

INDICE

DISPOSIZIONI GENERALI	4
1 OGGETTO E FINALITÀ	4
2 AMBITO DI APPLICAZIONE	4
3 AMBITO DI APPLICAZIONE TERRITORIALE	4
4 DEFINIZIONI.....	4
CAPO II PRINCIPI	7
5 PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI	7
6 LICEITÀ DEL TRATTAMENTO	7
7 CONDIZIONI PER IL CONSENSO.....	7
8 CONDIZIONI APPLICABILI AL CONSENSO DEI MINORI IN RELAZIONE AI SERVIZI DELLA SOCIETÀ DELL'INFORMAZIONE	8
9 TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI	8
10 TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI	8
11 TRATTAMENTO CHE NON RICHIEDE L'IDENTIFICAZIONE	8
CAPO III DIRITTI DELL'INTERESSATO	9
<i>SEZIONE 1 TRASPARENZA E MODALITÀ</i>	<i>9</i>
12 INFORMAZIONI, COMUNICAZIONI E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO	9
<i>SEZIONE 2 INFORMAZIONE E ACCESSO AI DATI PERSONALI</i>	<i>9</i>
13 INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI SIANO RACCOLTI PRESSO L'INTERESSATO	9
14 INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI NON SIANO STATI OTTENUTI PRESSO L'INTERESSATO	9
15 DIRITTO DI ACCESSO DELL'INTERESSATO.....	9
<i>SEZIONE 3 RETTIFICA E CANCELLAZIONE.....</i>	<i>9</i>
16 DIRITTO DI RETTIFICA	9
17 DIRITTO ALLA CANCELLAZIONE ("DIRITTO ALL'OBLIO").....	9
18 DIRITTO DI LIMITAZIONE DI TRATTAMENTO.....	9
19 OBBLIGO DI NOTIFICA IN CASO DI RETTIFICA O CANCELLAZIONE DEI DATI PERSONALI O LIMITAZIONE DEL TRATTAMENTO	9
20 DIRITTO ALLA PORTABILITÀ DEI DATI	10
<i>SEZIONE 4 DIRITTO DI OPPOSIZIONE E PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE.....</i>	<i>10</i>
21 DIRITTO DI OPPOSIZIONE.....	10
22 PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE, COMPRESA LA PROFILAZIONE	10
<i>SEZIONE 5 LIMITAZIONI.....</i>	<i>10</i>
23 LIMITAZIONI	10
CAPO IV TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO.....	11
<i>SEZIONE 1 OBBLIGHI GENERALI</i>	<i>11</i>
24 RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO	11
25 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA	12
26 CONTITOLARI DEL TRATTAMENTO.....	13
27 RAPPRESENTANTI DI TITOLARI DEL TRATTAMENTO O DEI RESPONSABILI DEL TRATTAMENTO NON STABILITI NELL'UNIONE	13
28 RESPONSABILE DEL TRATTAMENTO.....	13
29 TRATTAMENTO SOTTO L'AUTORITÀ DEL TITOLARE DEL TRATTAMENTO O DEL RESPONSABILE DEL TRATTAMENTO	13
30 REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO	13
VIDEOSORVEGLIANZA (RIF. PROVVEDIMENTO IN MATERIA DI VIDEOSORVEGLIANZA - 8 APRILE 2010):	13
31 COOPERAZIONE CON L'AUTORITÀ DI CONTROLLO	13
<i>SEZIONE 2 SICUREZZA DEI DATI PERSONALI.....</i>	<i>13</i>
32 SICUREZZA DEL TRATTAMENTO	13
33 NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO	14
34 COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO.....	14
<i>SEZIONE 3 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA</i>	<i>14</i>
35 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI	14
36 CONSULTAZIONE PREVENTIVA	15
<i>SEZIONE 4 RESPONSABILE DELLA PROTEZIONE DEI DATI</i>	<i>16</i>
37 DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI.....	16

