A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi-Cotugno-CTO
NAPOLI

ALL. B

Azienda Ospedaliera Specialistica "dei Colli"
e.p.c. al
Responsabile per la Protezione Dati

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a _____ nato/a _____il __/__/____
C.F. _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ in qualità di **interessato**:

ESERCITA

con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

- ☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
- ☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;
  - 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;
  - il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di rettifica

(artt. 16 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni:

☐ rettifica e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679) *(specificare quali):*

_____
_____
_____
_____

3. Richiesta di cancellazione

(artt. 17 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni:

☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quale tipologia di dati e per quali motivi)*:

a)_____
_____
_____;

b)_____
_____
_____;

c)_____
_____
_____;

☐ nel caso in cui il titolare del trattamento abbia reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, 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 riproduzioni dei suoi dati personali.

4. Richiesta di limitazione

(artt. 18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni:

- ☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ contesta l'esattezza dei dati personali;
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

5. Richiesta di notifica ai destinatari dei dati trattati afferenti l'Interessato

(artt. 19 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni:

- ☐ notificare ai destinatari dei dati trattati da parte del titolare per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ rettifica;
  - ☐ cancellazione;
  - ☐ limitazione.

6. Portabilità dei dati[1]

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare in base al consenso ex art. 6, par. 1, lett. a), e art. 9, par. 2, lett. a), o su un contratto ex art. 6, par. 1, lett. b), e trattati attraverso mezzi automatizzati, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

[1] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

☐ trasmettere direttamente al seguente diverso titolare del trattamento

(specificare i riferimenti identificativi e di contatto del titolare

*Titolare*_____*:*

*Indirizzo e P.I.*_____

*Dati di contatto*_____

*Nazione*_____*Rappresentante nell'Unione:*_____

☐ tutti i dati personali forniti al titolare;

☐ un sottoinsieme di tali dati.

☐ La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

7. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi:

_____

_____

_____

_____

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale. *(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)*

8. Richiesta di non sottoposizione a processi decisionali automatizzati

(artt. 22 del Regolamento (UE) 2016/679)

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi-Cotugno-CTO
NAPOLI

ALL. B

Il sottoscritto chiede di:

- ☐ non essere sottoposto ad un processo decisionale automatizzato compresa la profilazione
- ☐ ottenere conferma che non è in corso un trattamento automatizzato sui dati personali forniti

---

Il sottoscritto:

- ☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.
- ☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[2]: NOME_____COGNOME_____

Via/Piazza_____
Comune_____Provincia_____Codice postale_____

oppure

PEC: _____

Lì:_____ Data:__/__/____

L'Interessato

_____

[2] Allegare copia di un documento di riconoscimento

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi-Cotugno-CTO
NAPOLI

ALL. B

_____SPAZIO RISERVATO AL PROTOCOLLO GENERALE_____

TIPOLOGIA DI RICHIESTA/E

☐ ACCESSO ☐ CANCELLAZIONE ☐ PORTABILITÀ ☐ RETTIFICA ☐ NOTIFICA

☐ OPPOSIZIONE ☐ LIMITAZIONE ☐ PROCESSI DECISIONALI AUTOMATIZZATI

Ai sensi dell'art. 38 del D.P.R. 445/2000, la presente dichiarazione è stata:

☐ Sottoscritta, previa identificazione del richiedente, in presenza del dipendente addetto

☐ Sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore

SE LA DOMANDA È STATA PRESENTATA DAL PROCURATORE
È STATO IDENTIFICATO TRAMITE
☐ DOCUMENTO ☐ PROCURA

RICHIESTA DA EVADERE ENTRO[3] *(3O giorni dalla richiesta)*:
NOTIFICA ALL'INTERESSATO ENTRO *(3O giorni dalla richiesta):*

[3] La richiesta può prevedere un tempo maggiore di evasione, la notifica contenente tale termine che non può eccedere i 90 giorni dalla richiesta deve essere inviata all'interessato entro il termine perentorio di 30 giorni

