

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

REDATTO	
Luigi Rufo, Bruno Manno	
VERIFICATO	
Direttore Sanitario	Francesca Bellini
Direttore Amministrativo	Tito Berti
Qualità e accreditamento	Stefania Gianassi
APPROVATO	Nome
Direttore Generale	Alberto Zanobini

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

SOMMARIO

I.	INTRODUZIONE.....	3
A.	SCOPO	3
B.	CAMPO DI APPLICAZIONE.....	3
C.	DOCUMENTI DI RIFERIMENTO	3
D.	GLOSSARIO E ACRONIMI	3
II.	IDENTIFICAZIONE DEL RICHIEDENTE.....	5
III.	IDENTIFICAZIONE DELLA RICHIESTA.....	6
A.	RICHIESTA DI ACCESSO EX ART. 15 GDPR	6
B.	RICHIESTA DI RETTIFICA EX ART. 16 GDPR	6
C.	RICHIESTA DI CANCELLAZIONE-OBLIO EX ART. 17 GDPR	7
D.	RICHIESTA DI LIMITAZIONE DI TRATTAMENTO EX ART. 18 GDPR.....	7
E.	RICHIESTA DI REVOCA DEL CONSENSO EX ART. 7 GDPR	8
F.	RICHIESTA DI OPPOSIZIONE AL TRATTAMENTO EX ART. 21 GDPR	8
G.	RICHIESTA DI PORTABILITÀ DEI DATI EX ART. 20 GDPR.....	9
H.	DECISIONI BASATE SU UN PROCESSO DECISIONALE AUTOMATIZZATO EX ART. 22 GDPR.....	9
IV.	PRESA IN CARICO E LAVORAZIONE DELLA RICHIESTA.....	9
V.	TERMINE PER DARE RISCONTRO	9
VI.	MODALITÀ PER RICONTRARE LA RICHIESTA.....	10
VII.	COSTI DI RISCONTRO	10

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

INTRODUZIONE

SCOPO

La presente procedura ha lo scopo di fornire indicazioni pratiche con riferimento alle richieste finalizzate all'esercizio dei diritti da parte degli Interessati ex artt. 15-22 GDPR.

È possibile inviare le proprie istanze con raccomanda A/R

Ufficio Privacy - Azienda Ospedaliero Universitaria Meyer, Viale Pieraccini 24 50139 - Firenze

oppure via mail a

privacy.dpo@meyer.it

CAMPO DI APPLICAZIONE

La presente procedura si applica per la gestione e riscontro alle istanze degli interessati.

DOCUMENTI DI RIFERIMENTO

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

GLOSSARIO E ACRONIMI

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

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;


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 Particolari: Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

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;


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

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

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati 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 dell'azienda e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete Aziendale 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; nonché (c) 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;

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

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;

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;

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.

IDENTIFICAZIONE DEL RICHIEDENTE

Il Titolare del trattamento deve verificare l'identità del richiedente. È infatti possibile che la richiesta possa essere presentata sia dall'Interessato in nome proprio, sia da un terzo in nome e per conto dell'Interessato.

Se la richiesta proviene:

- **Dall'interessato in nome proprio:** il Titolare verifica l'identità dell'Interessato sulla base di idonei elementi di valutazione, quali, ad esempio, la conoscenza personale o l'attestazione da parte di terzi o mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. In caso di richiesta proveniente via e-mail o posta ordinaria, se l'attività richiesta implica azioni che il Titolare può portare a termine in autonomia (ad esempio: fornire l'indicazione dei Responsabili che hanno accesso ai Dati Personali), l'identificazione dell'Interessato dovrà avvenire

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

richiedendo o confrontando idonei elementi. A tale scopo, (salvo il caso summenzionato della richiesta via PEC) il mero confronto tra nome, cognome e indirizzo email non è considerato sufficiente. Dovrà pertanto essere richiesto all'Interessato di inviare via e-mail o via fax una copia del proprio documento di riconoscimento per risolvere la richiesta in backoffice.