MANUALE DI GESTIONE PRIVACY

38	POSIZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI	16
39	COMPITI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI.....	16
	<i>SEZIONE 5 CODICI DI CONDOTTA E CERTIFICAZIONE.....</i>	<i>16</i>
40	CODICI DI CONDOTTA.....	16
41	MONITORAGGIO DEI CODICI DI CONDOTTA APPROVATI.....	17
42	CERTIFICAZIONE.....	17
43	ORGANISMI DI CERTIFICAZIONE	17
CAPO V TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI.....		18
44	PRINCIPIO GENERALE PER IL TRASFERIMENTO	18
45	TRASFERIMENTO SULLA BASE DI UNA DECISIONE DI ADEGUATEZZA.....	18
46	TRASFERIMENTO SOGGETTO A GARANZIE ADEGUATE.....	18
47	NORME VINCOLANTI D'IMPRESA	18
48	TRASFERIMENTO O COMUNICAZIONE NON AUTORIZZATI DAL DIRITTO DELL'UNIONE	18
49	DEROGHE IN SPECIFICHE SITUAZIONI	18
50	COOPERAZIONE INTERNAZIONALE PER LA PROTEZIONE DEI DATI PERSONALI	18
CAPO VI AUTORITÀ DI CONTROLLO INDIPENDENTI.....		19
	<i>SEZIONE 1 INDIPENDENZA.....</i>	<i>19</i>
51	AUTORITÀ DI CONTROLLO	19
52	INDIPENDENZA	19
53	CONDIZIONI GENERALI PER I MEMBRI DELL'AUTORITÀ DI CONTROLLO.....	19
54	NORME SULL'ISTITUZIONE DELL'AUTORITÀ DI CONTROLLO.....	19
	<i>SEZIONE 2 COMPETENZA, COMPITI E POTERI</i>	<i>19</i>
55	COMPETENZA	19
56	COMPETENZA DELL'AUTORITÀ DI CONTROLLO CAPOFILA	19
57	COMPITI	19
58	POTERI	19
59	RELAZIONI DI ATTIVITÀ	19
CAPO VII COOPERAZIONE E COERENZA		19
	<i>SEZIONE 1 COOPERAZIONE.....</i>	<i>19</i>
60	COOPERAZIONE TRA L'AUTORITÀ DI CONTROLLO CAPOFILA E LE ALTRE AUTORITÀ DI CONTROLLO INTERESSATE	19
61	ASSISTENZA RECIPROCA	19
62	OPERAZIONI CONGIUNTE DELLE AUTORITÀ DI CONTROLLO	19
	<i>SEZIONE 2 COERENZA.....</i>	<i>20</i>
63	MECCANISMO DI COERENZA	20
64	PARERE DEL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI.....	20
65	COMPOSIZIONE DELLE CONTROVERSIE DA PARTE DEL COMITATO.....	20
66	PROCEDURA D'URGENZA.....	20
67	SCAMBIO DI INFORMAZIONI.....	20
	<i>SEZIONE 3 COMITATO EUROPEO PER LA PROTEZIONE DEI DATI</i>	<i>20</i>
68	COMITATO EUROPEO PER LA PROTEZIONE DEI DATI.....	20
69	INDIPENDENZA	20
70	COMPITI DEL COMITATO	20
71	RELAZIONI.....	20
72	PROCEDURA	20
73	PRESIDENTE.....	20
74	COMPITI DEL PRESIDENTE.....	20
75	SEGRETERIA.....	20
76	RISERVATEZZA.....	20
CAPO VIII MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI.....		21
77	DIRITTO DI PROPORRE RECLAMO ALL'AUTORITÀ DI CONTROLLO	21
78	DIRITTO A UN RICORSO GIURISDIZIONALE EFFETTIVO NEI CONFRONTI DELL'AUTORITÀ DI CONTROLLO	21
79	DIRITTO A UN RICORSO GIURISDIZIONALE EFFETTIVO NEI CONFRONTI DEL TITOLARE DEL TRATTAMENTO O DEL RESPONSABILE DEL TRATTAMENTO.....	21
80	RAPPRESENTANZA DEGLI INTERESSATI	21

81	SOSPENSIONE DELLE AZIONI.....	21
82	DIRITTO AL RISARCIMENTO E RESPONSABILITÀ.....	22
83	CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE.....	22
84	SANZIONI.....	23
CAPO IX DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO.....		24
85	TRATTAMENTO E LIBERTÀ D'ESPRESSIONE E DI INFORMAZIONE.....	24
86	TRATTAMENTO E ACCESSO DEL PUBBLICO AI DOCUMENTI UFFICIALI.....	24
87	TRATTAMENTO DEL NUMERO DI IDENTIFICAZIONE NAZIONALE.....	24
88	TRATTAMENTO DEI DATI NELL'AMBITO DEI RAPPORTI DI LAVORO.....	24
89	GARANZIE E DEROGHE RELATIVE AL TRATTAMENTO A FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE, DI RICERCA SCIENTIFICA O STORICA O A FINI STATISTICI.....	24
90	OBBLIGHI DI SEGRETEZZA.....	24
91	NORME DI PROTEZIONE DEI DATI VIGENTI PRESSO CHIESE E ASSOCIAZIONI RELIGIOSE.....	24
CAPO X ATTI DELEGATI E ATTI DI ESECUZIONE.....		24
92	ESERCIZIO DELLA DELEGA.....	24
93	PROCEDURA DI COMITATO.....	24
CAPO XI DISPOSIZIONI FINALI.....		24

