



Fondazione IRCCS  
Policlinico San Matteo

Sistema Socio Sanitario



Regione  
Lombardia

DIPARTIMENTO AMMINISTRATIVO

S.C. GESTIONE ACQUISTI  
(PROVVEDITORATO - ECONOMATO)

Direttore  
Dott.ssa Olivia Piccinini

Tel. 0382 503983  
Fax 0382 503990

o.piccinini@smatteo.pv.it

**INDAGINE PER MANIFESTAZIONE DI INTERESSE EX ART. 50 COMMA 2 - ALLEGATO II.1 D.LGS. 31 MARZO 2023, N. 36  
PER L'AFFIDAMENTO DELL'INCARICO DI DATA PROTECTION OFFICER (DPO) E DEI SERVIZI DI CONSULENZA FINALIZZATI A  
GARANTIRE L'ADEGUAMENTO CONTINUO AL GDPR 679/2016.**

**DETTAGLI DEL SERVIZIO:**

Al DPO, quale responsabile della protezione dei dati, competono i seguenti compiti previsti dall'art. 39 del GDPR, di seguito specificati, compiti che dovranno essere integrati dai relativi servizi accessori:

- LETT. A\_ "informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati."

Rientrano in questo compito, a titolo indicativo ma non esaustivo, le seguenti attività:

- erogare consulenza in ambito normativo, giuridico e amministrativo in relazione alla gestione delle attività relative all'applicazione del GDPR;
- fornire indicazioni operative per il rispetto delle normative vigenti in materia di protezione dei dati personali;
- effettuare l'analisi delle problematiche inerenti all'applicazione della normativa (aspetti teorici e pratici);
- fornire al Team Privacy gli elementi utili per dare agli interessati un riscontro circa i diritti previsti dal GDPR;
- organizzare riunioni con il Titolare e i referenti interni coinvolti nell'attuazione delle misure di sicurezza al fine di fornire un allineamento sull'evoluzione normativa e sulle conseguenti implicazioni sul sistema di gestione privacy aziendale;
- effettuare l'analisi dell'assetto complessivo dell'Ente e la verifica della completezza e conformità agli adempimenti in materia di trattamento e sicurezza dei dati.

Servizi accessori correlati:

- supporto alla stesura, aggiornamento, implementazione, analisi della documentazione relativa al sistema aziendale privacy e alla relativa applicazione pratica nella gestione organizzativa;
- supporto fattivo per la predisposizione di atti aziendali;
- partecipazione fattiva per la predisposizione di Istruzioni Operative, Regolamenti aziendali, informative e qualunque altra documentazione ufficiale, necessaria all'assolvimento degli obblighi del Titolare del trattamento;
- guida e supporto del Team Privacy della Fondazione IRCCS;
- presenza in Fondazione IRCCS, a cadenza mensile, per guidare l'attività, per gestire casi specifici individuati ad hoc.

Si richiede altresì la presenza per procedere al recepimento degli aggiornamenti ed ai confronti necessari a dare piena attuazione al GDPR. Gli incontri, laddove concordato, potrebbero essere svolti anche da remoto.

- supporto nella gestione delle richieste pervenute all'Ufficio Privacy attraverso pareri scritti che diano indicazioni pratiche sulla loro esecuzione. Il DPO deve rispondere non oltre 3 giorni per i quesiti di alta complessità e non oltre 2 giorni per i quesiti a bassa/media complessità;
- aggiornamento mensile sulle nuove e principali disposizioni vincolanti che abbiano attinenza con la presente realtà ospedaliera: il Dpo deve fornire un piano di adeguamento con relativo supporto alla messa in pratica dello stesso;
- fornire il materiale documentale necessario ad una migliore e più efficace operatività nell'ambito delle attività richieste (materiali informativi, modulistica standard, bozze di atti, disponibilità di materiale informativo e divulgativo ecc.);
- fornire consulenza in materia di trattamento di dati personali, bilanciando la tematica della privacy con quella degli obblighi di pubblicità e di trasparenza delle Pubbliche Amministrazioni;

