REGOLAMENTO INTERNO

in materia di protezione dei dati personali

("Policy Privacy")

Documento approvato dal C.d.A. della Fondazione Sant'Erasmo in data 13 settembre 2019

Indice

1. Finalità e contenuto del documento

La finalità del presente documento è quella di descrivere i principi generali di sicurezza e gli obblighi di riservatezza delle informazioni e dei dati personali, che il titolare del trattamento garantisce ed assicura a tutti i soggetti coinvolti nell'ambito del trattamento dei dati, con l'intento di sviluppare un efficiente sistema di gestione delle procedure e dei processi per la sicurezza dei dati nel rispetto dei diritti e delle libertà fondamentali nonché della dignità delle persone fisiche, in ottemperanza al Regolamento UE 2016/679 (di seguito, "GDPR").

In particolare, tale "Policy Privacy" vuole costituire uno strumento fondamentale per potenziare nei soggetti adibiti al trattamento dei dati all'interno della struttura l'analisi e la consapevolezza dei rischi e delle insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati, oltre all'archivio cartaceo, al fine di prevenire e ridurre situazioni di pericolo, quali la perdita dei dati, l'accesso non autorizzato o il trattamento non consentito o non conforme.

Tale Regolamento interno contiene, nello specifico:

- la definizione dei principali ruoli, dei compiti e delle responsabilità in materia di protezione dei dati personali all'interno dell'Ente (il cosiddetto "Organigramma Privacy");
- i princìpi generali a protezione dei dati personali su cui è improntata l'attività della Fondazione Sant'Erasmo;
- l'individuazione delle norme comportamentali, delle procedure tecnico-organizzative e delle istruzioni operative per gli incaricati (o "autorizzati") del trattamento dei dati personali della Fondazione Sant'Erasmo, cui è necessario attenersi in materia di trattamento di dati personali e di sicurezza nello svolgimento delle mansioni lavorative e di tutte le attività dell'Ente, volte a garantire che i trattamenti di dati personali, svolti con o senza l'ausilio di strumenti elettronici, siano effettuati conformemente al GDPR, al D.Lgs n. 196/2003 ("*Codice della Privacy*"), nonché agli ulteriori provvedimenti in materia di fonte normativa secondaria, in vigore al momento dell'approvazione della seguente policy, anche con riferimento alle decisioni e ai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali;
- Le modalità di aggiornamento e/o revisione del documento.

La presente Policy Privacy è approvata dal Consiglio di Amministrazione su proposta del *Data Protection Officer* ("DPO") nominato dalla Fondazione Sant'Erasmo.

2. Ambito di applicazione

Il presente Regolamento si applica a tutte le persone fisiche che, nell'esercizio delle proprie mansioni e nell'ambito delle rispettive competenze, svolgono attività in qualità di "*incaricato / autorizzato del trattamento dei dati personali*" ai sensi dell'art. 28 del GDPR (personale dipendente, collaboratori, stagisti, ecc.), nonché ai soggetti, incluse le persone giuridiche, che, in qualità di "Responsabili esterni del trattamento", collaborano alla gestione delle informazioni e trattano, per conto del titolare del trattamento, dati personali di titolarità della Fondazione Sant'Erasmo.

Con riferimento all'ambito oggettivo, il regolamento si applica alle diverse attività che comportano il trattamento dei dati personali di titolarità dell'Ente (quali, ad esempio, attività connesse alla gestione del personale, attività connesse alla gestione dell'Ospite, adempimenti relativi ai rapporti contrattuali con i fornitori, ecc.), come puntualmente specificate all'interno del "Registro delle attività di trattamento" predisposto dal Titolare ai sensi dell'art. 30, paragrafo primo, del GDPR.

