta per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco.

3. Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 9 del presente Regolamento Aziendale Privacy), laddove intenda: includere un nuovo Sub-Responsabile del Trattamento nell'elenco, 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 3 (tre) mesi dalla ricezione della comunicazione da parte del Responsabile.

4. Qualora il Titolare sollevi obiezioni su uno o più Sub-Responsabili del Trattamento, il Titolare 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 Centro Vojta abbia sollevato obiezioni; oppure adottare misure tese a superare le obiezioni del Centro Vojta (qualora le obiezioni fossero superabili).

5. Il Responsabile è responsabile nei confronti del Centro Vojta per l'adempimento del Sub-Responsabile del Trattamento ai propri obblighi.

6. 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 dame preventiva comunicazione al Centro Vojta per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

Articolo 14 – AMMINISTRATORI DI SISTEMA DEI RESPONSABILI

1. Il Responsabile si impegna a conformarsi al Provvedimento generale del Garante

per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

2. In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Responsabile eserciti attività di Amministrazione di Sistema, il Responsabile si impegna a:
   a) designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
   b) effettuare un'elencazione analitica degli ambiti di operatività consentili a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
   c) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
   d) comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
   e) verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
   f) mantenere i file di login conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
   g) garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

Articolo 15 – SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI CON DELEGA (SATD)

1. Il RAP 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, nel presente Regolamento Aziendale Privacy e nella normativa di settore in tema di riservatezza; in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate in tema di sicurezza dei dati personali dall'Azienda.
2. Possono essere nominati SATD i direttori/dirigenti e i Medici Responsabili di Unità e, ove ritenuto dal RAP necessario, di concerto con il Titolare, altri soggetti nell'organigramma aziendale 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 Aziendale Privacy e garantisca la tutela dei diritti dell'interessato.
3. Il SATD deve essere designato per iscritto dal RAP mediante atto formale e i compiti a lui affidati devono essere analiticamente specificati nell'atto di nomina e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati disposte dal Titolare, ove ritenuto

necessario da parte di quest'ultimo.

4. Il SATD, nell'espletamento della sua funzione, è sottoposto alle direttive del RAP e deve collaborare con il RPD/DPO al fine di:

a) comunicare al DPO ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 GDPR riguardanti: l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante Privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione ciel Registro dei trattamenti.

b) utilizzare – per competenza – il modello di Informativa e Consenso approvato per tempo dal Titolare, verificandone il rispetto e fornendo al RAP le informazioni utili per l'aggiornamento del Registro dei trattamenti;

c) coadiuvare il RAP e il Titolare nel rispondere alle istanze degli interessati e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

d) contribuire a far si 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;

e) informare il RAP e 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. Il SATD coadiuva il RAP e, se delegato lo fa personalmente, nella nomina delle persone fisiche autorizzate al trattamento dei dati personali ("SAT").

6. Il SATD tratta i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte dall'Unità Riabilitativa da lui/lei diretta. Le attività di trattamento sono correlate allo svolgimento delle Sue funzioni così come previste nel relativo contratto di Lavoro.

7. Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto dalla Sua designazione deve essere fornita dal RAP o dal Titolare al SATD per iscritto e diviene efficace solo a seguito di ricezione e conferma da parte di quest'ultimo.

8. I soggetti i cui dati personali sono oggetto del trattamento da parte del SATD possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Centro Vojta, terzi incaricati, a qualunque titolo, dall'Azienda, pazienti, controparti contrattuali del Centro Vojta 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.

9. Il SATD si impegna ad adottare le misure richieste dall'art. 32 del GDPR, 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.

13. Nei contratti di fornitura di prodotti e servizi in corso di esecuzione, aventi ad oggetto il trattamento di dati personali, il SATD si impegna, con il supporto del RAP e delle altre strutture aziendali del Titolare, a verificare l'attuazione delle misure tecniche e organizzative previste, dando aggiornamenti tempestivi al RAP

sull'implementazione delle misure richieste al Responsabile in questione.

Articolo 16 – PERSONE FISICHE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI (SAT)