Procedura per la Gestione dei diritti dell'Interessato

Indice delle Tabelle

1 INTRODUZIONE

Il Regolamento UE 2016/679 (di seguito GDPR o Regolamento) nasce con lo scopo di tutelare i dati personali delle persone fisiche. Il Regolamento sostituisce completamente quanto sancito nel decreto legislativo 196/2003 – detto anche codice privacy – che, pur non venendo abrogato, viene integralmente adeguato a quanto stabilito dal GDPR. Tra i punti cardine sanciti dal Regolamento vi è la mancanza di indicazioni mandatorie per i Titolari e i Responsabili sulle misure di sicurezza da adottare al fine di garantire la tutela nel trattamento dei dati. Con l'eliminazione dell'allegato B (DPS – Documento Programmatico per la Sicurezza) del Codice del 2003 il Regolamento ha sancito che le misure di sicurezza fossero stabilite scientemente dal Titolare e/o dal Responsabile secondo le proprie esigenze, attraverso la valutazione dei rischi che i loro trattamenti comportavano. Con tale abrogazione, infatti, il Regolamento ha teso evitare adempimenti onerosi per quei Titolari che svolgevano trattamenti di dati personali limitati. Inoltre, nel Regolamento vengono descritte non solo le attività cui fanno capo il Titolare del trattamento e il Responsabile del Trattamento, ma anche gli approcci omogenei sulla tutela dei diritti dell'Interessato attraverso il trattamento dei dati personali direttamente o indirettamente a questi riconducibili, favorendo la circolazione libera e sicura delle informazioni all'interno dell'Unione Europea. Gli enti pubblici afferenti al Servizio Sanitario Nazionale (SSN), per la criticità dei servizi erogati al cittadino e la sensibilità dei dati personali trattati, sono tenuti alla scrupolosa applicazione del regolamento, che indirizza gli adempimenti cogenti ed i principi guida per la tutela dei diritti dell'Interessato nel trattamento dei dati a questi riconducibili. Infine, l'integrale ribaltamento della responsabilità in capo al titolare, fa sì che debba dimostrarsi "compliant" con il Regolamento, ciò significa che i trattamenti posti in essere da quest'ultimo dovranno essere leciti, corretti, trasparenti e raccolti per finalità determinate esplicite e legittime. È la cosiddetta "*accountability*".

1.1 SCOPO DEL DOCUMENTO

Scopo del presente documento è descrivere il processo e le modalità operative adottate nel complesso di strutture facenti capo alla **Azienda Ospedaliera Specialistica dei Colli** per la gestione dell'esercizio dei diritti, riconosciuti dal Regolamento, da parte degli interessati.

Secondo quanto stabilito dal Regolamento, l'interessato ha un insieme di diritti che possono essere esercitati per tutelare i propri dati personali. Scopo intrinseco del Regolamento è quello di equiparare la tutela dei dati personali ai diritti fondamentali, come anche sanciti dalla nostra costituzione, quali il diritto al lavoro, il diritto al libero pensiero o alla salute. Al capo III del Regolamento, quindi, troviamo le sezioni dedicate ai **diritti dell'interessato**. Considerando il diritto all'informazione completa e trasparente (artt. 12-14) un adempimento necessario ed obbligatorio ricadente sul titolare ed il responsabile del trattamento e l'art. 77 riguardante il diritto di proporre reclamo all'Autorità di Controllo, sono gli articoli rubricati dal 15 al 22 che stabiliscono, nel concreto, quali diritti l'interessato può **esercitare**.

Questo documento si inquadra, quindi, nell'insieme delle misure organizzative e procedurali disposte dal Titolare del trattamento, finalizzate all'indirizzamento e alla regolamentazione dei processi interni alla

struttura sanitaria, dedicati alla tutela dei diritti dell'interessato, in ottemperanza al principio di responsabilizzazione ("accountability") del Titolare.

1.2 AMBITO DI APPLICAZIONE

La procedura operativa si applica, nello specifico, a tutto il personale dell'Azienda Ospedaliera che tratta a qualsiasi titolo e in qualsiasi modalità (digitale, cartacea, etc.) dati personali, ai responsabili del trattamento e, ove applicabile, alle terze parti che operano per conto della A.O. dei Colli.

Il presente paragrafo contiene la lista dei documenti di riferimento afferenti alla Struttura Sanitaria.

[1] Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR)

[2] D.Lgs 196/2003 "Codice in materia di protezione dei dati personali" così come novellato dal D. Lgs. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle prescrizioni del Regolamento UE/679/2016

[3] Garante Privacy: Linee guida in materia di dossier sanitario – 4 giugno 2015

[4] Garante Privacy: Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019 [docweb: 9091942]

[5] Legge 241/1990 sul diritto di accesso ai documenti amministrativi

[6] Legge 33/2013 sulla trasparenza

[7] Delibera aziendale n.258/2018 Azienda Ospedaliera "dei Colli"

[8] Decreto Ministeriale Sanità 14.02.1997 [referti ecografici, referti medicina nucleare]

[9] Circolare 61 del 19.12.1986 Ministero della Sanità [cartelle cliniche]

[10] Linee guida sul diritto alla portabilità dei dati WP 242 rev. 01, versione emendata 5 aprile 2017

