CENTRO CHIRONE

REGOLAMENTO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

sulla base del Regolamento Europeo 2016/679 e del D. Lgs. 196/2003 modificato dal D. Lgs. 101/2018

DATA ULTIMO AGGIORNAMENTO AGOSTO 2022

PARTE I: INTRODUZIONE

Premessa

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8): è un vero e proprio diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali.

Il presente Regolamento è stato predisposto per regolare, attraverso una serie di misure che compongono un vero e proprio "*Sistema Gestionale Privacy*", i compiti e le responsabilità di tutti coloro che trattano dati personali.
Il documento, che è stato elaborato tenendo conto dell'attuale quadro regolatorio, è uno strumento di applicazione del vigente D.lgs. 30 giugno 2003, n. 196 (cosiddetto "Codice in materia di protezione dei dati personali" come novellato dal recente D.lgs. 10 agosto 2018 n. 101) e, in particolare, del Regolamento Europeo n. 679/2016 (conosciuto come "GDPR"), nell'ambito dell'organizzazione del "Centro Polispecialistico Chirone" (di seguito Centro)

A far data dal 25 maggio 2018, sul territorio nazionale, ha trovato diretta e immediata applicazione il Regolamento Europeo n. 679/2016 del Parlamento Europeo e del Consiglio dell'Unione Europea, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 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).
Ciò ha comportato il superamento delle disposizioni legislative di cui al previgente Codice in materia di protezione dei dati personali, D.lgs. 196/2003 come successivamente modificato dal Legislatore italiano con il D. Lgs. 101 del 10 agosto 2018 di adeguamento al GDPR), così come delle norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, nella misura in cui le norme nazionali risultino contrastanti o incompatibili con quelle europee.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della *Accountability* che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche e organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della *Compliance*); vi è quindi l'obbligo di attuare comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE.
Nell'ottica del Legislatore europeo, quindi, in materia di Privacy ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci, in quanto risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto verso l'esterno.

PARTE II: DISPOSIZIONI GENERALI

Articolo 1: Oggetto del Regolamento

Il presente documento individua le politiche aziendali relative alla corretta gestione del trattamento dei dati personali, così come definiti dal **Regolamento UE 679/2016** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito *GDPR*), dal **Decreto Legislativo n. 196 del 2003** "Codice in materia di protezione dei dati personali" così come modificato dal **Decreto Legislativo n.101 del 2018** e dai Provvedimenti del Garante per la Protezione dei Dati, attraverso l'individuazione di una serie di misure nonché di compiti e di responsabilità di tutti coloro che trattano dati personali.
L'azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 15 del Regolamento UE 679/2016.

Articolo 2: Definizioni

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

a. **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;
b. **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 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;
c. **Limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
d. **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;
e. **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;
f. **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;
g. **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;

h. **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;
i. **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;
j. **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all' art. 37 del Regolamento europeo n.679/2016 dal Titolare o dal Responsabile del trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto, a livello interno, del già menzionato Regolamento;
k. **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;
l. **Designato**: la persona fisica cui il Titolare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, attribuisce specifici compiti e funzioni connessi al trattamento di dati personali;
m. **Autorizzato**: persone fisiche autorizzate a compiere operazioni di trattamento sotto la diretta autorità del Titolare e/o del Responsabile del trattamento e/o del Designato del trattamento;
n. **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. 101 del 2018 , 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;
o. **Diffusione**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
p. **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;
q. **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;
r. **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;
s. **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;
t. **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;
u. **Autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Articolo 3: Accountability e Sistema di Gestione Privacy

L'Azienda mette in atto tutte le misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità di trattamento in considerazione del possibile rischio di lesione dei diritti e delle libertà degli Interessati.
Tali misure sono riesaminate e aggiornate periodicamente e negli ulteriori casi in cui ciò si renda necessario, adottando politiche adeguate in materia di protezione dei dati.
Il sistema gestionale privacy aziendale include:

STRUTTURE:

- Gli Autorizzati
- L'Amministratore di sistema

DOCUMENTAZIONE:

- Registro delle Attività di Trattamento (RAT)
- Informative
- Atti di nomina a designati
- Atti di nomina a Responsabile del trattamento
- Modulo per l'esercizio dei diritti da parte dell'interessato.

PROCEDURE:

- Procedura *data breach* (violazioni dei dati personali);
- Sistema di formazione continua di tutti i soggetti coinvolti nelle attività di trattamento;
- Procedura di esercizio dei diritti degli Interessati.