COPIA N. _____ ASSEGNATA A: _____
DISTRIBUZIONE CONTROLLATA: <input type="checkbox"/> SI <input type="checkbox"/> NO
LIVELLO M (AD USO INTERNO)

0	Prima stesura		24.05.201		24.05.201
Rev.	PARTI REVISIONATE	REDAZIONE	DATA	APPROVAZIONE	DATA

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 4 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	----------------------------------------------

DISPOSIZIONI GENERALI

1 Oggetto e finalità

In conformità a quanto disposto dal Regolamento l'organizzazione ha definito le modalità di attuazione del proprio sistema di gestione privacy al fine di assicurare la protezione dei dati che la stessa tratta in qualità di Titolare o di Responsabile del Trattamento dati per conto di terzi.

2 Ambito di applicazione

Il presente manuale si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivi sia elettronici che fisici.

3 Ambito di applicazione territoriale

Il presente sistema di Gestione Privacy si applica al trattamento dei dati personali effettuato nell'ambito delle attività svolte **CENTRO DIAGNOSTICO S. CIRO S.R.L.** in qualità di titolare del trattamento dati.

Il **CENTRO DIAGNOSTICO S. CIRO S.R.L.** eroga prestazioni ambulatoriali :

1. Laboratorio di analisi
2. Dermatologia
3. – visita specialistica
4. – mappatura dei nei
5. – crioterapia
6. – dermatologia estetica
7. Endocrinologia
8. Otorinolaringoiatria
9. Oculistica
10. Pneumologia
11. Neurologia
12. – visita specialistica
13. – elettromiografia
14. – elettroencefalogramma
15. Senologia
16. Urologia
17. Ortopedia
18. Ozonoterapia
19. Medicina nucleare
20. Cardiologia
21. Diagnostica per immagini

4 Definizioni

Si intende per:

- 1) "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;
- 2) "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,

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 5 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------

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;

3) "limitazione di trattamento": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) "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;

5) "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;

6) "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;

7) "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;

8) "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;

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

10) "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;

11) "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;

12) "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;

13) "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;

14) "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;

15) "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;

16) "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

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016	MGP REV. 0 DEL 24.05.18 PAG 6 DI 24
	MANUALE DI GESTIONE PRIVACY	

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;

17) "rappresentante": la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) "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;

19) "gruppo imprenditoriale": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) "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;

21) "autorità di controllo": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) "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;

23) "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;

24) "obiezione pertinente e motivata": un'obiezione 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 del caso, alla libera circolazione dei dati personali all'interno dell'Unione;

25) "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 Consiglio¹;

1

26) "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.

¹ Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016	MGP REV. 0 DEL 24.05.18 PAG 7 DI 24
MANUALE DI GESTIONE PRIVACY		

CAPO II PRINCIPI

5 Principi applicabili al trattamento di dati personali

1. I dati personali che **CENTRO DIAGNOSTICO S. CIRO S.R.L.** raccoglie sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- b) raccolti solo per le finalità esplicite e legittime relative al servizio erogato dal **CENTRO DIAGNOSTICO S. CIRO S.R.L.** in forza di contratti in essere con i propri clienti
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- d) esatti e, se necessario, aggiornati ("esattezza") con periodicità definita nel registro del trattamento dati;
- e) conservati in assicurandone l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione"); i tempi di conservazione del dato sono indicati nella Policy Privacy
- f) trattati in modo da assicurarne integrità e riservatezza".

6 Liceità del trattamento

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. tratta i dati in forza della liceità del trattamento stesso nei seguenti casi:

- concludere i contratti per i servizi del Titolare;
- adempiere agli obblighi precontrattuali, contrattuali e fiscali derivanti da rapporti con Lei in essere;
- adempiere agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria o da un ordine dell'Autorità (come ad esempio in materia di antiriciclaggio);
- esercitare i diritti del Titolare, ad esempio il diritto di difesa in giudizio;

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle condizioni riportate all'art. 6 del Regolamento Europeo 679/2016:

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. specifica la liceità del trattamento nella INFORMATIVA Trattamento Dati (MOD. INF)

7 Condizioni per il consenso

Solo previo specifico e distinto consenso (art. 7 GDPR), i dati possono essere trattati per le seguenti Finalità di Marketing:

- inviarLe via e-mail, posta e/o sms e/o contatti telefonici, newsletter, comunicazioni commerciali e/o materiale pubblicitario su prodotti o servizi offerti dal Titolare e rilevazione del grado di soddisfazione sulla qualità dei servizi;
- inviarLe via e-mail, posta e/o sms e/o contatti telefonici comunicazioni commerciali e/o promozionali di soggetti terzi (ad esempio, business partner, compagnie assicurative, ecc).

