

Allegato n. 2 COMPITI FUNZIONI E POTERI DEI REFERENTI PRIVACY

- a) Trattare i dati personali solo su istruzione del Titolare del trattamento o Suo delegato e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018, nonché la conformità alle indicazioni dell'Autorità Garante per la protezione dei dati personali.
- b) **Osservare e fare osservare:**
- le direttive aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento o Suo delegato, anche per il tramite del Gruppo Aziendale Privacy e del Servizio Sistemi Informativi Aziendale (*es. regolamento sull'utilizzo delle risorse informatiche, regolamento sul DSE, procedura data breach, etc.*);
 - le istruzioni di carattere generale impartite dal Titolare o Suo delegato a tutti i soggetti **autorizzati al trattamento**;
 - eventuali ulteriori specifiche istruzioni predisposte dallo stesso in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.
- c) Porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (*es. pazienti, dipendenti, fornitori etc.*) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt. 13 e 14 del GDPR.
- d) Provvedere alla designazione di soggetto autorizzato al trattamento dei dati personali dei singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, stagisti etc.), attraverso la predisposizione dell'apposito modello.
- e) Vigilare sulla conformità dell'operato dei soggetti autorizzati, ad essi afferenti, alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto.
- f) Verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati.
- g) Attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento o Suo delegato e, compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale.
- h) Partecipare ai momenti formativi organizzati dall'Istituto ed assicurare la partecipazione dei propri autorizzati.
- i) Fornire le informazioni richieste dal Gruppo Aziendale Privacy (GAP) e segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO.
- j) Comunicare al Gruppo Aziendale Privacy (GAP) i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale.
- k) Collaborare con il Gruppo Aziendale Privacy (GAP) per la predisposizione del documento della valutazione di impatto sulla protezione dei dati (DPIA) qualora ne ricorrano i presupposti in base all'art. 35 del GDPR.
- l) Non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento o Suo delegato.
- m) Provvedere, qualora tra le attività istituzionali dell'Istituto vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali **oggetti esterni quali "Responsabili del trattamento" a norma dell'art. 28 del GDPR** e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina al Gruppo Aziendale Privacy (GAP) anche ai fini dell'aggiornamento del registro aziendale delle attività di trattamento dei dati.
- n) Comunicare tempestivamente al Gruppo Aziendale Privacy (GAP) i **potenziali casi di data breach** all'interno della propria struttura e collaborare alla istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito, secondo le indicazioni contenute nell'apposita procedura aziendale di riferimento.