Articolo 4: Categorie di Interessati e di dati personali trattati dal Centro

L 'Azienda tratta i dati personali relativi a:

- Pazienti/utenti;
- Personale in rapporto di dipendenza, convenzione o collaborazione;
- Clienti e fornitori.

I dati personali trattati comprendono anche le seguenti tipologie di dati "particolari":

- dati idonei a rivelare lo stato di salute.

Per effettuare il trattamento dei dati personali, il Centro utilizza sistemi manuali e automatizzati.
Il trattamento dei dati personali viene effettuato con il consenso dell'Interessato e soltanto previa erogazione di apposita informativa e adozione di apposite e adeguate misure di sicurezza.

Articolo 5: Principi applicabili al trattamento dei Dati

Il Centro, anche in considerazione dell'estrema delicatezza dei dati personali che correntemente tratta, adotta misure capaci di assicurare e documentare che il trattamento dei dati personali viene effettuato con modalità tali da preservarne l'integrità e la confidenzialità, nel rispetto delle adeguate misure di sicurezza.
Pertanto, lo stesso attiva le necessarie risorse organizzative, tecnologiche e finanziarie affinché il trattamento dei dati personali sia conforme alle disposizioni in materia di protezione dei dati e nell'osservanza dei seguenti principi:

- **liceità, correttezza e trasparenza**: trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **limitazione della finalità:** raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità;
- **minimizzazione dei dati**: debbano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esattezza**: siano esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- **limitazione della conservazione:** siano 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, salvo che vengano conservati per periodi più lunghi ai soli fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato;
- **integrità e riservatezza**: 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;
- **responsabilizzazione**: capacità di dimostrare che il trattamento dei dati viene svolto nel pieno rispetto della normativa vigente.

Articolo 6: Liceità del trattamento

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni (art.6 del Regolamento UE n. 679/2016):

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. Tale condizione non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Articolo 7: Finalità del trattamento

L'Azienda garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.
I trattamenti di dati personali effettuati sono finalizzati:

- all'erogazione di prestazioni sanitarie;
- alla tutela della sicurezza e della salute dei lavoratori e sorveglianza igienico-sanitaria delle strutture;
- alla tutela del proprio patrimonio aziendale;
- alla promozione dell'attività svolta dal centro.

Articolo 8: Trattamento di categorie particolari di dati personali

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino *l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Detta disposizione non si applica, secondo il Regolamento UE, quando ricorrono alcune condizioni, riportate al già menzionato articolo n. 9, tra le quali, ai fini delle attività istituzionali del Centro, si evidenzia:

a. l'interessato ha prestato il proprio consenso, esplicito ed informato, al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa opporsi al trattamento;
b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi del soggetto interessato;
c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
e. 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. il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;
g. 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. il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica a fini statistici.

PARTE III: DIRITTI DELL'INTERESSATO

Articolo 9: Informazioni sul trattamento dei dati

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 679/2016, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni:**

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b. i dati di contatto del Responsabile della protezione dei dati, ove applicabile;
c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) 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.

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

a. il *periodo di conservazione* dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'*accesso ai dati personali* e la *rettifica* o la *cancellazione* degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;
c. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) 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. 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'articolo 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.

Le informative di cui al presente articolo saranno rese accessibili all'interessato attraverso la modalità più confacente, cartacea o digitale (mediante affissione presso i locali aziendali o pubblicazione presso l'home page del sito del Centro)

Articolo 10: Diritto di accesso

Gli interessati possono contattare il Titolare del trattamento per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 679/2016, 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. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h. l'esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'accesso ai dati è garantito, all'Interessato, nei seguenti modi:

a. Direttamente anche per via telematica se disponibile;
b. Per il tramite del proprio medico di medicina generale;
c. Per delega o procura.

Articolo 11: Diritto di rettifica

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 679/2016, l'interessato ha il diritto di ottenere dal Titolare del trattamento la **rettifica dei dati personali inesatti** che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 12: Diritto alla cancellazione

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 679/2016, in capo all'interessato è riconosciuto il **diritto "all'oblio"**, che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti altrimenti trattati;
b. l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
c. l'interessato si oppone al trattamento in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano e non sussiste

alcun motivo legittimo prevalente per procedere al trattamento oppure qualora i dati personali siano trattati per finalità di marketing diretto;
d. i dati personali sono stati trattati illecitamente;
e. i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 del Regolamento UE.