- effettuare un risk assessment e definire le politiche di sicurezza: attività di valutazione, individuazione dei rischi ed attuazione di tutte le misure adeguate per garantire e poter dimostrare che i trattamenti siano effettuati conformemente al GDPR;
  - promuovere la cultura della protezione dei dati all'interno dell'azienda dedicando almeno 20 ore per anno a formazione e momenti di incontro, in aula o "sul campo", con i soggetti individuati insieme al Team Privacy;
  - garantire la propria partecipazione nei casi in cui il Titolare coinvolga il DPO in questioni attinenti la protezione dei dati, sin dalla fase di progettazione di dette attività e comunque garantire la propria pronta reperibilità con le modalità specificate nel piano di lavoro;
  - correlarsi direttamente con la Direzione Strategica, ovvero con l'Ufficio Privacy, riguardo alle indicazioni/raccomandazioni fornite nel quadro delle proprie funzioni e fornire alla Direzione Strategica della Fondazione IRCCS un report attestante il livello di conformità al GDPR;
  - redigere una relazione annuale delle attività svolte da sottoporre alla Direzione Strategica;
  - assistere il team Privacy nella definizione delle procedure e delle misure di sicurezza da adottare per il trasferimento dei dati in Paesi terzi (extra UE).
  - riferire al Direttore Generale della Fondazione IRCCS per tutte le questioni o le decisioni strategiche o ritenute comunque di rilevante importanza o al Referente dell'Ufficio Privacy della Fondazione IRCCS per la definizione degli aspetti più operativi.
  - il DPO, al fine di poter essere contattato in modo semplice e diretto, oltre che dal Titolare e dai suoi dipendenti, dall'Autorità di controllo e dagli interessati, dovrà mettere a disposizione mezzi idonei e sicuri di comunicazione che consentano un contatto tempestivo, e in ogni caso dovrà mettere a disposizione almeno una linea telefonica e una casella di posta elettronica dedicate.
  - per la gestione dei casi di violazione dei dati personali, il DPO supporta il Titolare per tutta la gestione del processo, dall'individuazione della violazione all'applicazione delle azioni di miglioramento.
  - il DPO, nell'esecuzione dei propri compiti, considera i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo, deve presentare un planning annuale che individui puntualmente le attività da realizzare, secondo una scala di priorità definita in funzione del grado di rischio e della relativa tempistica attuativa riferita alle scadenze normative da rispettare.
  - le analisi compiute dal DPO e le azioni correttive e/o migliorative proposte affinché la Fondazione IRCCS si adegui al GDPR ed altre normative applicabili devono risultare da documenti scritti.
  - nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
  - al termine del servizio, il DPO deve redigere una relazione finale sulle attività svolte e sulla attuale situazione in cui si trova la Fondazione IRCCS rispetto all'attuazione della normativa sulla protezione dei dati personali.
- LETT. B\_ "sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo."

Rientrano in questo compito, a titolo indicativo ma non esaustivo, le seguenti attività:

- raccolta di informazioni per mantenere costantemente aggiornato il Registro dei trattamenti di dati personali svolti dalla Fondazione IRCCS o di futura attivazione, anche attraverso l'esame di documenti aziendali ed il relativo confronto con il Referente Privacy della Fondazione IRCCS;
- analisi e aggiornamento costante dell'attuale modello organizzativo aziendale ("sistema privacy") e valutazione della sua conformità con il GDPR e con le altre disposizioni comunitarie e nazionali vigenti;
- analisi e verifica della conformità dei trattamenti effettuati rispetto alla designazione dei responsabili del trattamento, dei designati, delle persone autorizzate ("incaricati") al trattamento e degli amministratori di sistema, all'adeguatezza delle policy di sicurezza adottate e concretamente attuate, alle modalità di pubblicazione di dati e documenti contenenti dati personali effettuate dalla Fondazione IRCCS per le varie finalità previste dalla legge e alle procedure di gestione delle violazioni dei dati;

Servizi accessori correlati:

- il DPO deve coordinare l'attività di audit in tutte le sue fasi (pianificazione complessiva annuale/pianificazione nello specifico di ogni singola verifica/ esecuzione/redazione del verbale con l'indicazione delle azioni di miglioramento/supporto fattivo nell'applicare le azioni di miglioramento/follow up di problemi o miglioramenti rilevati),



garantendo la presenza in Fondazione IRCCS per un numero di giornate sufficienti all'esecuzione di almeno n. 2/3 audit all'anno oltre a quelli eventualmente necessari e non programmati;

- vagliare la corretta attuazione delle disposizioni contenute nel GDPR, occupandosi, in particolare di verificare che i sistemi, sin dalla fase della loro progettazione rispettino la privacy (privacy by design), verificare la protezione di default di dati e sistemi (privacy by default), rilevare che venga garantita la sicurezza nei trattamenti dei dati;
- elaborazione di procedure - anche informatiche - per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento dei dati personali;
- individuare le azioni correttive/migliorative tecniche ed organizzative atte a ridurre le criticità ed effettuare i correlati follow up.

- LETT. C\_ "fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR."

Rientrano in questo compito, a titolo indicativo ma non esaustivo, le seguenti attività:

- supportare il Titolare del trattamento nella figura del Referente Privacy e del relativo Team nell'individuazione dei casi in cui sia necessario effettuare la DPIA;
- fornire indicazioni necessarie, anche operative e metodologiche, per lo svolgimento delle DPIA e collaborare con il Referente Privacy e con il relativo team all'analisi delle DPIA;
- valutare la correttezza delle DPIA effettuate dal Titolare e verificare se le conclusioni raggiunte siano conformi con i requisiti in materia di protezione dei dati.
- esprimere un parere, positivo o negativo, con adeguata argomentazione per ciascuna DPIA, dall'argomentazione deve intuirsi l'iter logico adottato dal DPO nella redazione del parere.