3. Definizioni

Ai fini della presente "*Policy Privacy*" si applicano le seguenti definizioni, in coerenza con le indicazioni contenute nella normativa di riferimento:

- "*trattamento di dati*", 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 (art. 4.2 del GDPR);

- "*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;

- "*dati identificativi*", i dati personali che permettono l'identificazione diretta dell'interessato;

- "*dati sensibili*", cioè quella "*categoria particolare di dati*" (art. 9 del GDPR) che, per sua natura, richiede particolari cautele durante un trattamento; sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di

altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute, la vita sessuale o l'orientamento sessuale della persona;

- "*dati giudiziari*", i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

- "*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 personali 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;

- *"titolare del trattamento*", 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;

- "*responsabile del trattamento*", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- "*incaricati*" (o "*autorizzati*"), le persone fisiche che, agendo sotto la responsabilità del Titolare e/o del Responsabile e, a tal fine, autorizzate dagli stessi, compiono le operazioni di trattamento dei dati personali, attenendosi alle istruzioni ricevute ed ai vincoli di riservatezza e confidenzialità;

- "*interessato*", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (in via esemplificativa, e non esaustiva, l'interessato può essere un cliente, un dipendente o un fornitore);

- "*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;

- "*Registro delle attività di trattamento*", documento previsto dall'art. 30 del GDPR con cui il Titolare o il Responsabile del trattamento specifica le finalità dei trattamenti effettuati, le tipologie di dati, le categorie di interessati e di destinatari dei dati,

nonché definisce le misure e gli standard di sicurezza in merito al trattamento dei dati;

- "*violazione dei dati personali*": 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;

- "*misure di sicurezza*", tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati sono raccolti;

- "*comunicazione*", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- "*diffusione*", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- "*Autorità Garante per la protezione dei dati personali*" (o "*Garante della Privacy*"), l'autorità amministrativa indipendente, istituita dalla legge n. 675 del 31 dicembre 1996, per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali;

- "*posta elettronica*", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino al momento in cui il ricevente non ne ha preso conoscenza;

- "*virus*": programma che infetta i *files* del computer inserendo copie di se stesso in tali *files*.

4. Riferimenti normativi

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato il Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (il cosiddetto "GDPR"). Tale

Regolamento è entrato in vigore il 25 Maggio 2016 ed è direttamente applicabile in tutta l'Unione Europea dal 25 Maggio 2018.

Il GDPR modifica in maniera rilevante la normativa in materia di "privacy", in quanto, nello specifico:

- armonizza la disciplina sulla protezione dei dati personali all'interno di tutta l'Unione Europea;
- attribuisce fondamentale importanza ai principi della *accountability*, della *privacy by design e by default*;
- coerentemente con il principio della *accountability,* introduce, gli istituti del Registro delle attività di trattamento, della valutazione d'impatto sulla protezione dei dati (DPIA) e della *data breach notification*;
- rafforza e introduce nuovi diritti degli interessati, che i titolari del trattamento sono tenuti a garantire al fine di assicurare che il trattamento dei dati personali sia svolto in piena conformità alla normativa, anche per incrementare il livello dei servizi forniti ai soggetti interessati;
- introduce la figura del Responsabile della Protezione dei Dati o *Data Protection Officer* (DPO).

Il contesto normativo di riferimento comprende, inoltre, l'ulteriore normativa primaria e secondaria in materia di "privacy" e protezione dei dati personali, in particolare il Decreto Legislativo 30 giugno 2003 n. 196 ("*Codice in materia di Protezione dei dati personali*"), i provvedimenti emanati dall'Autorità Garante della Protezione dei Dati, dalle Istituzioni europee e dal WP29, nonché le norme previste del codice civile e penale italiano.

5. Principi applicabili al trattamento dei dati

Il presente Regolamento si applica a tutti i trattamenti dei dati effettuati dalla Fondazione Sant'Erasmo, automatizzati o svolti manualmente, in cui la predetta agisce in qualità di Titolare del trattamento.

In particolare, nella pianificazione o nell'espletamento di qualsiasi attività, Fondazione Sant'Erasmo si impegna a garantire e a dimostrare che il trattamento dei dati avvenga in maniera conforme a quanto previsto dalla normativa italiana ed europea in materia di protezione dei dati e, in particolare, nel puntuale rispetto dei fondamentali principi enunciati all'art. 5 del GDPR:

- **Liceità**. Un trattamento è lecito solo se fondato su uno dei presupposti individuati dalla normativa. Per ogni trattamento effettuato all'interno della struttura dell'Ente è puntualmente individuata, all'interno del Registro delle attività di trattamenti ex art. 30 del GDPR, una specifica base giuridica. Inoltre, all'interno delle informative ex

art. 13-14 fornite agli interessati viene esplicitata la base giuridica inerenti i dati raccolti.