Articolo 13: Diritto di opposizione

L'Interessato ha il diritto di opporsi (articolo 21 del Regolamento UE) in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'Azienda si astiene dal trattarli ulteriormente, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici l'Interessato ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

PARTE IV: TITOLARE DEL TRATTAMENTO E ALTRE FIGURE

Articolo 14: Titolare del Trattamento

Il **Titolare del trattamento dei dati personali** è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

L' Azienda, nella persona del Legale Rappresentante è il Titolare del trattamento (Controller) cui spetta la responsabilità del rispetto di tutti i princìpi previsti dal Regolamento europeo. Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Il rappresentante legale può delegare le relative funzioni ai soggetti Designati di cui all'*art.2-quaterdecies* del Codice Privacy.

Il Titolare, unitamente a quanto sopra e nei casi previsti dalla legge, provvede anche:

a. a cooperare, su richiesta, con l'Autorità Garante per la Privacy nell'esecuzione dei suoi compiti;
b. a nominare i *Responsabili del trattamento* (*Processor*) dei dati personali, impartendo ad essi, i compiti e le necessarie istruzioni, come da prospetto di incarico adottato dall' Azienda e che fa parte del sistema privacy aziendale;

Articolo 15: Personale autorizzato al trattamento dei dati personali

Il D.lgs. 196/2003, come novellato dal recente D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del GDPR stabilisce, al nuovo **articolo 2-quaterdecies, comma 2**, che il Titolare "*individui le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Gli Autorizzati del trattamento dei dati personali sono le persone fisiche che effettuano le operazioni di trattamento di dati personali, autorizzate e individuate a tale scopo dal Titolare del Trattamento. Sono da nominare come Autorizzati tutti i soggetti che a qualsiasi titolo prestino la loro opera, anche in via temporanea, all'interno del Centro.
Per la loro designazione è utilizzata apposita modulistica, che prevede la trascrizione della data di inizio ed eventuale fine dell'attività all'interno della struttura e indica i trattamenti di dati di cui sono autorizzati a svolgere le relative operazioni.

Gli Autorizzati ricevono un atto formale dal Titolare del Trattamento, che impartisce loro disposizioni sul corretto uso dei dati, in special modo sotto il profilo della sicurezza, e vengono informati sulle direttive vigenti sulla protezione dei dati da loro trattati. L'atto di designazione costituisce l'unico presupposto di liceità per il trattamento dei dati personali, dovrà essere controfirmato per accettazione dallo stesso Autorizzato.

Gli Autorizzati del trattamento dei dati personali:

a. trattano i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza;
b. qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata, ed è fatto loro assoluto divieto di cedere la propria password ad altri;
c. sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento e hanno l'obbligo di restituirli al termine delle operazioni affidate;
d. si impegnano ad avvalersi dei sistemi informatici aziendali, nonché di ogni altro strumento reso disponibile dal Titolare del trattamento, al fine di garantire un miglior adempimento della normativa di che trattasi e, parimenti, della normativa relativa alla conservazione digitale.

Articolo 16: Responsabile della protezione dei dati

Il Regolamento Europeo impone la nomina del ***Data Protection Officer*** (**DPO** in italiano: **Responsabile della protezione dei dati**), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.
La nomina del DPO è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come attività principali i dati particolari su larga scala, come ospedali, assicurazioni e istituti di credito.

L'art 37, all'uopo, prevede che: "Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

A seguito di specifica indagine istruttoria sull'attività posta in essere, il Centro ritiene non obbligatoria la nomina di un Responsabile della protezione dati DPO.
Il trattamento che il medesimo realizza, seppur coinvolga dati particolari, non presenta un'estensione tale considerarsi come "larga scala" e tale da integrare i requisiti di cui al considerando 91.
Purtuttavia, il Titolare si riserva di nominare la figura aziendale rappresentata nell'ipotesi in cui le circostanze analizzate alla data del presente regolamento dovessero essere tali da integrare il concetto di "larga scala".

Articolo 17: Amministratore di Sistema

L'Azienda nomina un amministratore di sistema preposto a compiti di vigilanza e controllo sul corretto utilizzo del sistema informatico gestito e utilizzato.

Lo stesso viene individuato tra i dipendenti aziendali e/o soggetti esterni previa valutazione dell'esperienza, capacità e affidabilità, in grado di fornire idonea garanzia del rispetto delle vigenti disposizioni in ambito di trattamento dei dati e di sicurezza.

