MEDICA S.p.A.
Via Degli Artigiani, 7
41036 MEDOLLA
MODENA - ITALY

Tel. 0535 51159
Fax 0535 52605
e-mail: info@medica.it
home page: www.medica.it

International:
Tel. +39 0535 51159
Fax +39 0535 52605

MEDICA S.P.A.

Policy sui diritti dell'interessato
Gestione delle richieste

INFORMAZIONI DOCUMENTO:

Titolo	Policy sui diritti dell'interessato – gestione delle richieste		
Data di emissione		**Versione**	1.0

Approvata con delibera del Consiglio di Amministrazione n.

1. INTRODUZIONE

1.1. FINALITA'

La presente *policy* (di seguito, "***Policy***") ha la finalità di definire le istruzioni pratiche necessarie per la gestione di richieste da parte dei soggetti interessati (**"Interessati"**) concernenti l'esercizio dei propri diritti come garantito dalle disposizioni contenute nel Regolamento UE 679/2016 (di seguito "**GDPR**").

1.2. NORMATIVA DI RIFERIMENTO

- **GDPR**, e segnatamente, artt. 12-22 e 34 del GDPR (Allegato D)

1.3. AMBITO DI APPLICAZIONE

La presente *Policy* si applica ai seguenti soggetti:

i. componenti degli organi societari, dirigenti e dipendenti della società;

ii. soggetti nominati da Medica s.p.a. quali Responsabili del Trattamento, e più precisamente:

- avv. Marco Pala, ing. Davide Bagnoli, dott. Marco Fecondini, dott. Antonio Rossetti, dott.ssa Chiara Stancari, ing. Lorenzo Barbieri;
- altri soggetti terzi nominati Responsabili del Trattamento, con riferimento ad attività e servizi effettuati per conto di Medica s.p.a., che implicano il trattamento di dati personali di cui Medica s.p.a. risulta Titolare.

La *Policy* deve inoltre essere resa vincolante per:

iii. soggetti Incaricati/Autorizzati, cioè soggetti che svolgano per conto del Medica s.p.a. attività o servizi, che implicano il trattamento di dati personali di cui Medica s.p.a. è Titolare, secondo la definizione di "Incaricato/Autorizzato" sotto riportata.

1.4. DEFINIZIONI

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.

Aree Sensibili: sono quei luoghi fisici o della Rete in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR.

Cloud: modello di conservazione dati su computer in rete dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati.

Comunicazione di Dati Personali: dare conoscenza dei Dati Personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

Consenso dell'Interessato o **Consenso**: 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,

Data Breach ovvero **Violazione Dei Dati Personali:** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Dati Biometrici: i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati Comuni: sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari.

Dati Genetici: i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati Giudiziari: Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Dati Sensibili (definiti come dati rientranti in "Categorie Particolari" *ex* Art 9.1 GDPR): Dati Personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale. Rientrano in questa categoria anche i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

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;

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.;

Destinatario/i: 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;

Device Fissi (Aziendali o Personali): le Risorse Informatiche non facilmente rimuovibili dal perimetro aziendale quali personal computer, server locali, stampanti.

Device Mobili (Aziendali o Personali): le Risorse Informatiche che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet, laptop e smartphone.

Diffusione di Dati Personali: la comunicazione dei Dati Personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dossier Sanitario Elettronico: è lo strumento costituito presso un'unica struttura sanitaria che raccoglie informazioni sulla salute del paziente al fine di documentarne la storia clinica presso quella struttura e offrirgli un migliore processo di cura.

DPO o **Data Protection Officer**: la persona nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR, che deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR.

GDPR: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Incaricato/Autorizzato al Trattamento: qualsiasi collaboratore autorizzato al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4 (10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; (c) nonché, i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

Limitazione Di Trattamento: il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

Processo Decisionale Automatizzato: decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;

Profilazione: qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere

aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

Responsabile del Trattamento o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

Rete: rappresenta il perimetro digitale della Società contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet) a cui ci si può collegare via rete LAN, Wi-Fi o VPN.