1.3 DEFINIZIONI

Termine	Descrizione
Interessato ex art. 4	La persona fisica a cui si riferiscono i dati personali oggetto del trattamento
Titolare del Trattamento ex art. 4	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** per il trattamento dei dati personali
Delegato interno al Trattamento dati	Soggetto intermo all'Amministrazione, formalmente individuato, cui il Titolare attribuisce compiti e funzioni specificamente individuati nell'ambito delle operazioni di trattamento effettuate nell'ambito della struttura di diretta competenza.
Incaricati ex art. 4	Soggetti incaricati dal titolare del trattamento facenti capo a quest'ultimo direttamente o indirettamente all'interno della struttura organizzativa aziendale
Dato Personale ex art 4	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 ad un identificativo come il nome, id online e ad uno degli elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica ed economica
Dato Genetico ex art. 4	Il dato personale relativo alle caratteristiche genetico-ereditarie di una persona fisica che rappresentano informazioni univoche sulla fisiologia o sulla salute di detta persona fisica
Dato Biometrico ex art. 4	Il dato personale ottenuto da un trattamento tecnico specifico relativo a caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consente o conferma l'identificazione
Dati relativi alla salute ex art. 4	Il dato personale attinente alla salute fisica e mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rilevano informazioni relative al suo stato di salute
Trattamento ex art. 4	Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

Termine	Descrizione
Responsabile del Trattamento ex art. 4	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo esterno all'azienda, che tratta i dati personali **per conto** del titolare del trattamento
Informazione ex art. 4	Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento dei dati, alle finalità e alla base giuridica su cui si fonda il trattamento
Accesso (art. 15)	L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali ed in particolare alle informazioni relative alle finalità ai destinatari, al periodo di conservazione.
Rettifica (art. 16)	L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti.
Oblio (art. 17)	L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nei casi previsti dalla norma
Minimizzazione/Limitazione (art. 18)	L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorrono determinate ipotesi specificamente dettagliate dalla norma
Notifica (art. 19)	Il titolare ha l'obbligo di comunicare ai soggetti a cui ha trasmesso i dati personali dell'interessato di aver effettato attività' di rettifica, cancellazione o limitazione per conto dell'interessato
Portabilità (art. 20)	L'interessato ha il diritto di ricevere in formato strutturato, di uso comune e leggibile dal dispositivo automatico i dati personali che lo riguardano raccolti attraverso il consenso dell'interessato
Opposizione (art. 21)	L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano quando la base giuridica di cui all'art. 6 si fonda sulle lett. e) o f) compresa la profilazione
Processo decisionale automatizzato (art. 22)	L'interessato ha il diritto di non essere sottoposto a una 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
Limitazioni ex art. 23	Il diritto dell'unione può limitare, mediante misure legislative, la portata degli obblighi e dei diritti previsti dagli artt. da 12 a 22 e 34 per salvaguardare interessi specificamente disciplinati dalla norma qualora tale limitazione

Termine	Descrizione
	rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria per salvaguardare la sicurezza nazionale, la sicurezza pubblica, la difesa […]
DPO ex art. 37	Data Protection Officer – è il soggetto nominato dal Titolare del Trattamento svolge attività di consulenza e controllo sulle attività del trattamento di quest'ultimo. La figura del DPO funge da punto di contatto tra il Titolare del Trattamento e l'Autorità di Controllo
Autorità di Controllo ex art. 4	È il Garante per la Protezione dei Dati Personali al quale l'interessato può rivolgersi attraverso lo strumento del ricorso ex art. 77 del GDPR in caso quest'ultimo ritenga che il Titolare stia svolgendo un trattamento in contrasto con il Regolamento
Data Breach ex art. 33	È la violazione dei dati personali suscettibile di rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche
PEC	La **P**osta **E**lettronica **C**ertificata è un servizio di posta elettronica a valore legale utilizzabile come valida, economica e più immediata alternativa alla raccomandata A/R come strumento di comunicazione tra privati e tra privati e la pubblica amministrazione. L'utenza viene rilasciata da un ente di certificazione riconosciuto da AgID
Protocollo Informatico	Sistema di protocollo informatico in uso presso l'Azienda Ospedaliera Specialistica dei Colli per le comunicazioni tra gli uffici
Registro dei Trattamenti	Registro in cui il titolare descrive tutte le attività di trattamento svolte sotto la propria responsabilità
Pseudonimizzazione ex art. 4	Il processo attraverso il quale i dati personali non possano più essere associati o attribuiti all'interessato senza l'utilizzo di informazioni aggiuntive, a condizioni che queste informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati non siano attribuiti o attribuibili ad una persona fisica identificata o identificabile
Profilazione ex art. 4	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per la valutazione e lo scoring di determinati aspetti personali quali ad esempio interessi, preferenze personali, ubicazione, comportamento, situazione economica e salute

Tabella 1 – Definizioni

2 OVERVIEW DEL PROCESSO

Il processo di gestione delle richieste di esercizio dei diritti dell'interessato ha come obiettivo quello di indirizzare quanto previsto dal Regolamento così come indicato al punto 2.1. In particolare, il presente documento descrive il processo e le modalità operative adottate presso l'A.O.R.N. dei Colli per governare:

- Acquisizione delle richieste di esercizio dei diritti;
- Valutazione preliminare della UOC Privacy - DPO;
- Decisione finale del Titolare del Trattamento sulla richiesta;
- Richiesta di intervento al Responsabile (UOC/UOSD) competente;
- Evasione della richiesta;
- Riscontro all'interessato.