1. Ferma restando la possibilità di nomina per il Titolare, il RAP e/o la Persona Fisica Autorizzata al Trattamento dei Dati Personali con Delega (SATD), ove autorizzato dal RAP, nominano la Persona Fisica Autorizzata al Trattamento dei Dati Personali (SAT) tra le persone fisiche in servizio all'interno del Centro Vojta.
2. La Persona Autorizzata tratta i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte. Le attività di trattamento sono correlate allo svolgimento delle sue funzioni (Contratto di Lavoro).
3. Il trattamento dei dati personali deve 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 Centro Vojta, terzi incaricati, a qualunque titolo, dal Centro Vojta, pazienti, controparti contrattuali del Centro Vojta e, in generale, terze parti rispetto alle quali il Centro Vojta 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. La Persona Autorizzata effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal RAP e/o dal Soggetto autorizzato con delega in forma scritta. L'atto di nomina costituisce parte delle istruzioni del Centro Vojta per il trattamento dei dati personali da parte della Persona Autorizzata 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 RAP e/o dal SATD.
5. Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto dalla designazione deve essere fornita dal Centro Vojta al SAT per iscritto e diviene efficace solo a seguito di ricezione e conferma da parte della Persona Autorizzata.
6. Il SAT si impegna a mantenere la riservatezza dei dati trattati e si assoggetta a tale obbligo.
7. Il SAT si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.
8. 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.
9. I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del SAT, 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.
10. L'atto di nomina viene controfirmato dal SAT, per presa visione, ed è conservato agli atti dal RAP o dal SATD che formano e tengono aggiornato l'elenco del personale individuato quale SAT, aggiornandolo con cadenza annuale e, comunque, ogni qual volta si verifichi una variazione (quiescenza, trasferimento, altro) sono tenuti a comunicare tempestivamente gli aggiornamenti al Titolare, per il seguito di competenza.

11. Tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito del Centro Vojta, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima Azienda (quali consulenze, collaborazioni o borse di studio, devono essere designati da parte del Responsabile (Ente, Società, ecc.) tramite una lettera di nomina come Soggetti autorizzati al trattamento. Ci si riferisce, a titolo esemplificativo, al personale tirocinante o al personale volontario che opera temporaneamente all'interno del Centro Vojta in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato (es. Associazione di volontariato o Ente universitario) per Io svolgimento di tirocini formativi/ attività di volontariato a sostegno dei pazienti ricoverati nei reparti ospedalieri.

12. 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.

13. Nel caso dei SAT di cui al precedente punto 11, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

Articolo 17 – PERSONA FISICA ESTERNA ALL'AZIENDA 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, con o senza retribuzione, qualora in ragione della propria attività venga a conoscenza di dati personali trattati dall'Azienda 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.

2. In relazione alle finalità di cui al precedente comma, il RAP e il SATD dell'Unità Riabilitativa interessata, ove il personale presta la propria attività fornisce le necessarie informazioni e provvede per iscritto alla nomina a SAT.

3. L'atto di nomina viene controfirmato dal SAT ed è conservato agli atti dal RAP che forma e tiene aggiornato l'elenco del personale individuato quale SAT, ed è tenuto a comunicare gli aggiornamenti al Titolare, per il seguito di competenza.

Articolo 18 – SERVIZI DI AMMINISTRAZIONE DI SISTEMA IN OUTSOURCING

1. Nel caso in cui l'Azienda 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.

2. 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;

3. Ogni qualvolta l'Azienda intenda esternalizzare servizi di amministrazione di sistema l'atto di nomina a Responsabile di cui all'art 8 del presente Regolamento Aziendale Privacy deve essere integrato con l'esplicitazione delle puntuali prescrizioni di cui al precedente comma 2.

4. Per i servizi già esternalizzati, il RAP si attiva – avvalendosi di ciascun SATD per le banche dati di propria competenza – nei confronti del Responsabile provvedendo a integrare le istruzioni/indicazioni già impartite.

Articolo 19 – REFERENTE INFORMATICO AZIENDALE

1. Il Referente Informatico Aziendale svolge, nell'ambito aziendale, le seguenti funzioni;

a) di concerto con il RAP, il RPD/DPO e con gli uffici e dipartimenti aziendali competenti, elabora e mantiene aggiornato il Regolamento Interno Informatica Aziendale;
b) predispone direttamente linee guida e direttive volte a migliorare la sicurezza informatica afferente i trattamenti effettuati con strumenti elettronici;
c) provvede alla ricognizione delle banche dati informatiche presenti in Azienda con indicazione delle rispettive sedi e caratteristiche;
d) fornisce al RAP, al RPD/DPO e al Titolare la necessaria assistenza informatica e il supporto per tutti gli aspetti correlati alla sicurezza dei trattamenti effettuati con strumenti elettronici.

Articolo 20 – DIRITTI DELL'INTERESSATO

1. L'Azienda ha regolato la materia in oggetto attraverso la Delibera n. 978 del 20.09.2018, recante il seguente oggetto "Regolamento sull'esercizio dei Diritti in Materia di Protezione dei Dati Personali dell'interessato ai Sensi degli Artt. 12 – 22 del Regolamento Ue 679/2016", alla quale si rimanda.

Articolo 21 – RELAZIONE TRA PRIVACY E ACCESSO

1. L'accesso ai documenti amministrativi, contenenti dati personali di terzi, formati o detenuti dall'Azienda è disciplinato dalle disposizioni delle norme applicabili.