Richiesta: qualsiasi istanza/domanda proveniente da un Interessato in relazione all'esercizio dei propri diritti in materia privacy previsti dal GDPR e rivolta al Titolare del Trattamento o ad un Responsabile del Trattamento in relazione ai Dati Personali dell'Interessato.

Risorse Informatiche: sono da considerarsi risorse informatiche qualsiasi tipo di hardware e device contenente un hardware, mezzo di comunicazione elettronica, rete di trasmissione dati, software ed applicazioni software, informazioni in formato elettronico.
Le Risorse Informatiche possono essere **"Aziendali"** cioè messe a disposizione dalla società quali strumenti di lavoro, ovvero **"Personali"** cioè appartenenti al singolo dipendente o collaboratore – il cui uso puo' essere ammesso a fini aziendali solo in determinate condizioni e seguendo le procedure eventualmente stabilite dall'Azienda.

Sub-Responsabile del Trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale un Responsabile del Trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del Titolare.

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;

Titolare del Trattamento o **Titolare:** 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Trattamento o **Trattato/Trattati:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Trattamento Transfrontaliero: indica a) un 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 o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) un Trattamento di dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro.

2. DIRITTI DELL'INTERESSATO

2.1. INTRODUZIONE E PRINCIPI GENERALI.

Art 12-23, 28 e 34, Considerando 67 GDPR

L'Interessato può rivolgersi direttamente al Titolare del trattamento per l'esercizio dei suoi diritti (interpello).

Capitale sociale € 3.538.100,00 i.v. – Registro Ditte/REA n° 229672 – Registro Imprese di Modena n° 01604300366
Iscrizione Registro Nazionale Produttori A.E.E. n. IT08020000003645
Partita IVA e Codice Fiscale 01604300366 – Identification Number IT 01604300366

Ciascun Responsabile del Trattamento[1] è tenuto a collaborare col Titolare ai fini dell'esercizio dei diritti dell'Interessato.
In caso di mancata risposta, o di risposta inadeguata, l'Interessato può rivolgersi all'Autorità amministrativa (Garante della Privacy) o giudiziaria competente per la tutela dei suoi diritti.
Il termine per la risposta è di 1 mese per tutti i diritti.
Tale termine può essere esteso a 3 mesi in casi di particolare complessità. In questo caso il Titolare del Trattamento deve comunque avvertire l'Interessato entro il termine di 1 mese. L'esercizio dei diritti è in linea di massima gratuito[2].
La risposta si deve fornire di regola in forma scritta, anche attraverso strumenti elettronici e deve essere chiara, coincisa, e facilmente accessibile e comprensibile.
Il Titolare può chiedere informazioni all'Interessato al fine di identificarlo e l'Interessato è obbligato a fornire tali informazioni.

2.1.1. Diritto di accesso (art. 15 del GDPR)

Il diritto di accesso è il diritto riconosciuto all'Interessato di essere informato quali dei suoi Dati Personali il Titolare sta trattando, con quali finalità (non le modalità invece), per quale periodo, con quali criteri di gestione automatizzata[3] e di ricevere una copia (gratuita) dei Dati. Viene prevista, come modalità di attuazione di questo diritto, che i Titolari possano eventualmente anche consentire un accesso diretto ai Dati Personali da remoto.

2.1.2. Diritto di rettifica (art. 16 del GDPR)

[1] Art. 28, comma 3 lett. e) del GDPR.
[2] Spetta comunque al titolare, secondo il principio di accountability, valutare se la risposta è complessa al punto da dover chiedere un contributo all'interessato, e stabilirne l'ammontare, ma solo se si tratta di richieste manifestamente infondate o eccessive o ripetitive (cfr. delibera del 2004 - *Contributo spese in caso di esercizio dei diritti dell'interessato*).
[3] L'Interessato ha il diritto di conoscere: - le finalità del trattamento; - le categorie di dati personali trattate; - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali, e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi;- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; - 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; - l'esistenza del diritto di proporre reclamo a un'autorità di controllo; - qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Capitale sociale € 3.538.100,00 i.v. – Registro Ditte/REA n° 229672 – Registro Imprese di Modena n° 01604300366
Iscrizione Registro Nazionale Produttori A.E.E. n. IT08020000003645
Partita IVA e Codice Fiscale 01604300366 – Identification Number IT 01604300366