- **Da un terzo per conto dell'Interessato:** il Titolare verifica che il terzo alleggi copia della procura, ovvero della delega sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'Interessato.

Qualora il Titolare del trattamento avesse dubbi sulla documentazione allegata o da allegare, sarà opportuno richiedere l'assistenza di un legale o di consulenti esterni in materia di privacy.

IDENTIFICAZIONE DELLA RICHIESTA

RICHIESTA DI ACCESSO EX ART. 15 GDPR

A mezzo dell'esercizio del diritto di accesso ex art. 15 GDPR, l'Interessato ha il diritto di ottenere la conferma che sia o meno in corso un Trattamento di Dati Personali che lo riguardano e se del caso, il Titolare deve fornirgli l'accesso in forma intellegibile e comunicargli le informazioni di cui all'art. 15 GDPR.

Se il Trattamento consiste in una notevole quantità di informazioni che riguardano l'Interessato, prima di fornire le informazioni, la Funzione Competente deve tempestivamente contattare, con gli stessi strumenti con cui riceve la richiesta l'Interessato per chiedergli di precisare le informazioni o le attività di Trattamento a cui si riferisce la sua richiesta di accesso.

RICHIESTA DI RETTIFICA EX ART. 16 GDPR


In tal caso, l'Interessato ha il diritto di ottenere la correzione/rettifica dei Dati Personali inesatti.

Se possibile, e se non implica uno sforzo sproporzionato, il Titolare del trattamento deve comunicare la rettifica/integrazione a ciascun Destinatario cui ha comunicato i Dati Personali entro 15 giorni attraverso uno dei seguenti mezzi:

- Posta elettronica con notifica di ricezione
- Raccomandata a/r

Una volta proceduto alla rettifica o alla integrazione dei Dati Personali autonomamente è necessario tempestivamente e comunque non oltre 30 giorni comunicare le modifiche all'Interessato per:

- Posta elettronica con notifica di ricezione
- Raccomandata a/r

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

Il Titolare del Trattamento, salvo che ciò non implichi uno sforzo proporzionato, deve tempestivamente informare via PEC della richiesta di rettifica, tutti gli altri Destinatari cui sono stati comunicati i Dati Personali oggetto di richiesta ex art. 16 GDPR.

RICHIESTA DI CANCELLAZIONE-OBLIO EX ART. 17 GDPR

L'Interessato ha il diritto di richiedere e di ottenere la cancellazione dei Dati Personali o la loro trasformazione in forma anonima purché effettuata con tecniche che garantiscano l'impossibilità di re-identificazione.

Il Titolare del trattamento, previa valutazione della sussistenza dei presupposti e condizioni di cui all'art. 17.1 GDPR, considerate le tecnologie disponibili e i costi, e salvo che ciò non implichi uno sforzo proporzionato, deve:

- tempestivamente informare via PEC (o altro mezzo idoneo a dimostrare la ricezione) della richiesta di cancellazione tutti i Destinatari cui sono stati comunicati i Dati Personali - invitandoli a procedere a loro volta alla cancellazione;
- in caso i Dati Personali siano stati diffusi/ resi pubblici - (per esempio pubblicati sul sito web dell'azienda), adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento, qualora noti, che stanno trattando i Dati Personali, della richiesta dell'interessato di cancellare qualsiasi link ai dati stessi come anche di qualsiasi copia o riproduzione.

La cancellazione dei dati deve avvenire in maniera definitiva da tutti i sistemi informativi aziendali.

Eseguita la richiesta di cancellazione-oblio dei Dati Personali, il Titolare lo comunica all'interessato.


RICHIESTA DI LIMITAZIONE DI TRATTAMENTO EX ART. 18 GDPR

La richiesta da parte dell'Interessato di limitazione di Trattamento ex art. 18 GDPR comporta, ad esclusione della conservazione, il divieto di qualsiasi tipo di trattamento del Dato Personale oggetto di richiesta salvo non ricorrano le seguenti circostanze:

- consenso dell'Interessato
- accertamento dei diritti in sede giudiziaria
- tutela dei diritti di altra persona fisica o giuridica
- interesse pubblico rilevante

Se nessuna di queste condizioni si verifica, la Funzione Competente procede alla limitazione di Trattamento, informando l'Interessato.