2.1 DIRITTI ESERCITABILI DALL'INTERESSATO

Con la presente procedura, l'Azienda Ospedaliera Specialistica dei Colli, in qualità di Titolare del trattamento dispone l'attuazione delle misure organizzative e procedurali che assicurino la corretta informazione e comunicazione, nonché una tempestiva risposta alle richieste dell'Interessato nei casi previsti dal GDPR.

Di seguito sono enunciati i principi che normano l'esercizio dei diritti dell'Interessato da parte della struttura sanitaria, secondo le modalità descritte nel seguito del presente documento:

- Diritto di accesso (art. 15);
- Diritto di rettifica (art. 16);
- Diritto alla cancellazione (art. 17);
- Diritto di limitazione del trattamento (art. 18);
- Obbligo di notifica (art. 19);
- Diritto alla portabilità dei dati (art. 20);
- Diritto di opposizione al trattamento (art. 21);
- Diritto di non essere sottoposto a processi decisionali o di profilazione automatizzata (art.22).

Le comunicazioni con l'interessato che esercita i propri diritti riguardanti il trattamento dei dati personali, avvengono secondo le modalità definite al paragrafo "**Allegato A**. **Modalità di comunicazione con l'interessato**" del presente documento.

2.2 RUOLI E RESPONSABILITA'

RUOLO	RESPONSABILITA'
Richiedente (Interessato)	La persona fisica i cui dati sono oggetto del trattamento da parte del Titolare che, in costanza di trattamento, esercita uno dei diritti di cui agli artt. 15-22 del GDPR secondo le modalità stabilite dalla struttura. Esercita i diritti di cui agli articoli 15-22 e controlla la correttezza e la conformità dei risultati rispetto alla richiesta.
URP – Ufficio Relazioni con il Pubblico	È l'interfaccia tra l'Azienda Ospedaliera Specialistica dei Colli e l'interessato. Fornisce all'interessato la documentazione e le informazioni necessarie al fine di consentire l'esercizio dei diritti di cui al paragrafo **"Diritti esercitabili dall'interessato",** indicando l'ufficio del Protocollo Generale come unico ufficio competente all'accettazione ed evasione delle richieste riguardanti l'esercizio dei diritti dell'interessato (ex GDPR).
Direzione Generale	È l'ufficio responsabile della procedura per l'esercizio dei diritti dell'interessato (ex. GDPR). Supervisiona e monitora il processo. Smisterà la richiesta alla UOC Privacy, Trasparenza e Integrità – DPO per la valutazione preliminare della richiesta. Conferma ed invia la risposta elaborata dal Responsabile UOC/UOSD di competenza attraverso il Protocollo Generale.
Protocollo Generale	Verifica l'identità e/o la ricezione delle richieste di esercizio dei diritti da parte dell'interessato e/o del delegato, occupandosi di protocollare e smistare le stesse mediante il sistema di protocollo in uso presso la struttura sanitaria. È responsabile di tutte le comunicazioni che intercorrono tra l'ente e l'interessato.
Comitato Tecnico Privacy	È il gruppo di lavoro costituito attraverso la delibera n.258 del 2018 ed ai sensi dell'art.39 dell'Atto Aziendale .
UOC Privacy, Trasparenza e Integrità - DPO	È l'ufficio a cui fa capo il DPO. Collabora con il DPO alla valutazione preliminare e nell''esprimere un parere non vincolante, riguardo le richieste di esercizio dei diritti dell'interessato. Individua il Responsabile della UOC/UOSD competente all'evasione della richiesta inviando copia alla Direzione Generale.
UOC Affari Legali	È l'ufficio di supporto alla gestione dei diritti dell'interessato (ex delibera 258/2018). Si occupa di coadiuvare il DPO e l'ufficio UOC Privacy, Trasparenza e Integrità nelle attività di valutazione e gestione delle richieste di esercizio dei diritti dell'interessato.
Delegato Interno al trattamento dati personali (Responsabile della UOC/UOSD	È il responsabile della Unità Operativa Complessa o della Unità Operativa Semplice Dipartimentale competente che evade - o individua il soggetto competente ad evadere - le richieste pervenute dalla Direzione Generale. Predispone ed elabora il riscontro finale che invia alla Direzione Generale per la conferma ed invio all'interessato.