Il diritto di rettifica è il diritto riconosciuto all''Interessato di ottenere dal Titolare del Trattamento senza ritardo la correzione, l'integrazione e la modifica dei propri Dati Personali quando gli stessi risultino errati, non aggiornati o insufficienti – al fine di garantire all'Interessato un controllo costante e attivo sui propri Dati Personali e sull'utilizzo che ne viene fatto.

2.1.3. Diritto alla cancellazione (art. 17 del GDPR)

L'Interessato ha il diritto di ottenere dal Titolare del Trattamento la cancellazione dei Dati Personali che lo riguardano nei seguenti casi:
a) i Dati Personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'Interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, par. 1, a), o all'articolo 9, par.2, a) del GDPR e non sussiste altro fondamento giuridico per il trattamento (cioè non esiste un obbligo di legge o di contratto che comporti direttamente o indirettamente la conservazione dei Dati);
c) l'Interessato si oppone al Trattamento ai sensi dell'articolo 21 (par. 1 e 2) del GDPR e non sussiste alcun motivo legittimo prevalente per procedere al Trattamento;
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 GDPR.
Il Titolare del Trattamento, se ha reso pubblici Dati Personali ed è obbligato, ai sensi del paragrafo 1 dell'art. 17 del GDPR, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i Titolari del Trattamento che stanno trattando i Dati Personali della richiesta dell'Interessato di cancellare qualsiasi link, copia o riproduzione dei suoi Dati Personali.
Il diritto alla cancellazione trova un limite quando il Trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il Trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del Trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

2.1.4. Diritto di limitazione del trattamento (art. 18 del GDPR)

Il diritto di limitazione del Trattamento rappresenta una versione più articolata del diritto di cancellazione di cui al precedente paragrafo.
L'Interessato ha la possibilità di pretendere una limitazione dell'uso che il Titolare fa dei propri Dati Personali nei casi elencati dall'art. 18 del GDPR.
Qualora l'Interessato contesti l'esattezza dei Dati Personali, per tutto il tempo tecnico necessario al fine di verificare l'esattezza dei Dati oggetto di contestazione, il Trattamento sarà "congelato". All'esito della verifica di esattezza dei Dati Personali, il Titolare del Trattamento agirà correggendo o integrando i Dati Personali dell'Interessato.
L'Interessato può chiedere la limitazione del Trattamento quando il Trattamento sia illecito e l'Interessato si opponga alla loro cancellazione, preferendo che ne sia disposta una limitazione d'utilizzo, oppure quando il Titolare non abbia più bisogno di conservare i dati ai fini del Trattamento ma essi siano necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, infine, quando l'Interessato si sia opposto al Trattamento nell'attesa delle necessarie verifiche sulla prevalenza dei motivi legittimi del Titolare del Trattamento rispetto a quelli dell'Interessato.
In queste ipotesi, i Dati dell'Interessato potranno essere trattati solo ai fini della loro conservazione, a meno che vi sia il consenso dell'Interessato o il Trattamento sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti di un'altra persona o per ragioni di interesse pubblico rilevante.
Il dato deve essere contrassegnato in attesa delle ulteriori valutazioni.

2.1.5. Diritto alla portabilità (art. 20 del GDPR)

Il diritto alla portabilità dei Dati è il diritto riconosciuto all'Interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati Personali che lo riguardano forniti a un determinato Titolare del Trattamento e di

trasmetterli o chiederne la trasmissione ad 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 prestato per finalità specifiche (ex art. 6, par 1, a), o art. 9, paragrafo 2, lettera a) del GDPR),

b) il Trattamento è necessario per l'esecuzione di un contratto o di attività precontrattuali (ex art.6, par 1, b del GDPR); e

c) il Trattamento sia effettuato con mezzi automatizzati.