- **Trasparenza e correttezza**. Sono comunicate in maniera esplicita ai soggetti interessati le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali nonché la misura in cui tali dati sono o saranno trattati; inoltre le comunicazioni relative al trattamento dei dati personali sono, come richiesto dalla normativa, facilmente accessibili e comprensibili tramite l'utilizzo di un linguaggio semplice e chiaro.

- **Limitazione della finalità**. I dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non vi sia incompatibilità con tali finalità. Al fine di rispettare tale principio, il titolare del trattamento aggiornerà i moduli di informativa in conseguenza di eventuali modifiche al Registro delle attività di trattamento ex art. 30 del GDPR, nonché fornirà all'interessato il modulo dell'informativa aggiornato nel caso in cui dovesse utilizzare i dati personali per finalità diverse da quelle per cui essi sono stati raccolti.

- **Minimizzazione dei dati**. I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Al fine di rispettare tale principio l'Ente definisce ed implementa misure tecniche e organizzative adeguate al fine di garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

- **Esattezza**. I dati devono essere esatti e, se necessario, aggiornati; in tal senso Fondazione Sant'Erasmo ha previsto, al suo interno, procedure operative ed organizzative al fine di poter garantire tempestivamente il riscontro alle richieste degli interessati in relazione all'accesso, alla modifica o alla rettifica dei dati personali trattati. Tali diritti vengono indicati, in maniera esplicita e con chiarezza, nelle informative fornite agli interessati.

- **Limitazione della conservazione**. I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Fondazione Sant'Erasmo, con la consulenza del DPO, al fine di ottemperare ai principi inerenti la conservazione, prevede un adeguato processo finalizzato ad indicare, per ogni trattamento, le politiche di conservazione e gli interventi mirati per procedere alla corretta identificazione dell'interessato, alla cancellazione o all'anonimizzazione di tali dati. Gli interessati hanno il diritto di richiedere che i propri dati personali siano cancellati e non più sottoposti a trattamento qualora la conservazione di tali dati violi le norme previste.

- **Integrità e riservatezza**. I dati devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (accesso o utilizzo non autorizzato) e dalla perdita, dalla distruzione o dal danno anche solo accidentali. A tal proposito l'Ente garantisce che i dati non siano comunicati a soggetti che non abbiano la necessità lavorativa di venirne a conoscenza, secondo la regola in base alla quale ogni incaricato o soggetto autorizzato al trattamento può trattare solo i dati personali di competenza, necessari per il conseguimento delle rispettive finalità.

Il rispetto dei suddetti principi nonché la garanzia di protezione e di adozione di corrette misure di sicurezza è, inoltre, richiesta ai soggetti terzi che, in qualità di responsabili esterni, hanno assunto l'incarico della gestione di alcuni trattamenti per conto del Titolare.

6. Distribuzione dei compiti e delle responsabilità

Fondazione Sant'Erasmo, in qualità di Titolare del trattamento di dati personali, ha individuato la propria struttura interna di tutela della "privacy", implementando un sistema di nomine e distribuzione dei compiti e delle responsabilità (il cosiddetto "*Organigramma Privacy*") come di seguito delineate, al fine di garantire al meglio la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali.

6.1 Il titolare del trattamento dei dati. Ai sensi dell'art. 4 del GDPR, il titolare rappresenta la persona fisica o giuridica, che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Conformemente a quanto previsto dalla normativa, Fondazione Sant'Erasmo, in persona del legale rappresentante *pro tempore*, è il Titolare del trattamento avente i seguenti compiti:
assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, per i trattamenti svolti all'interno della propria struttura; adeguare il proprio assetto organizzativo per il governo della "privacy;" adottare le modalità operative connesse con la gestione degli adempimenti ed il trattamento dei dati ai fini di "privacy"; individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative istruzioni e direttive; vigilare sulla puntuale osservanza delle disposizioni ed istruzioni impartite ad incaricati e a responsabili esterni; garantire l'esercizio dei diritti degli interessati adottando, a tal fine, apposite procedure al fine di informare gli interessati dell'esistenza dei loro diritti in materia di protezione dei dati personali; consultare il Responsabile della Protezione dei Dati (DPO) in tutte le questioni riguardanti la protezione dei dati.