RUOLO	RESPONSABILITA'
competente)	
Soggetto incaricato	Evade materialmente, quando possibile, la richiesta. Elabora ed invia la stessa alla Direzione Generale, con in copia l'ufficio del DPO, per il riscontro finale all'interessato.

Tabella 2 – Ruoli e Responsabilità

3 DESCRIZIONE DEL PROCESSO

Nel presente capitolo sono descritte le attività di processo tramite rappresentazione grafica dei flussi (flow-chart). I simboli utilizzati nel flow-chart, con una breve descrizione degli stessi, sono illustrati nella seguente tabella:

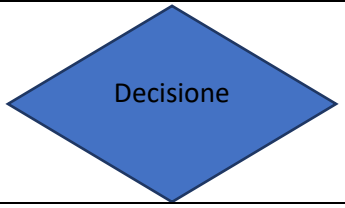
Simbolo	Denominazione	Descrizione
	Inizio	Rappresenta l'inizio del processo.
	Attività	Rappresenta la singola attività attuata, identificata da: • dal numero della Fase di riferimento (i.e. 1.1)
	Decisione	Rappresenta un momento decisionale.
	Linee di flusso	Connette le attività fra di loro indicando il flusso delle informazioni.
	Fine	Rappresenta la fine del processo.

Tabella 3 – Legenda Flow-chart

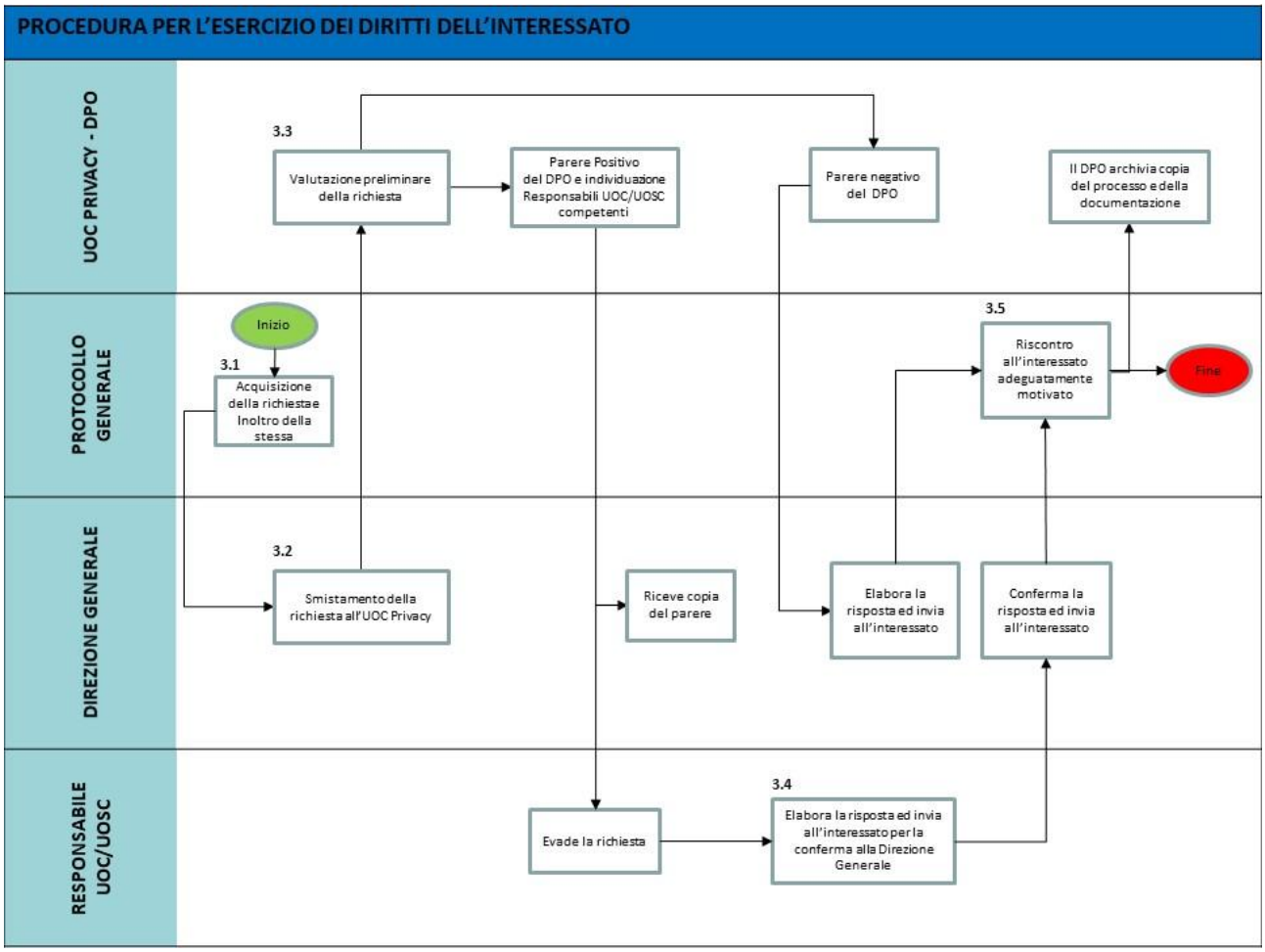


Tabella 4 – Flow-chart

3.1 Acquisizione delle richieste

L'Interessato invia le richieste di esercizio dei propri diritti utilizzando canali di comunicazione cartacea oppure elettronica.