2.1.6. Diritto di opposizione (art. 21 del GDPR)

Il diritto di opposizione è il diritto dell'Interessato di opporsi in qualsiasi momento, e per motivi connessi alla sua situazione particolare, al Trattamento dei Dati Personali che lo riguardano. Conseguenza dell'esercizio di tale diritto è l'obbligo, in capo al Titolare, di astenersi dal Trattamento.
Questo diritto riguarda però situazioni in cui il Titolare sta lecitamente trattando dei Dati Personali: pertanto, è riconosciuta la facoltà per il Titolare di dimostrare che i suoi interessi specifici connessi al Trattamento prevalgono su quelli evidenziati dall'Interessato.
Inoltre e in particolare, nel caso in cui i Dati Personali siano trattati con finalità di marketing diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento e gratuitamente al Trattamento, anche (e soprattutto) nel caso in cui questo avvenga mediante attività di profilazione.

3. DIFFUSIONE DELLA CONSAPEVOLEZZA IN MATERIA

L'esercizio dei diritti dell'Interessato è uno degli aspetti della normativa in tema di data privacy, nella gestione del quale ogni persona che lavora (come dipendente o collaboratore o componente degli organi societari) per Medica s.p.a. può essere coinvolta, in particolare nella primissima fase, di ricezione di una Richiesta da parte di un Interessato.

È quindi importante che il contenuto di questa Policy sia reso noto a tutto il personale (dipendenti e collaboratori) che lavora per Medica s.p.a.

A questo fine, l'Amministrazione di Medica s.p.a. deve provvedere a quanto segue.

1. Inserimento della presente *Policy*, al pari di ogni altra *policy* rilevante in materia di privacy nella documentazione che accompagna il contratto di

lavoro con i dipendenti di Medica s.p.a. ed i contratti di collaborazione con Medica s.p.a.

2. Diffusione della presente Policy presso Medica s.p.a., al pari di ogni altra *policy* rilevante in materia di privacy, accompagnata da possibili iniziative di formazione ai dipendenti e collaboratori con i quali si sia già formalizzato un contratto di lavoro o collaborazione;

3. Inserimento della presente *Policy*, al pari di ogni altra *policy* rilevante in materia di privacy nel sito di Medica s.p.a. al seguente indirizzo https://www.medica.it/chi-siamo/privacy-policy .

4. GESTIONE DELLA RICHIESTA

4.1. Principi generali per la gestione della Richiesta

La presente *Policy* è diretta a definire una procedura che garantisca:

(i) l'effettivo esercizio dei diritti dell'Interessato da parte di coloro che ne facessero richiesta, nei tempi previsti dalla legge;

(ii) una procedura chiara al fine di evitare ritardi e minimizzare il coinvolgimento di risorse non necessarie;

(iii) la minimizzazione dei Dati trattati nella procedura interna, diretta a dare risposta all''Interessato;

(iv) il rispetto delle previsioni del GDPR, che nel rafforzare la tutela di diritti dell'Interessato già noti, tiene anche conto della necessità di contenere Richieste pretestuose e ripetitive dirette a finalità diverse dall'esercizio dei diritti garantiti dal GDPR all'Interessato.

4.2. Canale Abilitato per l'esercizio dei diritti dell'Interessato

Al fine di garantire una gestione uniforme delle Richieste da parte degli Interessati, l'esercizio dei diritti dell'Interessato deve avvenire per iscritto attraverso un unico canale abilitato a ricevere le Richieste di esercizio dei diritti provenienti dagli Interessati (di seguito, "**Canale Abilitato**"), definito nel presente paragrafo.

Le Richieste concernenti l'esercizio dei diritti dell'Interessato dovranno pervenire al Titolare in forma scritta[4]:

(i) all'indirizzo e-mail privacy@medica.it;

(ii) oppure mediante raccomandata a/r all'indirizzo segnalato dal Titolare.