Il consenso viene richiesto in forma scritta e specifico per ogni finalità attraverso sottoscrizione del consenso su moduli cartacei, in ogni caso per ogni specifico trattamento diverso da quelli indicati al par. 6 viene richiesto sempre esplicito consenso con modulistica di sistema specifica (modulo consenso MOD. 06)

L'evidenza del consenso viene conservata per tutto il tempo necessario al trattamento del dato per cui il consenso è stato richiesto.

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 8 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	----------------------------------------------

8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

Il **CENTRO DIAGNOSTICO S. CIRO S.R.L.** può trattare anche dati di minori con un'età inferiore ai 16 anni ed in tali casi il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

9 Trattamento di categorie particolari di dati personali

Il **CENTRO DIAGNOSTICO S. CIRO S.R.L.** non tratta dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati biometrici.

Il laboratorio potrebbe trattare dati genetici, intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, in tali casi l'interessato :

- ha prestato il proprio consenso esplicito al trattamento dei dati personali per una o più finalità specifiche;
- 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. tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali

I dati personali dei dipendenti oggetti per legge a visite mediche di idoneità fisica alla mansione sono trattati esclusivamente dal medico competente incaricato che resta Titolare del dato sanitario in funzione dell'erogazione del suo servizio

Il consenso al trattamento dei dati dei dipendenti per le finalità relative al contratto di assunzione è implicito nella sottoscrizione del contratto stesso.

Il consenso al trattamento dei dati personali degli interessati comunicati da Titolari del Trattamento alla **CENTRO DIAGNOSTICO S. CIRO S.R.L.** in qualità di Responsabile del Trattamento dati per conto Terzi e necessari per l'erogazione del servizio richiesto è raccolto a cura dello stesso Titolare del Trattamento

10 Trattamento dei dati personali relativi a condanne penali e reati

CENTRO DIAGNOSTICO S. CIRO S.R.L. non tratta dati personali relativi a condanne penali e reati

11 Trattamento che non richiede l'identificazione

La **CENTRO DIAGNOSTICO S. CIRO S.R.L.** tratta esclusivamente dati personali che richiedono identificazione.

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 9 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	----------------------------------------------

CAPO III DIRITTI DELL'INTERESSATO

SEZIONE 1 TRASPARENZA E MODALITÀ

12 Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. ha definito apposita INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI (MOD. INF) per le modalità di accesso e gestione dei dati personali

SEZIONE 2 INFORMAZIONE E ACCESSO AI DATI PERSONALI

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

Rif. Informativa Trattamento Dati MOD. INF

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

Rif. Informativa Trattamento Dati MOD. INF

15 Diritto di accesso dell'interessato

L'interessato può, in qualsiasi momento, richiedere informazioni in merito ai propri dati (finalità e categorie, destinatari, ecc) secondo quanto indicato nell'Informativa al Trattamento dei Dati MOD. INF

SEZIONE 3 RETTIFICA E CANCELLAZIONE

16 Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. (rif. Informativa al Trattamento dei Dati MOD. INF)

17 Diritto alla cancellazione ("diritto all'oblio")

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano facendone esplicita richiesta a mezzo mail, pec o raccomandata.

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. assicura la cancellazione del dato entro **un mese dal ricevimento della richiesta stessa** (art. 13 co 3)

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. informa l'interessato sulle modalità di esercizio di tale diritto (rif. Informativa Trattamento Dati MOD. INF)

18 Diritto di limitazione di trattamento

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle ipotesi definite nell'art. 18 del Regolamento

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. informa l'interessato sulle modalità di esercizio di tale diritto (rif. Informativa Trattamento Dati MOD. INF)

19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 10 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

La CENTRO DIAGNOSTICO S. CIRO S.R.L. informa l'interessato sulle modalità di esercizio di tale diritto (rif. Informativa Trattamento Dati MOD. INF)

20 Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

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

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

La **CENTRO DIAGNOSTICO S. CIRO S.R.L.** informa l'interessato sulle modalità di esercizio di tale diritto (rif. Informativa Trattamento Dati MOD. INF) –

SEZIONE 4 DIRITTO DI OPPOSIZIONE E PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE

21 Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.

La **CENTRO DIAGNOSTICO S. CIRO S.R.L.** informa l'interessato sulle modalità di esercizio di tale diritto (rif. Informativa Trattamento Dati MOD. INF)

22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

I processi automatizzati in essere non hanno valenza decisionale in merito alla gestione del dato

SEZIONE 5 LIMITAZIONI

23 Limitazioni

Non applicabile

CAPO IV TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

SEZIONE 1 OBBLIGHI GENERALI

24 Responsabilità del titolare del trattamento

Il trattamento è effettuato conformemente al Regolamento 679/2016.