Successivamente, in vista dell'imminente scadenza del vincolo di limitazione del Trattamento dei Dati Personali oggetto di richiesta, la Funzione Competente informa l'Interessato - via PEC o lettera raccomandata a/r - della revoca del vincolo,

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

Il Titolare del trattamento, salvo che ciò non implichi uno sforzo proporzionato, deve tempestivamente informare via PEC della richiesta di limitazione e della cessazione di tale limitazione, tutti i Destinatari cui sono stati comunicati i Dati Personali oggetto di richiesta ex art. 18 GDPR.

RICHIESTA DI REVOCA DEL CONSENSO EX ART. 17 GDPR

L'Interessato può richiedere in ogni momento senza motivazioni la revoca del Consenso prestato; a seguito della richiesta di revoca, i Dati Personali oggetto dell'esercizio del diritto devono essere cancellati o in alternativa anonimizzati ex art. 17.1 GDPR, salvo non sia presente un'ulteriore base giuridica che legittima la prosecuzione del Trattamento dei dati (es. assolvere ad un obbligo di legge).

RICHIESTA DI OPPOSIZIONE AL TRATTAMENTO EX ART. 21 GDPR

L'Interessato può esercitare il diritto di opposizione al trattamento dei propri Dati Personali, inclusa la Profilazione, se:

- il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento;
- il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare del Trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei Dati Personali, in particolare se l'Interessato è un minore. ^[1]_[5EP]


In tali casi la richiesta di opposizione deve essere motivata e può essere rifiutata dal Titolare se:

- dimostra l'esistenza di motivi legittimi cogenti per procedere al Trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato;
- il Trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Al di fuori di queste ipotesi il Titolare si astiene dal Trattare ulteriormente i Dati Personali.

- Qualora i Dati Personali siano Trattati per finalità di marketing diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al Trattamento dei Dati Personali che lo riguardano effettuato per tali finalità, compresa la Profilazione nella misura in cui sia connessa a tale marketing diretto. La richiesta non deve essere motivata e l'opposizione non può essere rifiutata.
- In caso di trattamento per finalità di ricerca scientifica o storica o per finalità statistica la richiesta di opposizione che proviene dall'Interessato deve essere motivata e può essere rifiutata solo nel caso in cui il Trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

L'esercizio del diritto di opposizione ha come effetto la cessazione in maniera definitiva e permanente del Trattamento con la cancellazione o l'Anonimizzazione dei dati ex art. 17.1, salvo non si applichi una delle eccezioni di rifiuto più sopra.

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

RICHIESTA DI PORTABILITÀ DEI DATI EX ART. 20 GDPR

In caso di Trattamento automatizzato, la richiesta da parte dell'Interessato di portabilità ex art. 20 GDPR comporta che il Titolare debba fornire allo stesso in un formato strutturato e di uso comune e leggibile da un dispositivo automatico i Dati Personali che lo riguardano da lui forniti. I dati "forniti" devono comprendere anche quelli forniti in conseguenza dell'uso di un servizio o di un dispositivo. Possono ad esempio comprendere lo storico delle ricerche su Internet, dati di traffico o dati di localizzazione; o ancora, dati grezzi prodotti da un dispositivo di rilevazione del battito cardiaco (es.: un braccialetto).

Se l'Interessato lo richiede espressamente, i suddetti dati devono essere direttamente trasmessi ad altro Titolare del Trattamento da lui indicato, se tecnicamente fattibile.

DECISIONI BASATE SU UN PROCESSO DECISIONALE AUTOMATIZZATO EX ART. 22 GDPR

Se l'Interessato è sottoposto a decisioni basate unicamente su un Trattamento automatizzato, compresa la Profilazione, che produce effetti giuridici che lo riguardano o che incide in modo analogo significativamente sulla sua persona, ove l'Interessato lo richieda il Titolare deve comunicare all'interessato la logica applicata al Trattamento e le decisioni che sono prese in esito alla Profilazione o al Trattamento automatizzato.