Il personale di Medica s.p.a. quale Responsabile del Trattamento, deve mettere a disposizione dell'Interessato, sia verbalmente sia per iscritto:

(i) i dati di contatto del Titolare;
(ii) chiarire che, l'esercizio dei diritti dell'Interessato avviene esclusivamente attraverso il Canale Abilitato, definito appositamente al fine di dare all'Interessato un riscontro celere e di garantire la tutela di tutti Dati Personali di cui Medica s.p.a. è Titolare, anche a fronte di Richieste fittizie – e quindi a beneficio degli Interessati stessi;
(iii) fornire all'Interessato ogni istruzione necessaria affinché possa esercitare i propri diritti attraverso il Canale Abilitato;
(iv) mettere a disposizione dell'Interessato che lo richieda il formulario per agevolare l'inoltro della Richiesta, specificando che l'utilizzo è suggerito ma non obbligatorio.

4.3. Analisi della Richiesta

L'Ufficio Legale di Medica s.p.a. effettua l'analisi della Richiesta.

3.3.1. Accertamento preliminare dell'identità dell'Interessato richiedente

Entro 3 giorni dalla Ricezione della Richiesta, l'Ufficio Legale di Medica s.p.a. provvede alla verifica dell'effettiva legittimazione dell'Interessato richiedente, controllandone l'identità.

Nota: questa verifica preliminare dell'identità dell'Interessato richiedente è una fase indispensabile all'evasione di qualsiasi Richiesta, in quanto è vietata la comunicazione di Dati a soggetti diversi dagli Interessati o dai titolari della responsabilità genitoriale in caso di figli minori (rappresentando ciò una violazione dei Dati Personali).

[4] La forma scritta si deve ritenere l'unica adeguata a fini di prova, chiarezza e tutela dei Diritti dell'Interessato, ed il questo senso il Titolare ha diritto a prendere in considerazione Richieste che provengano esclusivamente in forma scritta.

Capitale sociale € 3.538.100,00 i.v. – Registro Ditte/REA n° 229672 – Registro Imprese di Modena n° 01604300366
Iscrizione Registro Nazionale Produttori A.E.E. n. IT08020000003645
Partita IVA e Codice Fiscale 01604300366 – Identification Number IT 01604300366

L'accertamento deve avvenire sulla base del principio di ragionevolezza, per cui si riterrà soddisfatto nel caso in cui:

i. venga prodotta copia della carta d'identità dell'Interessato, nonché,

ii. nel caso in cui la Richiesta provenga da un legale, copia della procura.

L'Ufficio Legale di Medica s.p.a. ha la facoltà di richiedere ulteriori chiarimenti ed informazioni in merito all'Interessato ed eventualmente al suo legale, lasciandone traccia scritta, qualora ciò appaia necessario a valutare l'effettiva identità dell'Interessato richiedente.

Qualora la verifica di cui al presente paragrafo avesse esito negativo, il Dipartimento Legal risponderà all'Interessato ed eventualmente al suo legale, per iscritto che non è possibile procedere, invitandoli a chiarire la legittimazione del presunto Interessato in relazione alla Richiesta.

Qualora la verifica avesse esito positivo, si procederà invece con l'analisi di merito della Richiesta.

3.3.2. Analisi della Richiesta e riscontro all'Interessato

Entro 5 giorni dal momento in cui la fase preliminare di verifica della identità dell'Interessato abbia avuto esito positivo, l'Ufficio Legale di Medica s.p.a. esprimerà una valutazione in merito alla complessità della Richiesta.

Richiesta particolarmente complessa. Qualora la Richiesta presenti aspetti di complessità tali da richiedere un termine superiore al termine di 1 (un) mese, l'Ufficio Legale di Medica s.p.a. informa immediatamente di ciò l'Interessato ed eventualmente il suo legale, specificando le ragioni per cui è necessario un ulteriore periodo per dare riscontro alla Richiesta dell'Interessato.

Richiesta standard. Qualora l'Ufficio Legale di Medica s.p.a. ritenga che la Richiesta non presenti particolari aspetti di complessità, si procede alla gestione della Richiesta come "Richiesta standard".