Servizi accessori correlati:

- fornire i differenti format di DPIA adattati alle variegate esigenze e contesti della Fondazione IRCCS;
- valutare le azioni da applicare, comprese le misure tecniche ed organizzative, per eliminare/attenuare i rischi per i diritti delle persone interessate;
- riesaminare ciclicamente le DPIA effettuate e rilevare l'eventuale necessità di effettuare di ulteriori.

- LETT. D\_ "cooperare ed interagire con l'Autorità di controllo."

Rientrano in questo compito, a titolo indicativo ma non esaustivo, le seguenti attività:

- oltre che con l'Autorità di controllo il DPO dovrà collaborare e coordinarsi con i DPO eventualmente designati dai Responsabili del trattamento che trattano dati per conto della Fondazione IRCCS o con i DPO nominati dai Titolari per i quali la Fondazione IRCCS svolge il ruolo di Responsabile del trattamento, o con i DPO degli altri Contitolari.

Servizi accessori correlati:

- il DPO deve fornire supporto nell'elaborazione di memorie e di altri documenti funzionali ad un incontro col Garante Privacy o alla redazione di una risposta ai quesiti o ai provvedimenti provenienti dall'Autorità Garante.

- LETT. E\_ "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relative a qualunque altra questione."

Rientrano in questo compito, a titolo indicativo ma non esaustivo, le seguenti attività:

- il DPO, assieme al Titolare, deve inquadrare le casistiche di trattamento dati che necessitano di una consultazione preventiva (o qualsiasi altra consultazione) da parte dell'Autorità Garante;

Servizi accessori correlati:



- fornire supporto nell'elaborazione di memorie o altri documenti funzionali alla consultazione richiesta al Garante Privacy o a soddisfare eventuali ulteriori richieste documentali da parte dello stesso.
- fungere da punto di contatto per gli interessati coinvolti nel trattamento oggetto di consultazione, comunicando, per il tramite del Team Privacy, con gli interessati in modo efficiente e in conformità alle disposizioni normative;
- supportare il Titolare nella ricezione delle indicazioni del Garante e nella realizzazione di eventuali azioni correttive proposte.

Con riferimento all'oggetto, gli operatori economici interessati, dovranno caricare sul portale SINTEL entro le ore 16:00 del giorno 18/10/2024 nella sezione BUSTA UNICA quanto segue:

- Dichiarazione di interesse, su carta intestata, alla presentazione di un'offerta per l'affidamento del servizio in oggetto di cui alle caratteristiche indicate, **comprensiva pure dell'indicazione del CCNL applicato al personale dipendente impiegato nell'appalto.**

**SI PRECISA CHE NELLA DOCUMENTAZIONE DI CUI AI PUNTI PRECEDENTI NON DOVRANNO ESSERE INDICATI, IN NESSUN CASO, PROPOSTE/OFFERTE DI CARATTERE ECONOMICO.**

**NB:**

**Il portale chiede necessariamente di indicare un valore di carattere economico per completare la procedura, si prega, quindi, nello step dedicato di inserire il valore di € 1,00 = al fine procedere. DETTO VALORE NON SARA' IN NESSUN CASO CONSIDERATO.**

Si precisa, altresì, che eventuali valori relativi ai costi della sicurezza afferenti l'attività svolta dell'operatore economico, costi del personale e costi della sicurezza da interferenza, **SE RICHIESTI DALLA PIATTAFORMA ALL'ATTO DEL CARICAMENTO DELLA MANIFESTAZIONE DI INTERESSE,** dovranno essere inseriti per un valore pari a € 0,00 =.

**Si precisa, infine, che il presente avviso non presuppone la formazione di una graduatoria di merito o l'attribuzione di punteggi e non è impegnativo per la Fondazione la quale si riserva, in ogni caso e in qualsiasi momento, il diritto di sospendere, interrompere, modificare o cessare la presente consultazione.**

Il presente avviso ed ogni eventuale determinazione verrà revocata in caso di presenza dei dispositivi in oggetto nell'ambito di convenzioni ARIA attive.

Per ulteriori chiarimenti si prega di prendere contatti con: Dott.ssa Antonina Sottile tel. 0382-502379 – mail: a.sottile@smatteo.pv.it.

IL DIRETTORE  
DELLA S.C. GESTIONE ACQUISTI  
(PROVVEDITORATO - ECONOMATO)  
(Dr.ssa Olivia Piccinini)