Per garantire un'acquisizione più omogenea, la Struttura adotta il "**Modulo unico per le richieste dell'interessato**" fornito in allegato B, siano esse spedite tramite PEC, raccomandata A/R o presentate *de visu*. La Struttura garantirà l'acquisizione delle richieste pervenute anche in forma "libera".

Le richieste in forma cartacea sono inviate a mezzo raccomandata A/R ovvero consegnate a mano dall'interessato presso il Protocollo Generale.

Le richieste in forma elettronica sono inviate tramite Posta Elettronica Certificata all'indirizzo PEC del Protocollo Generale, utilizzando l'apposito modulo per l'esercizio dei diritti di cui "**Allegato B. Modulo unico per le richieste dell'interessato"** del presente documento messo a disposizione dalla struttura anche attraverso il sito istituzionale dell'Azienda Ospedaliera.

La richiesta via PEC deve essere fatta dall'interessato per l'interessato. Si intende quindi che la domanda deve essere inviata da un indirizzo di posta elettronica certificata, di cui l'interessato è l'intestatario. Eccezion fatta se la richiesta è presentata da un procuratore legale.

Al fine di rendere i canali di comunicazione sicuri ed efficienti, non è prevista la ricezione di richieste tramite e-mail semplice relativamente alle comunicazioni tra gli utenti e l'Azienda Ospedaliera.

L'acquisizione della domanda in data certa consente alla struttura di gestire la ricerca documentale/informativa e far seguire la risposta all'interessato nei tempi previsti e descritti in questo documento.

Al fine di una corretta tracciabilità dei tempi di risposta, stabiliti per legge, non sono accettati altri canali di ricezione delle richieste, all'infuori di quelli sopra indicati. Inoltre, per specifica previsione, essendo l'URP il primo punto di contatto con il pubblico, sarà l'URP ad indicare al pubblico le specifiche istruzioni per formulare la richiesta tramite il canale corretto.

Laddove la domanda venga consegnata direttamente al Protocollo Generale, l'interessato dovrà essere identificato dal personale mediante presentazione di un documento di riconoscimento in corso di validità.

Nel caso di presentazione della domanda attraverso un altro soggetto, questi dovrà essere identificato mediante un documento di riconoscimento in corso di validità, il personale dovrà inoltre controllare la corrispondenza dei dati oggetto della richiesta ed il documento di riconoscimento dell'interessato richiedente.

Qualora l'esito della verifica dell'identità risulti positivo, le richieste sono protocollate e smistate, attraverso il protocollo informatico, alla Direzione Generale lo stesso giorno.

3.2 Smistamento della richiesta all'Ufficio Privacy - DPO

La Direzione Generale provvederà, tenendo conto che la risposta finale deve essere per Regolamento GDPR fornita entro 30gg dalla data certa di ricezione della richiesta dell'interessato, a smistare la richiesta all'UOC

Privacy – DPO per la valutazione preliminare della stessa e l'individuazione del Responsabile della UOC/UOSD competente per l'evasione della richiesta.

3.3 Valutazione preliminare della richiesta

L'ufficio Privacy a cui fa capo il DPO, ricevuta la richiesta protocollata, tenendo conto che la risposta finale deve essere per Regolamento GDPR fornita entro 30gg dalla data certa di ricezione della richiesta dell'interessato, collabora alla valutazione preliminare e a rendere il parere comunque non vincolante. Potrà avvalersi del Comitato Tecnico Privacy e dell'Ufficio Affari Legali per la valutazione del caso. Il parere verrà allegato alla richiesta originaria ed insieme saranno inviati al Responsabile della UOC/UOSD competente per l'evasione della richiesta inviando una copia alla Direzione Generale.

La Direzione Generale, considerato il parere non vincolante del DPO e la risposta elaborata dal responsabile UOC/UOSD - tenendo conto che la risposta finale deve essere, per Regolamento GDPR, fornita entro 30gg dalla data certa di ricezione della richiesta dell'interessato - assumerà la decisione circa la prosecuzione del procedimento.

Nel caso in cui la Direzione Generale non ammetta la richiesta, predisporrà la risposta e la invierà all'interessato a mezzo PEC – o comunque tramite il canale prescelto dall'interessato – attraverso il Protocollo Generale.