Entro 5 giorni dalla valutazione dell'Ufficio Legale di Medica s.p.a. sulla complessità di cui sopra, lo stesso Ufficio consultando, laddove necessario, i Responsabili esterni coinvolti:

(i) provvede ad un'analisi della fondatezza giuridica della Richiesta; e, in esito a questa valutazione,

(ii) invia senza ritardo una prima versione della risposta da dare all'Interessato (**"Draft di Replica"**). Il Draft di Replica è un documento ad uso interno che deve essere inviato a tutti i soggetti che, nella loro qualità di soggetti Incaricati/Autorizzati al Trattamento ovvero Responsabili, sono coinvolti nell'adozione delle misure che rendono effettivo l'esercizio dei propri diritti da parte dell'Interessato.

Il Draft di Replica contiene:

a) in caso di valutazione negativa della fondatezza di una o più delle Richieste dell'Interessato, le ragioni per cui non è possibile dare seguito alla Richieste dell'Interessato;

b) in caso di valutazione positiva della fondatezza di una o più delle Richieste dell'Interessato, la specificazione delle misure da adottare in merito ai Dati Personali dell'Interessato.

Il Draft di Replica avrà valore di istruzione vincolante per tutti i soggetti che, nella loro qualità di soggetti Incaricati/Autorizzati al Trattamento ovvero Responsabili, sono coinvolti nell'adozione delle misure che rendono effettivo l'esercizio dei propri diritti da parte dell'Interessato.

Entro 2 giorni dalla ricezione, ciascuno dei soggetti coinvolti dovrà dare riscontro dell'avvenuta adozione delle misure indicate.

Il Dipartimento Legale, una volta acquisiti i riscontri necessari, in merito al fatto che tutte le misure indicate l'adozione di tutte le azioni necessarie è stata portata a termine, inoltrerà senza ritardo all'Interessato ed eventualmente al suo legale una risposta (**"Replica all'Interessato"**)[5].

La Replica all'Interessato contiene:

i. una spiegazione dettagliata delle ragioni per cui una o più delle Richieste dell'Interessato non sono accettabili – e/o

[5] Con riferimento alle Richieste particolarmente complesse, il Dipartimento Legal sentita la FLU stabilisce un calendario per l'evasione della Richiesta dell'Interessato in modo tale da consentire:
1. Che il Draft di Replica sia inviato ai soggetti coinvolti almeno un mese prima della scadenza del termine prolungato di tre mesi;
2. Che sia possibile raccolgiere tutti i riscontri da parte dei soggetti coinvolti almeno 10 giorni prima della scadenza del termine per la replica all'interessato.

ii. la dichiarazione che una o più delle sue Richieste sono state ritenute fondate e la conferma che a tali Richieste si è dato seguito, allegando laddove sia possibile, evidenza di quanto affermato[6].

Il Dipartimento Legal tiene inoltre un Registro delle Richieste come da template C allegato alla presente *Policy* per verificare lo storico delle Richieste degli Interessati e i relativi profili di rilevanza/criticità.

4. ALLEGATI

Allegato A - template di risposta a Richiesta pervenuta a Medica s.p.a. tramite il servizio postale

Allegato B - template di risposta a Richiesta pervenuta a Medica s.p.a. tramite e-mail

Allegato C – template di Registro delle Richieste

Allegato D – artt. 12-23, 28 e 34, Considerando 67 GDPR.

[6] L'art. 34 del GDPR stabilise che quando la violazione della sicurezza dei Dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve darne notizia all'Interessato senza ingiustificato ritardo. La norma fissa i requisiti di contenuto della comunicazione, che deve essere redatta con un linguaggio semplice e chiaro. Altresì la norma individua i casi in cui la detta comunicazione non è richiesta (per semplicità, quando il Titolare ha adottato misure tali da scongiurare il rischio o quando la comunicazione richiederebbe sforzi sproporzionati. Ne deriva che quest'obbligo previsto all'art. 34 del GDPR configura in modo corrispondente un diritto in capo all'Interessato.