Sono definite adeguate misure di trattamento (vedi Registro dei Trattamenti MOD.01) in base alla tipologia di dato trattato ed al rischio valutato (vedi Risk Asssment MOD. RAS).

VALUTAZIONE DEL RISCHIO

METODOLOGIA

La valutazione dei rischi è effettuata utilizzando i seguenti indici:

INDICE DI PROBABILITA' (P): probabilità che si verifichi un evento

INDICE DI GRAVITA' (M): esprime l'entità delle conseguenze possibili

INDICE DI RISCHIO (R): definito come prodotto dell' indice di probabilità (P) per l'indice di gravità (M)
I criteri di quantificazione dei tre indici, definiti secondo una scala semi-qualitativa, sono i seguenti:

INDICE DI PROBABILITA' (P)

Valore, Livello, Definizione

1) Improbabile: Non sono noti episodi già verificatisi. L'evento può provocare un danno per la concomitanza di più eventi poco probabili indipendenti.

2) Poco Probabile: Sono noti rarissimi episodi già verificatisi. L'evento può provocare un danno solo in caso di fortuite condizioni particolari.

3) Probabile: E' noto qualche episodio in cui l'evento si è verificato causando un danno anche se non in maniera automatica o diretta.

4) Altamente Probabile

Si sono verificati eventi simili che hanno prodotto un danno all'interno dello stesso stabilimento o in situazioni operative simili. Esiste una correlazione diretta tra l'evento ed il danno ipotizzabile.

INDICE DI GRAVITA' (M)

Valore, Livello, Definizione

1) Lieve: Le conseguenze sono sicuramente e rapidamente reversibili e possono essere dovute ad una situazione

2) Medio: Effetti reversibili dovuti ad esposizione cronica o episodio di esposizione acuta. anomala o di emergenza

3) Grave: Effetti irreversibili e/o parzialmente irreversibili dovuti ad una situazione anomala o di emergenza

4) Gravissimo: Effetti totalmente irreversibili

Il valore del rischio è stato classificato nel modo seguente:

< di 20 **Basso trascurabile:** non si applicheranno nuove contromisure e si verificherà la

consistenza di quelle in essere

20<41 **Medio da valutare**: si valuteranno interventi integrativi con programmazione anche nel lungo periodo

>40 **Alto**: Valutato l'impatto sugli interessati si procederà ad inserire contromisure congrue alla sua mitigazione. In assenza di tali contromisure si provvederà con richiesta preventiva al garante.

SCHEMA DI VALUTAZIONE DEL RISCHIO

INDICE DI RISCHIO - $R = P \times M$

La stima dell'indice di rischio (R) è stata effettuata utilizzando la seguente matrice:

		10 ⁻³					
FREQUENZA (Eventi/Anno)	Altamente Probabile	10 ⁻⁴	4	8	12	16	Area - Rischio Molto Alto - NON Accettabile Area di rischio - Non Moderato - necessario intervenire Area di Attenzione - Rischio Moderato - opportuno intervenire
	Probabile	10 ⁻⁵	3	6	9	12	
	Poco probabile	10 ⁻⁶	2	4	6	8	
	Improbabile	Estr. Raro	1	2	3	4	
			Lieve	Medio	Grave	Gravissimo	Area di Rischio Trascurabile
			CONSEGUENZE				

25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

Per dati trattati informaticamente e cartaceamente vigono specifiche regole e restrizioni come riportato nell'Istruzione IO 01 distribuita ai singoli incaricati alla gestione dei dati.

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016	MGP REV. 0 DEL 24.05.18 PAG 13 DI 24
	MANUALE DI GESTIONE PRIVACY	

26 Contitolari del trattamento

La CENTRO DIAGNOSTICO S. CIRO S.R.L. non ha nominato al momento contitolari del trattamento dati.

27 Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione

Non applicabile

28 Responsabile del trattamento

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. ha incaricato, quale Responsabile del Trattamento Dati Esterno conb singole lettere di incarico.

Incarico che è specificato come richiesto dal Regolamento 679/2016 nella nomina Mod. INC (art. 28 co. 1,3):

il Titolare del dato resta **CENTRO DIAGNOSTICO S. CIRO S.R.L.**

29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

CENTRO DIAGNOSTICO S. CIRO S.R.L., in qualità di Titolare del Trattamento dati nell'erogazione del proprio servizio, si assicura che il Responsabile del Trattamento Dati esterni detenga il dato al solo fine indicato nella relativa Lettera di nomina.

30 Registri delle attività di trattamento

CENTRO DIAGNOSTICO S. CIRO S.R.L. ha definito i registri delle attività di trattamento dei dati relativi ad ogni paziente e tipologia di dati trattati (rif. Registro Trattamento dati MOD. RTT).

È stato definito anche un registro per il trattamento della videosorveglianza.