2. Nel caso di istanza di accesso riguardante documentazione contenente dati comuni o sensibili di terzi, in ossequio ai principi di pertinenza e non eccedenza sanciti dalla normativa di settore il RAP, di concerto con il Centro Vojta, metterà a disposizione del richiedente i soli dati realmente necessari a tutelare l'interesse da questi esplicitato nell'istanza di accesso.

3. Qualora l'istanza di accesso riguardi categorie particolari di dati personali (ai sensi dell'art. 9 GDPR) l'accesso è consentito nei limiti stabiliti dalla normativa di settore. Resta fermo in capo al RAP, di concerto con il Titolare, l'onere di consentire l'accesso ai soli dati pertinenti e non eccedenti le finalità dell'istanza di accesso.

4. In ogni caso in cui l'esame di un'istanza di accesso ai documenti amministrativi implica problematiche connesse alla tutela della riservatezza di terzi, il RAP si avvale della consulenza del RPD/DPO nella valutazione dell'istanza stessa, riferendone preventivamente al Titolare.

Articolo 22 - DIRITTO DI ACCESSO DELL'INTERESSATO

1. Ai sensi dell'art. 15 GDPR, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.
3. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 GDPR relative al trasferimento.
4. Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.
5. In caso di ulteriori copie richieste dall'interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
6. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.
7. Per altri aspetti relativi all'esercizio del diritto di accesso si rinvia, anche in via analogica e ove applicabile, alla normativa di settore in materia di "accesso documentale", di "accesso civico" e di "accesso generalizzato".

Articolo 23 – PUBBLICAZIONE/DIFFUSIONE DI DATI PERSONALI

1. La pubblicazione da parte dell'Azienda di documenti contenenti dati personali determina una diffusione degli stessi consentita unicamente alle condizioni richiamate dalla normativa di settore, in materia di trattamento dei dati personali.
2. Relativamente alla presenza di dati personali, alla luce dei principi di pertinenza e non eccedenza sanciti dalla normativa in materia di trattamento dei dati personali, il Titolare verifica che l'inclusione nel testo di dati personali sia realmente necessaria per le finalità proprie di ciascuna pubblicazione/diffusione; nel caso di categorie particolari di dati personali (ai sensi dell'art. 9 GDPR) la verifica attiene all'indispensabilità degli stessi rispetto alle finalità della pubblicazione/diffusione, fermo restando il divieto assoluto di diffusione dei dati sanitari e di ogni informazione anche indirettamente correlabile alle condizioni di salute degli interessati.
3. Nel caso in cui gli allegati dei provvedimenti del Titolare contengano dati sensibili che ne determinano la non pubblicazione, nel provvedimento deve essere evidenziato che l'allegato non viene pubblicato, rimanendo depositato agli atti presso l'Azienda, per

esigenze di tutela della riservatezza dei destinatari o di terzi. Sull'allegato viene apposta la dicitura "*Riservato ai sensi della vigente normativa in materia di protezione dei dati personali*".

Articolo 24- 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 i seguenti strumenti:
   a) predisposizione del Regolamento Interno Informatica Aziendale;
   b) sistematico raccordo del Referente Informatico, del RAP e del RPD/DPO per la definizione delle modalità di intervento informativo rivolte ai SATD, SAT e ai Responsabili del trattamento;
   c) sistematica verifica da parte del RAP e dei SATD, in collaborazione con il Referente Informatico Aziendale – che agiranno di concerto con gli altri dipartimenti e uffici aziendali – dell'applicazione delle misure di sicurezza individuate nel Piano Aziendale per la Sicurezza Informatica e nelle indicazioni/direttive ulteriormente impartite.
   d) Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1, GDPR), tenuto conto che la lista di cui al paragrafo 1 dell'art. 32 GDPR è una lista aperta e non esaustiva ("tra le altre, se del caso").

Articolo 25 – SICUREZZA DEGLI ARCHIVI CARTACEI

1. L'accesso agli archivi aziendali deve essere controllato e devono essere identificati e registrati i soggetti delle strutture ove gli archivi sono collocati che vi accedono dopo l'orario di chiusura.
2. La Responsabilità della conservazione e della sicurezza degli archivi contenenti dati personali spetta al RAP nel suo complesso e al SAPT della singola Unità Riabilitativa avente a oggetto i dati stessi, inclusa l'archiviazione, digitalizzazione e deposito della documentazione amministrativa e/o sanitaria.
3. Per quanto qui non previsto e attinente alla specifica conservazione delle cartelle cliniche e della documentazione sanitaria si rinvia alle norme di gestione della documentazione clinica.
4. Qualora per la gestione del servizio di archiviazione della documentazione l'Azienda si avvalga di un soggetto terzo mediante rapporto di natura convenzionale, si intendono richiamate le disposizioni contenute nel presente Regolamento Aziendale Privacy.