L'individuazione è da ritenersi personale e avviene con apposito atto di nomina a Designato che deve contenere l'elencazione degli specifici compiti e istruzioni operative allo stesso impartite.

L'Amministratore di Sistema ha il compito di:

- assicurare l'adozione di idonee misure di sicurezza dei sistemi informativi dell'Azienda adeguate al tipo di trattamento posto in essere;
- rilasciare le credenziali iniziali agli Autorizzati del trattamento per l'accesso alle banche dati;
- organizzare il database e gestire i flussi di dati e di rete;
- vigilare affinché l'accesso alle banche dati sia consentito solo al personale autorizzato e limitatamente alle proprie mansioni;
- fornire supporto al Titolare e ai Responsabili del trattamento per l'individuazione, applicazione ed aggiornamento delle necessarie misure di sicurezza;
- gestire eventuali incidenti e violazioni dei dati personali (Data Breach) in ambito informatico;
- svolgere ogni altro compito previsto dalla legge o dai regolamenti.

Articolo 18: Registro delle attività di trattamento

Tutti i titolari e i Responsabili di trattamento, eccetto gli organismi con meno di 250 dipendenti ma solo nel caso in cui non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **Registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.
Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Centro provvede, inoltre, alla rilevazione dei trattamenti dei dati personali suddivisi per tipologia e per struttura organizzativa e ogni altro elemento necessario a individuare le responsabilità relative al loro trattamento.
Il Centro tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato, e contiene le seguenti informazioni:

a. il nome e i dati di contatto del titolare del trattamento;
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;
e. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento UE.

Il Registro è tenuto in forma scritta, anche in formato elettronico e, su richiesta, viene messo a disposizione dell'Autorità Garante Privacy.

Articolo 19: Formazione degli Autorizzati del trattamento ed Amministratori di sistema

L'Azienda, nel rispetto dell'art.32 del GDPR "Sicurezza del trattamento" paragrafo 4 prevede che il titolare e il Responsabile del trattamento fanno sì che *chiunque agisca sotto la propria autorità e abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento.*

Il Centro prevede iniziative atte ad assicurare la formazione e il continuo aggiornamento di tutti gli Autorizzati al trattamento sui temi della protezione dei dati personali e sui diritti, doveri e adempimenti previsti dalla normativa vigente.

Per il personale, l'obbligo formativo, almeno in fase iniziale, potrà eventualmente essere soddisfatto attraverso la messa a disposizione della specifica documentazione prodotta dall'Azienda.

Articolo 20: Violazione dei dati personali (Data Breach) - notifica e comunicazione

Una violazione dei dati personali è "*ogni infrazione alla sicurezza degli stessi 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 dal Titolare del trattamento*." La violazione dei dati è un tipo particolare di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del Regolamento UE 679/2016.

Ogni Autorizzato al trattamento dei dati personali è tenuto a informare senza ingiustificato ritardo il Titolare, del possibile caso di una violazione dei dati personali, contattando il Titolare all'indirizzo e-mail privacy@centrochirone.it

L'Azienda provvede a notificare la violazione all'Autorità Garante Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita *comunicazione dell'avvenuta violazione* nei modi previsti dalla normativa vigente. La notifica della violazione dei dati personali deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui non sia possibile fornire le informazioni contestualmente, le stesse potranno essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il Titolare del trattamento documenta qualsiasi violazione dei dati personali in un apposito registro delle violazioni di dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione consente all'autorità di controllo di verificare il rispetto delle indicazioni di legge.

DISPOSIZIONI FINALI

Articolo 21: Responsabilità in caso di violazione

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è punito con le sanzioni di natura amministrativa e di natura penale previste dagli artt. 166-172 del D. Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 nonché con sanzioni di natura disciplinare per violazione dei regolamenti aziendali.

Il Responsabile del Trattamento risponde per danno causato se non ha adempiuto agli obblighi previsti dal Regolamento a lui specificatamente attribuiti o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal titolare del trattamento.

Il titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo a loro imputabile.

Articolo 22: Rinvio a disposizioni di legge

Per tutto quanto non espressamente previsto dal presente Regolamento si rinvia alla normativa vigente in tema di protezione dei dati personali: Regolamento EU 679/2016 del 27/04/2016 e al D. Lgs. 196/2003 modificato dal D. Lgs. 101/2018 e ai provvedimenti specifici del Garante.

Il centro si riserva, inoltre, di adeguare, modificare o integrare il testo del presente Regolamento qualora per motivi organizzativi e/o la normativa e le direttive sopra citate lo rendano opportuno.