VIDEOSORVEGLIANZA (rif. Provvedimento in materia di videosorveglianza - 8 aprile 2010):

IL CENTRO DIAGNOSTICO S. CIRO S.R.L. ha predisposto specifico registro per il trattamento dei dati effettuati a mezzo di videocamere.

31 Cooperazione con l'autorità di controllo

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. in qualità di titolare del trattamento collabora su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

SEZIONE 2 SICUREZZA DEI DATI PERSONALI

32 Sicurezza del trattamento

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. ha implementato il proprio sistema di gestione della privacy partendo dalla definizione dei dati trattati ed effettuando un'analisi dei rischi ad essi legati (Risk Assesment MOD. RAS)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, Ha definito nella Matrice dei Rischi (MOD. RAS) le misure tecniche e organizzative adeguate da attuare per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità e la disponibilità e dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016	MGP REV. 0 DEL 24.05.18 PAG 14 DI 24
MANUALE DI GESTIONE PRIVACY		

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (stress test).

Nel valutare l'adeguato livello di sicurezza, CENTRO DIAGNOSTICO S. CIRO S.R.L. tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (RISK ASSESSMENT MOD. RAS)

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. assicura che gli incaricati addetti al trattamento dei dati vengano adeguatamente istruiti al fine di assicurare l'adeguato livello di sicurezza degli stessi attraverso la stesura di un programma formativo adeguato (rif. Piano di Formazione) e la distribuzione di apposita istruzione di lavoro (IO 01 "Istruzioni Incaricati al Trattamento dati).

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

In caso di violazione dei dati personali, Il **CENTRO DIAGNOSTICO S. CIRO S.R.L.**, in qualità di titolare del trattamento provvede alla notifica della violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

La notifica, strutturata su apposito modulo (MOD VDP) contiene le seguenti informazioni:

- a) natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) le probabili conseguenze della violazione dei dati personali;
- d) 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.

34 Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche CENTRO DIAGNOSTICO S. CIRO S.R.L. comunica la violazione all'interessato, senza ingiustificato ritardo.

La comunicazione avviene a mezzo mail e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

Il rischio legato alla possibile violazione dei dati personali è stato analizzato da CENTRO DIAGNOSTICO S. CIRO S.R.L. ed è riportato, incluso le misure di mitigazione da attuare nel Risk Assessment (MOD. RAS)

SEZIONE 3 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA

35 Valutazione d'impatto sulla protezione dei dati

Nei casi stabiliti dall'art. 35 è necessario effettuare una Valutazione di Impatto sulla protezione dei dati.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016	MGP REV. 0 DEL 24.05.18 PAG 15 DI 24
	MANUALE DI GESTIONE PRIVACY	

- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza).

CENTRO DIAGNOSTICO S. CIRO S.R.L. ha definito la valutazione di impatto nel modello di Risk Assessment (MOD. RAS)

Se i trattamenti effettuati rientrano nell'elenco redatto dall'autorità di controllo (art. 35 co.4-5-6) CENTRO DIAGNOSTICO S. CIRO S.R.L. per tali trattamenti definisce una valutazione che contiene:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Periodicamente il CENTRO DIAGNOSTICO S. CIRO S.R.L. procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Il riesame viene formalizzato su apposito modulo (Riesame Sistema di Gestione)

36 Consultazione preventiva

il CENTRO DIAGNOSTICO S. CIRO S.R.L., prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

L'Autorità di Controllo, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, comunica con un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento in merito alla sua richiesta di consultazione.

Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.

La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

L'autorità di controllo può stabilire di iniziare attività di indagini, come indicato all'art. 58 del Regolamento

Al momento di consultare l'autorità di controllo CENTRO DIAGNOSTICO S. CIRO S.R.L. comunica all'autorità di controllo:

- a) le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- b) le finalità e i mezzi del trattamento previsto;
- c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
- d) se del caso, i dati di contatto del titolare della protezione dei dati;
- e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
- f) ogni altra informazione richiesta dall'autorità di controllo.

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 16 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

SEZIONE 4 RESPONSABILE DELLA PROTEZIONE DEI DATI

37 Designazione del responsabile della protezione dei dati

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. ha designato sistematicamente un responsabile della protezione dei dati in quanto rientra nella casistica art. 37 comma 1,a) individuandolo come esterno al Centro e incaricando La ITADVICE SCARL nella persona di Silvio Tortora Maione in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39. I dati di contatto del responsabile della protezione dei dati sono resi noti attraverso le informative e comunicati all'autorità di controllo. I dati di contatto sono disponibili nella nomina presso l'autorità garante.

38 Posizione del responsabile della protezione dei dati

Il responsabile della protezione dei dati è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali dispone delle risorse necessarie per assolvere ai compiti previsti dall'art. 39 GDPR e accedere ai dati personali ed ai trattamenti e per mantenere la propria conoscenza specialistica.