Articolo 26 – MISURE DI SICUREZZA INFORMATICHE

1. Il trattamento di dati personali a mezzo di strumenti elettronici è consentito ai SATD e 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 SATD/SAT associato a una parola chiave riservata conosciuta solamente dal medesimo;
   b) un dispositivo di autenticazione in possesso e uso esclusivo del SATD/SAT, eventualmente associato a un codice identificativo o a una parola chiave;
   c) una caratteristica biometrica del SATD/SAT, eventualmente associata a un codice identificativo o a una parola chiave.
3. Il RAP richiede all'amministratore di sistema l'attivazione della credenziale di autenticazione informatica per i SATD/SAT, specificando a quali dati e tipi di operazioni

ciascun SATD/SAT deve poter accedere in relazione ai propri compiti (c.d. profilo di autorizzazione). Periodicamente e comunque almeno annualmente il RAP verifica la sussistenza per la conservazione dei profili di autorizzazione, dandone formale comunicazione all'amministratore di sistema, al RPD/DPO e al Titolare.

4. Lo stesso codice per l'identificazione, quando tale misura venga adottata, non può essere assegnato ad altri SATD/SAT, neppure in tempi diversi.
5. Ove ricorrano le condizioni, il potere sostitutivo del RAP si esercita con le seguenti modalità:
   a) la funzione di custode delle copie delle credenziali di autenticazione è posta in capo al RAP, con facoltà di delega al SATD di riferimento o a propri collaboratori formalmente individuati;
   b) il RAP 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, previa redazione di un verbale, accede al computer del SATD/SAT e a conclusione delle operazioni necessarie provvede a immettere una nuova password provvisoria e a spegnere il computer;
   e) il RAP informa tempestivamente il SATD/SAT dell'effettuazione dell'intervento;
   f) il SATD/SAT ha l'obbligo di sostituire la precedente password.

Articolo 27 – VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

1. Ai sensi dell'art. 32.1 GDPR, 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 GDPR: dall'ammonimento del Titolare fino alla limitazione o al divieto di procedere al trattamento.

Articolo 28 – 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 personale 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 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 SATD/SAT da parte del RAD 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 Unità Riabilitativa, dipartimenti e uffici 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. Il RAP, i SATD e i SAT 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. Il RAP e 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 fornite 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. L'Azienda può 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.

Articolo 29 – FORMAZIONE/DIDATTICA

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.

Articolo 30 – USO DELLE APPARECCHIATURE DI VIDEO-SORVEGLIANZA

1. L'installazione di apparecchiature di video-sorveglianza è autorizzata dall'Azienda nel rispetto delle disposizioni vigenti, solo quando ciò sia strettamente indispensabile per l'esercizio delle attività assistenziali e/o didattiche, ovvero per la sicurezza delle persone e delle attrezzature (monitoraggio delle persone ricoverate, controllo di corridoi, sale di attesa, reparti o di altri locali, di spazi esterni, delle porte di accesso agli edifici) e non siano attuabili o sufficienti altre misure di sorveglianza.
2. In particolare, il trattamento dei dati personali con le apparecchiature di cui al comma 1 è effettuato nel rispetto della dignità e dell'immagine delle persone, delle nonne a tutela dei lavoratori e delle prescrizioni del Garante.
3. Il trattamento di dati personali attraverso sistemi di video sorveglianza è presidiato dal RAP e dal SATD della singola Unità Riabilitativa, che ne cura la istruttoria in tutte le sue fasi chiedendo un parere al RPD/DPO.
4. L'Azienda fornisce le istruzioni necessarie sulle modalità di trattamento dei dati raccolti con le apparecchiature di video-sorveglianza, sulle misure di sicurezza da osservare, nonché sull'informativa da fornire agli utenti, agli operatori e alle altre persone che a qualsiasi titolo accedono agli spazi sorvegliati, in relazione alle finalità e alla tipologia del sistema di sorveglianza.

Articolo 31 – NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

1. Il Centro Vojta, 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"). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Titolare.
2. Se la probabilità di tale 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 GDPR. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 GDPR.
3. Il Titolare del trattamento, sentito il RAP e il RPD/DPO, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Articolo 32 – RINVIO

1. Per quanto non previsto dal presente Regolamento trovano applicazione le seguenti disposizioni: Regolamento UE 2016/679; D. lgs 196/2003 "Codice in materia di protezione dei dati personali" cosi come modificato dal D.lgs. n. 101/2018; Provvedimenti del Garante.

Articolo 33 – VALORE DEGLI ALLEGATI

1. Gli allegati al Regolamento, data la loro caratteristica di essere strumenti di lavoro necessariamente saranno soggetti a continue modifiche e revisioni, che avverranno attraverso il ricorso a note a firma del Direttore Generale e saranno pubblicate sul sito aziendale alla voce Privacy, senza richiedere quindi la adozione di un nuovo atto deliberativo.