6.2 **Il Delegato al trattamento dei dati**. È il soggetto che, considerati i requisiti di esperienza, capacità ed alta affidabilità dimostrati, nonché gli oneri e i poteri inerenti la sua carica di direzione presso l'Ente (o un'area della struttura), ha il dovere di attivarsi affinché l'unità aziendale diretta si conformi a quanto previsto dalla normativa vigente e di futura emanazione in materia di trattamento dei dati personali.

Il Delegato svolge un fondamentale ruolo di collegamento tra il titolare, il DPO e gli incaricati al trattamento dei dati, avente, in particolare, i seguenti compiti: osservare e far osservare scrupolosamente dai suoi collaboratori tutte le disposizioni del GDPR e i relativi decreti attuativi; rispettare e far rispettare dai propri incaricati le misure di sicurezza approvate dal titolare del trattamento; verificare la corretta adozione delle misure idonee di sicurezza (in collaborazione con l'Amministratore di Sistema, nell'ambito delle proprie competenze), ai sensi dell'art. 32 del GDPR, in modo da ridurre al minimo i rischi di distruzione o perdita dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta dei dati personali medesimi; assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. 32-36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione; aggiornare le misure di sicurezza adottate in ragione delle conoscenze acquisite in base al progresso tecnico; informare prontamente il Titolare di ogni questione rilevante ai fini di legge; curare il coordinamento di tutte le operazioni di trattamento dei dati personali; aggiornare almeno ogni anno l'ambito del trattamento consentito ai singoli incaricati / autorizzati e comunicare tempestivamente al Titolare la situazione aggiornata; procedere alle verifiche sulla metodologia di introduzione e di gestione dei dati personali, anche attraverso controlli a campione da eseguirsi periodicamente; evadere tempestivamente i reclami degli interessati ai sensi dell'art. 15 e seguenti del GDPR e comunicare le richieste, le segnalazioni, le istruzioni avanzate dall'Autorità Garante al titolare e predisporre su richiesta del medesimo le relative risposte, collaborando, a tal fine con il Titolare; distruggere, dandone preventiva comunicazione al Titolare, i dati personali alla cessazione del trattamento degli stessi, conformemente alle disposizioni di legge in materia di conservazione della documentazione amministrativa.

6.3 **I Responsabili esterni del trattamento.** Il Titolare può esternalizzare alcuni trattamenti a soggetti individuati quali "Responsabili del trattamento", selezionati tenendo in considerazione la capacità di offrire garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate al rispetto dei requisiti del GDPR. Qualora un trattamento sia esternalizzato ad una persona fisica o giuridica, il Titolare assicura che tale soggetto terzo sia nominato Responsabile esterno del trattamento nel rispetto delle disposizioni del GDPR. Il Responsabile esterno del trattamento rappresenta la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Nel

contesto della Fondazione Sant'Erasmo, ciascun fornitore che abbia accesso ai dati oggetto di trattamento è nominato Responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR, per mezzo di idoneo contratto attraverso cui vengono fornite istruzioni in merito alle modalità di trattamento dei dati personali. L'elenco aggiornato dei responsabili esterni del trattamento è conservato presso la sede del titolare e a disposizione degli interessati che volessero visionarlo.

L'art. 28, comma 3, del GDPR dispone, infatti, che l'accordo vincolante per il responsabile del trattamento debba prevedere, in particolare:

- l'obbligo di trattare i dati solo in conformità alle istruzioni ricevute dal titolare;
- l'obbligo di garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da obblighi di riservatezza, contrattualmente assunti o stabiliti per legge;
- l'obbligo di adottare le misure richieste ai sensi dell'art. 32 del Regolamento, vale a dire le misure tecniche e organizzative a protezione dei dati ritenuti idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento;
- l'obbligo di assistere il titolare, mediante misure tecniche e organizzative adeguate, e nella misura in cui ciò sia possibile, nel dar seguito alle eventuali richieste degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione);
- l'obbligo, ex art. 33 del GDPR, di assistere il titolare nel notificare all'Autorità Garante eventuali *data breaches* (violazioni di dati) occorsi, nonché comunicarli agli interessati nei casi previsti dall'art. 34 del GDPR;
- l'obbligo di cancellazione o restituzione dei dati, su scelta del titolare, al momento della cessazione del rapporto, salvo che la legge non imponga specifici obblighi di conservazione;
- l'obbligo di mettere a disposizione del titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al presente elenco;
- l'obbligo di consentire al titolare di effettuare attività di audit, direttamente o per il tramite di terze parti all'uopo incaricate.