Nel caso in cui vi siano richieste complesse che richiedano tempi lunghi di elaborazione e che impediscano l'adempimento del Titolare nei tempi stabiliti, l'interessato deve essere informato relativamente ad un eventuale allungamento dei tempi di risposta di due mesi, rispetto ai termini di legge di **30**gg dalla richiesta, dovuto ad eccessiva onerosità/complessità della richiesta stessa (ex art. 12 comma 3 GDPR).

3.4 Evasione della richiesta

Il Responsabile della UOC/UOSD competente per la tipologia di richiesta, procede ad individuare il soggetto da incaricare per l'evasione della richiesta. Pertanto, in base al diritto esercitato, il soggetto incaricato provvederà a processare la richiesta dandone riscontro al Responsabile della UOC/UOSC competente il quale inoltrerà alla Direzione Generale e alla UOC Privacy la comunicazione, adeguatamente predisposta, da inviare all'interessato.

Le attività necessarie per processare la richiesta devono esser svolte tenendo conto che la risposta finale deve essere, per Regolamento GDPR fornita entro 30gg dalla data certa di ricezione della richiesta dell'interessato.

Una volta processata la richiesta il Responsabile della UOC/UOSD competente, tenendo conto che la risposta finale deve essere, per Regolamento GDPR fornita entro 30gg dalla data certa di ricezione della richiesta dell'interessato, trasmette alla Direzione Generale e alla UOC Privacy la risposta elaborata da confermare ed inviare all'interessato.

3.5 Riscontro all'interessato

La Direzione Generale, ricevuta la comunicazione dal Responsabile della UOC/UOSD competente, trasmetterà la stessa all'interessato attraverso il Protocollo Generale per il riscontro finale tenendo conto

che la risposta finale deve essere, per Regolamento GDPR fornita entro 30gg dalla data certa di ricezione della richiesta dell'interessato nella modalità definita secondo i criteri descritti in **"Allegato A – Modalità di comunicazione con l'interessato".**

La comunicazione è eseguita dal Protocollo Generale a seconda del canale di risposta indicato dall'interessato al momento della richiesta originaria (PEC o Raccomandata).

Il Protocollo Generale conferma l'invio o il rilascio della documentazione all'interessato inviando copia della stessa al DPO (UOC Privacy, Trasparenza ed Integrità) che procederà all'archiviazione della richiesta stessa in un repository centralizzato per eventuali verifiche ed interrogazioni successive.

Potrebbero essere previsti dei costi per l'interessato se i dati dovranno necessariamente essere inseriti su supporto informatico (i.e. i record non stampabili con chiarezza su pdf e che devono necessariamente essere "aperti" attraverso un supporto informatico).

Registrazione e conservazione delle evidenze relative alle attività svolte

Le attività di processo devono prevedere l'utilizzo di un repository centralizzato in cui vengano conservate le evidenze di ogni attività eseguita nella gestione delle richieste dell'interessato già debitamente registrate dal DPO (UOC Privacy, Trasparenza ed Integrità) e protocollate univocamente dal Protocollo Generale. La conservazione delle richieste e risposte all'interessato è prevista, a norma di legge, per la durata di 10 anni. Superato questo termine, la richiesta e tutta la documentazione ad essa collegata potrà essere cancellata e definitivamente distrutta ad eccezione delle richieste ricevute attraverso l'Autorità Giudiziaria che non avranno limitazione temporale in termini di conservazione.

Allegato A – Modalità di comunicazione con l'interessato

Durante l'espletamento delle attività afferenti l'esercizio dei diritti dell'interessato, le comunicazioni con la struttura sanitaria devono rispettare le seguenti modalità:

a) **comunicazioni verbali** telefoniche con la "URP (Ufficio Relazioni con il Pubblico)", limitatamente al rilascio di informazioni generiche sulle modalità di esercizio dei diritti dell'Interessato, escludendo tassativamente la comunicazione di ogni altra tipologia di informazione. Fornisce il modulo per l'esercizio dei diritti ex GDPR.

b) **presso la sede** della struttura sanitaria per:

- La ricezione delle raccomandate, delle richieste in forma cartacea "libera" e consegnate a mano inerenti la richiesta di esercizio dei diritti dell'interessato;
- La ricezione delle richieste effettuate attraverso la compilazione del modulo messo a disposizione dalla struttura sanitaria previo accertamento dell'identità o dei requisiti di legittimità per la presentazione (procura);
- La consegna *brevi manu* della documentazione prodotta contenente le informazioni in formato cartaceo o su un supporto digitale, a seguito di formale richiesta e dell'eventuale pagamento delle spese di produzione e di cancelleria, previo accertamento dell'identità o dei requisiti di legittimità per la presentazione (procura); tale modalità prevede l'archiviazione di una ricevuta di consegna verso l'interessato;
- Ogni altra comunicazione verbale relativa anche a chiarimenti sui dati personali e sui trattamenti effettuati, previo appuntamento con la UOC Privacy, Trasparenza ed Integrità, a seguito di formale richiesta e previo accertamento dell'idoneità e dell'identità dell'interessato.