Il Titolare deve concedere all'Interessato la possibilità di un intervento umano, e/o di esprimere la propria opinione e/o di contestare la sua decisione.


PRESA IN CARICO E LAVORAZIONE DELLA RICHIESTA

Il Titolare del trattamento per ottemperare alla richiesta, si confronta via e-mail con il personale in grado di fornire supporto e, se del caso, con consulenti esterni all'azienda. Tutte le comunicazioni devono essere inviate sempre anche per conoscenza al titolare.

TERMINE PER DARE RISCONTRO

Il Titolare del trattamento deve dare riscontro alla richiesta di esercizio dei diritti in oggetto all'Interessato:

- **entro il termine di un mese dal ricevimento della richiesta,**
- fornendo adeguate motivazioni, in caso di particolare complessità, entro **tre mesi** dal ricevimento della richiesta (art. 12.3; c. 59 GDPR) previo tempestivo (entro un mese dal ricevimento della richiesta) preavviso all'Interessato della proroga.
- In caso di diniego, la Funzione Competente informa l'Interessato **senza ritardo e al più tardi entro un mese dal ricevimento della richiesta**, indicando:
 - ✓ i motivi del diniego;
 - ✓ la possibilità di proporre reclamo all'Autorità di Controllo (Garante per la Protezione dei Dati Personali);
 - ✓ la possibilità di proporre ricorso giurisdizionale.

	Linee guida diritti interessato	CODICE
	MEYER	All.17 AZI056 rev.0 Data 13/05/2020

In caso di richieste manifestamente infondate o eccessive o ripetitive ex art. 12.5 GDPR, il Titolare del trattamento può rifiutarsi di soddisfare la richiesta. In tal caso, deve dare riscontro all'Interessato del diniego entro un mese dal ricevimento della stessa.

MODALITÀ PER RISCONTRARE LA RICHIESTA

La risposta fornita all'Interessato deve essere intellegibile, concisa, trasparente e facilmente accessibile, e deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua con cui l'Interessato rivolge la richiesta.

- Le comunicazioni di cui agli art. 15-22 GDPR devono essere fornite in forma scritta ed in linea generale a mezzo di lettera raccomandata a/r;
- se l'interessato presenta la richiesta mediante e-mail o posta elettronica certificata PEC, le informazioni devono essere fornite attraverso i medesimi strumenti elettronici, salvo diversa indicazione da parte dell'Interessato;
- solo se richiesto espressamente dall'Interessato, le informazioni vengono fornite oralmente.

Nel caso di esercizio del diritto di accesso, il Titolare fornisce gratuitamente all'Interessato una copia dei Dati Personali oggetto di Trattamento salvo che ciò non leda:

- il diritto altrui;
- le libertà altrui;
- segreto industriale e/o aziendale;
- proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software.

L'azienda deve documentare ogni richiesta ex art. 15-22 GDPR in un registro generale delle richieste di esercizio dei diritti ex art. 15-22, in cui deve documentare l'evasione delle richieste. Del registro deve avere cura la Funzione Competente sotto la supervisione del Titolare.

Il registro deve contenere:

- identificativo dell'Interessato;
- dati di contatto dell'Interessato;
- richiesta e data in cui si viene a conoscenza della stessa;
- data di evasione della richiesta;
- sintesi del relativo riscontro.

COSTI DI RISCONTRO

L'esercizio dei diritti è gratuito per l'Interessato ad eccezione dei seguenti casi, in cui l'azienda può addebitare all'Interessato un contributo spese ragionevole basato sui costi amministrativi:

- richieste manifestamente infondate o eccessive o ripetitive ex art. 12.5 GDPR;
- richieste di più copie su supporto fisico (ottico o cartaceo ecc..) dei Dati Personali nel caso di accesso ex art. 15.3 GDPR.