Nel corso di tutta la relazione contrattuale è assicurato da parte della Fondazione Sant'Erasmo un continuo monitoraggio, tramite verifiche periodiche sull'operato dei Responsabili esterni, eventualmente coinvolgendo anche il DPO, al fine di appurare il rispetto della normativa in materia di privacy e delle istruzioni impartite.

6.4 **L'Amministratore di Sistema.** É La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati. L'attribuzione delle funzioni di Amministratore di Sistema, da parte della Fondazione Sant'Erasmo, avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo

relativo alla sicurezza. In particolare, l'Amministratore di Sistema ha le seguenti responsabilità:

a) attivare le credenziali di autenticazione ai soggetti incaricati del trattamento, su espressa indicazione del Titolare del trattamento dei dati personali, per tutti i trattamenti che vengano effettuati con l'utilizzo di strumenti informatici, nonché assumere il compito di gestire a livello informatico tutti i soggetti incaricati del trattamento;

b) individuare le politiche che dovranno essere adottate per garantire la massima protezione dei sistemi contro i virus informatici e verificarne l'efficacia ogni tre mesi;

c) proteggere gli elaboratori dal rischio di accesso da parte di personale interno privo di autorizzazione nonché da parte di soggetti esterni;

d) garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduca nel sistema informatico o telematico;

e) predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici, garantendo che tali registrazioni (access log) posseggano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;

f) dare tempestiva comunicazione al Titolare del trattamento dei dati personali qualora vengano rilevati rischi relativamente alle misure di sicurezza predisposte per la protezione dei dati trattati;

g) coordinare assieme al Titolare (e/o al Delegato, qualora nominato) le attività operative degli incaricati del trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento delle informazioni nell'ambito del sistema informatico;

h) collaborare con il Titolare (e/o al Delegato, qualora nominato) per l'attuazione delle prescrizioni impartite dal Garante;

i) verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi installati negli elaboratori presenti nelle strutture aziendali;

j) comunicare i nominativi della persona o delle persone che saranno assegnate all'Ente per l'espletamento dell'incarico ed aggiornare tempestivamente il Titolare qualora ci siano delle modifiche nell'assegnazione.

6.5 Il Responsabile della Protezione dei Dati ("DPO"). Il DPO rappresenta la principale figura avente uno specifico ruolo di consultazione, consulenza, sorveglianza e controllo in materia di protezione dei dati personali. Il GDPR attribuisce, infatti, al DPO compiti di consulenza, informazione e sorveglianza, nonché un ruolo di contatto con l'Autorità Garante e con i soggetti interessati.

Il DPO è individuato in base alle sue qualità professionali e, in particolare, alla conoscenza specialistica della normativa e delle prassi di gestione dei dati personali; alle competenze relazionali, all'integrità ed agli elevati standard deontologici; all'indipendenza ed all'assenza di qualsiasi conflitto di interesse con il ruolo svolto.

Su indicazione dell'articolo 37, la designazione di tale figura si è resa necessaria in relazione alle attività condotte dal titolare che prevedono il trattamento, su larga scala, di categorie particolari di dati personali (dati sullo stato di salute o di natura sanitaria). La nomina del DPO della Fondazione Sant'Erasmo è stata formalizzata tramite apposito atto di designazione che specifica l'ambito del suo mandato. I dati di contatto e il nominativo del DPO sono comunicati a tutti i soggetti interessati, al Garante e a tutto il personale, in modo tale da garantire che il suddetto possa essere contattato agevolmente in qualsiasi momento.

Ai sensi dell'art. 38 del GDPR, il DPO deve essere tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, riferendo direttamente al vertice gerarchico del titolare e garantendo il segreto e la riservatezza in merito all'adempimento dei propri compiti.

In maniera più specifica, le responsabilità del DPO della Fondazione Sant'Erasmo sono le seguenti:

- sorvegliare l'osservanza del GDPR, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborare con il titolare, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal GDPR e da altre disposizioni in materia di protezione dei dati;
- cooperare e fungere da contatto con il Garante su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un Registro delle attività di trattamento.