Il responsabile della protezione dei dati non riceve alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. E non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del Trattamento per l'adempimento degli stessi e nell'esercizio delle sue mansioni riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. fornisce agli interessati le modalità con cui gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR. Attraverso mail appositamente creata dpo@cemsmdp.it

Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. CENTRO DIAGNOSTICO S. CIRO S.R.L. si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

39 Compiti del responsabile della protezione dei dati

Il responsabile della protezione dei dati è incaricato di .:

informare e fornire consulenza al CENTRO DIAGNOSTICO S. CIRO S.R.L. e nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR

sorvegliare l'osservanza del GDPR,

fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento

cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

SEZIONE 5 CODICI DI CONDOTTA E CERTIFICAZIONE

40 Codici di condotta

Gli Stati Membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 17 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------

CENTRO DIAGNOSTICO S. CIRO S.R.L. ha definito un proprio “codice di Condotta” cui aderisce e, in sede di riunione periodica per il riesame del proprio sistema privacy, valuterà la conformità dello stesso ad eventuali codici di condotta emessi da organismi ed associazioni di riferimento e/o dalle autorità di Controllo.

41 Monitoraggio dei codici di condotta approvati

Il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 deve essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente. CENTRO DIAGNOSTICO S. CIRO S.R.L. si allineerà a quanto definito da tali organismi se e quando verranno emessi codici di condotta a cui deciderà di aderire.

42 Certificazione

Al momento non sono ancora state emesse norme per la certificazione dei sistemi di gestione per la privacy. Il CENTRO DIAGNOSTICO S. CIRO S.R.L. valuterà a tempo debito l'opportunità di conformarsi ad una norma volontaria per eventuale certificazione del proprio sistema di gestione per la privacy

43 Organismi di certificazione

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 18 DI 24
----------------------------	----------------------------------------------------------------------------------------------	-----------------------------------------------

CAPO V TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

CENTRO DIAGNOSTICO S. CIRO S.R.L. NON TRASFERISCE DATI VERSO PAESI TEZI O ORGANIZZAZIONI INTERNAZIONALI PER CUI IL CAPO V DEL REGOLAMENTO UE N679/2016 NON SI APPLICA

(artt. da 44 a 50)

44 Principio generale per il trasferimento

45 Trasferimento sulla base di una decisione di adeguatezza

46 Trasferimento soggetto a garanzie adeguate

47 Norme vincolanti d'impresa

48 Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

49 Deroghe in specifiche situazioni

50 Cooperazione internazionale per la protezione dei dati personali

CAPO VI AUTORITÀ DI CONTROLLO INDIPENDENTI**SEZIONE 1 INDIPENDENZA****51 Autorità di controllo**

L'autorità di controllo in Italia è il Garante per la Privacy

52 Indipendenza

Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al Regolamento UE n. 679/2016.

53 Condizioni generali per i membri dell'autorità di controllo

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

54 Norme sull'istituzione dell'autorità di controllo

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

SEZIONE 2 COMPETENZA, COMPITI E POTERI**55 Competenza**

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

56 Competenza dell'autorità di controllo capofila

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

57 Compiti

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

58 Poteri

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

59 Relazioni di attività

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

CAPO VII COOPERAZIONE E COERENZA**SEZIONE 1 COOPERAZIONE****60 Cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate**

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

61 Assistenza reciproca

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

62 Operazioni congiunte delle autorità di controllo

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 20 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

SEZIONE 2 COERENZA

63 Meccanismo di coerenza

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

64 Parere del comitato europeo per la protezione dei dati

Di competenza del Comitato Europeo per la protezione dei dati

65 Composizione delle controversie da parte del comitato

Di competenza del Comitato Europeo per la protezione dei dati

66 Procedura d'urgenza

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE e del Comitato Europeo per la protezione dei dati

67 Scambio di informazioni

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE e del Comitato Europeo per la protezione dei dati

SEZIONE 3 COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

68 Comitato europeo per la protezione dei dati

Di competenza del Comitato Europeo per la protezione dei dati

69 Indipendenza

Di competenza del Comitato Europeo per la protezione dei dati

70 Compiti del comitato

Di competenza del Comitato Europeo per la protezione dei dati

71 Relazioni

Di competenza del Comitato Europeo per la protezione dei dati

72 Procedura

Di competenza del Comitato Europeo per la protezione dei dati

73 Presidente

Di competenza del Comitato Europeo per la protezione dei dati

74 Compiti del presidente

Di competenza del Comitato Europeo per la protezione dei dati

75 Segreteria

Di competenza del Comitato Europeo per la protezione dei dati

76 Riservatezza

Di competenza del Comitato Europeo per la protezione dei dati

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 21 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

CAPO VIII MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI

77 Diritto di proporre reclamo all'autorità di controllo

L'art. 77 del regolamento recita: *Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.*

L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. , in qualità di Responsabile del trattamento dati per conto terzi o di Titolare del trattamento dei propri dati, se viene a conoscenza di una violazione del regolamento nel trattamento dei dati, lo comunica al proprio Responsabile della Protezione dati che si attiverà per interpellare l'autorità di controllo in merito e per porre in essere tutte le azioni di mitigazione e ripristino della liceità del trattamento.