c) **tramite Posta Elettronica Certificata** proveniente dall'indirizzo PEC dell'interessato, o da un suo rappresentante a tale scopo delegato, relativamente a:

- Ricezione della richiesta;
- Eventuali comunicazioni di servizio, esclusivamente correlate alla richiesta di esercizio dei diritti dell'interessato preventivamente inoltrata come la necessità di prorogare il termine per l'eccessiva onerosità nell'espletamento della richiesta;
- Consegna in formato digitale, strutturato e intellegibile, delle informazioni richieste.

d) **tramite il Portale Istituzionale**, limitatamente alle comunicazioni unidirezionali tra l'interessato e la struttura sanitaria relative a:

- Acquisizione delle informazioni inerenti i diritti dell'interessato e sulle modalità di esercizio dei propri diritti;

- Download della modulistica predisposta dalla struttura sanitaria per agevolare l'interessato nell'esercizio di propri diritti (es. richieste di informazione/conoscenza, acquisizione, revoca di consenso al trattamento, rettifica, oscuramento e cancellazione.

Allegato B – Modulo unico per le richieste dell'interessato

esercizio diritti in materia di protezion

Allegato C – Limitazioni ai diritti esercitabili

Diritto di accesso

L'esercizio del diritto di accesso non si applica ai dati personali nei seguenti casi:

- Dati personali sanitari oggetto di prestazioni a pagamento che non risultino saldate al momento della richiesta di accesso;
- Dati personali di qualsiasi tipologia non più disponibili presso la struttura sanitaria a seguito di:
  - cessazione dei termini di custodia/archiviazione;
  - cessazione di utilità ai fini dei trattamenti in essere;
  - anonimizzazione dei riferimenti direttamente o indirettamente volti a rilevare l'identità dell'interessato.
- Il diritto di richiedere copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui (ex art. 15 par. 4)

Dati personali per i quali non è esercitabile il diritto di accesso, in base a specifiche norme di legge (e.g. dati riconducibili ai rapporti tra la struttura sanitaria e le Autorità Giudiziarie o di Polizia) ex art. 23 par. 2.

Diritto di rettifica e integrazione dei dati

L'esercizio del diritto di rettifica/integrazione non si applica ai dati personali relativi a:

- Dati sullo stato di salute riconducibili a prestazioni sanitarie;
- Dati anagrafici identificativi e di recapito acquisiti da fonti autoritative (es. anagrafe, anagrafe tributaria);

- Dati personali non più disponibili presso la struttura sanitaria a seguito di:
  - cessazione dei termini di custodia/archiviazione;
  - cessazione di utilità ai fini dei trattamenti in essere;
  - anonimizzazione dei riferimenti direttamente o indirettamente riconducibili all'interessato.

Diritto di cancellazione

L'esercizio del diritto di cancellazione/oscuramento dei dati personali non si applica nei seguenti casi:

- Dati personali sullo stato di salute raccolti e/o generati nell'erogazione dei servizi di sanità pubblica, ad eccezione di quelli riconducibili al dossier sanitario o a servizi simili;
- Dati personali di qualsiasi tipologia non più disponibili presso la struttura sanitaria a seguito di anonimizzazione dei riferimenti direttamente o indirettamente riconducibili all'interessato.
- Dati personali per i quali non è esercitabile il diritto di cancellazione/oscuramento, in base a specifiche norme di legge (es. dati riconducibili ai rapporti tra la struttura sanitaria e le Autorità Giudiziarie o di Polizia);
- Dati sanitari il cui trattamento è necessario ai fini di ricerca scientifica, storica o statistica;
- Dati sanitari trattati 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 del GDPR.

Diritto alla portabilità dei dati

L'esercizio del diritto di portabilità dei dati personali non si applica nei seguenti casi:

- Tutti i documenti contenenti dati personali conservati in archivi ed elenchi cartacei art. 20 par.1 lett. b);
- Tutti i dati personali che il Titolare del trattamento è tenuto a conservare e trattare in presenza e costanza di un interesse pubblico giuridicamente rilevante, obbligo di legge ovvero l'esecuzione di un dovere cui è tenuto il Titolare del trattamento ex art. 20 par. 3;
- Tutti i dati creati dal Titolare, detti "inferenziali", sulla base dei dati forniti dall'interessato ex art. 20;
- I dati oggetto del trattamento che non siano stati acquisiti mediante consenso dell'interessato (e.g. dati trattati in base ad obbligo di legge) ex art. 20 part. 1 lett. a).