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. provvederà altresì a revisionare la sua analisi dei rischi (MOD. RAS) al fine di evitare il ripetersi del trattamento illecito.

78 Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.

Le modalità sono definite dal Regolamento all'art. 78 e sono di competenza dell'autorità di Controllo.

79 Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

L'art. 79 del Regolamento 679/2016 recita:

"1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri".

80 Rappresentanza degli interessati

L'interessato al trattamento può proporre reclamo anche attraverso un organismo, un'organizzazione o un'associazione autorizzati (rif. Art. 80 Regolamento UE 679/2016) all'Autorità Competente (Garante Privacy, Autorità giurisdizionale)

81 Sospensione delle azioni

Di competenza dell'Autorità di Controllo di ogni paese membro dell'UE

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 22 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

82 Diritto al risarcimento e responsabilità

L'art. 82 del Regolamento UE 679/2016 recita:

1. *Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.*
2. *Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che viola il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*
3. *Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.*
4. *Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.*
5. *Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.*
6. *Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.*

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. si attiene, in merito all'eventualità di richiesta di risarcimento danni per violazione del regolamento 679/2016 a quanto riportato nel suddetto articolo

83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

Il CENTRO DIAGNOSTICO S. CIRO S.R.L. nel proprio sistema di gestione per la privacy, tiene conto di quanto stabilito all'articolo 83 del Regolamento UE 679/2016:

L'autorità di controllo può infliggere sanzioni pecuniarie e amministrative in funzione delle circostanze di ogni singolo caso.

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso l'Autorità di Controllo tiene debito conto dei seguenti elementi:

- a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- b) il carattere doloso o colposo della violazione;
- c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto (rif. par 25 e 32);
- e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- g) le categorie di dati personali interessate dalla violazione;
- h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 23 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

- i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- j) l'adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati
- k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso (ad esempio i benefici finanziari conseguiti o le perdite evitate), direttamente o indirettamente, quale conseguenza della violazione.

Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del regolamento 679/2016, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

La violazione delle disposizioni seguenti del Regolamento UE 679/2016 è soggetta a sanzioni amministrative pecuniarie fino a **10 000 000 EUR**, o per le imprese, fino al **2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore:

- a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 e 43;

La violazione delle disposizioni seguenti del Regolamento UE 679/2016 è soggetta a sanzioni amministrative pecuniarie fino a **20 000 000 EUR**, o per le imprese, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore:

- a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- b) i diritti degli interessati a norma degli articoli da 12 a 22;
- c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49 ;
- d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

L'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2 del Regolamento UE 679/2016, è soggetta a sanzioni amministrative pecuniarie fino a **20 000 000 EUR**, o per le imprese, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

84 Sanzioni

Altre sanzioni in merito possono essere stabilite dai singoli Stati membri dell'Unione Europea.

CENTRO DIAGNOSTICO S. CIRO	SISTEMA DI GESTIONE PRIVACY REG. UE 679/2016 MANUALE DI GESTIONE PRIVACY	MGP REV. 0 DEL 24.05.18 PAG 24 DI 24
----------------------------	---------------------------------------------------------------------------------------------------------	-----------------------------------------------

CAPO IX DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO

85 Trattamento e libertà d'espressione e di informazione

N.A.

86 Trattamento e accesso del pubblico ai documenti ufficiali

I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento.

87 Trattamento del numero di identificazione nazionale

N.A.

88 Trattamento dei dati nell'ambito dei rapporti di lavoro

Di competenza di ogni Stato Membro

89 Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

N.A.

90 Obblighi di segretezza

Di competenza di ogni Stato Membro

91 Norme di protezione dei dati vigenti presso chiese e associazioni religiose

N.A.

CAPO X ATTI DELEGATI E ATTI DI ESECUZIONE

92 Esercizio della delega

Di competenza della Commissione Europea

93 Procedura di comitato

Di competenza della Commissione Europea e del Comitato Europeo

CAPO XI DISPOSIZIONI FINALI

Per le disposizioni finali riportate nel Regolamento UE 679/2016 CENTRO DIAGNOSTICO S. CIRO S.R.L. si attiene a quanto riportato negli artt. 94-95-96-97-98-99