6.6 Soggetti autorizzati al trattamento dei dati (o "incaricati")

L'incaricato del trattamento è la persona fisica autorizzata dal titolare o dal responsabile, a seguito di espressa nomina, a compiere determinate operazioni di trattamento dei dati, attenendosi alle istruzioni impartite. L'incaricato è, dunque, colui che effettua materialmente le operazioni di trattamento sui dati personali e ha il dovere di rispettare, durante lo svolgimento della propria attività, i principi generali di cui al GDPR nonché le misure di sicurezza idonee adottate dall'Ente, atte a salvaguardare la riservatezza e l'integrità dei dati.

Il personale della Fondazione Sant'Erasmo che tratta dati personali (dipendenti o collaboratori) assume, dunque, la qualifica di "incaricato" o "autorizzato".

Il Titolare adotta procedure interne per la nomina per iscritto deli incaricati, in relazione alla funzione aziendale nella quale ciascun soggetto opera, e per il costante controllo ed aggiornamento (con cadenza almeno annuale) di tali nomine.

La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

Il Titolare garantisce, inoltre, un'adeguata formazione degli incaricati tramite corsi (come specificato al punto 8 del presente Regolamento) e fornendo istruzioni precise su come effettuare i trattamenti.

In particolare, già con l'atto di nomina ciascun incaricato del trattamento viene informato:

- di limitare il trattamento dei dati a quanto necessario ed indispensabile all'adempimento delle mansioni, osservando inderogabilmente le norme di legge, i regolamenti interni, le politiche aziendali, le circolari o gli ordini di servizio, le istruzioni comunque impartite dal Titolare del Trattamento e dai suoi Delegati;
- di seguire i corsi di formazione in materia di disciplina della protezione dei dati, secondo le indicazioni e modalità fornite dal Titolare.

7. Istruzioni operative per il trattamento dei dati da parte dei soggetti autorizzati

I dipendenti, i collaboratori, i volontari e, in generale, tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relative ai dati, devono ispirarsi ai principi generali di diligenza e correttezza. L'utilizzo dei dati personali deve avvenire in base al fondamentale principio del "*need to know*", secondo cui questi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento).
Ogni utilizzo dei dati in possesso della Fondazione diverso da finalità strettamente professionali è espressamente vietato.
Di seguito vengono esposte le principali istruzioni operative e le regole comportamentali che ogni "incaricato" deve seguire per evitare e prevenire condotte che, anche inconsapevolmente o incolpevolmente, potrebbero comportare rischi alla sicurezza del patrimonio informativo e all'immagine dell'Ente.

7.1 Norme logistiche per l'accesso fisico ai locali

I locali della struttura, in cui sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere accessibili da parte di soggetti non autorizzati. Si

raccomanda ad ogni incaricato, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia autorizzato, soprattutto se esterno all'Ente. Laddove si esegue un trattamento di dati personali (fosse anche una semplice visione o raccolta di dati), bisogna riporre in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti i trattamenti di dati personali.

7.2 "Clean Desk Policy"

Deve essere costantemente adottata una "politica della scrivania pulita", la quale, oltre a garantire un'immagine di ordine e professionalità, risulta fondamentale per ridurre sia il rischio che dati ed informazioni possano essere visti da persone non abilitate a conoscerle, sia il rischio che documenti possano essere smarriti o sottratti.

In maniera più specifica:

- si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa, oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
- a fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio e la documentazione utilizzata, in modo da lasciare la scrivania sgombra da documenti contenenti dati personali.

7.3 Trattamento dei dati senza l'ausilio di strumenti elettronici (atti e documenti cartacei)

Per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, l'incaricato è tenuto ad osservare le seguenti disposizioni ed istruzioni:

a) I documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e, qualora ciò avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento. Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi; è vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o accessibili da soggetti terzi (corridoi o sale). Nel caso dei dati "particolari" (dati sensibili), il rispetto di queste norme è essenziale.

b) L'incaricato del trattamento deve controllare che i documenti cartacei contenenti dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed

integri. Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti nei locali individuati per la loro conservazione.

c) I documenti contenenti dati personali non devono essere mai lasciati incustoditi o abbandonati (su tavoli, scrivanie) durante l'orario di lavoro, quando ci si debba assentare dal proprio posto (ad esempio per la pausa pranzo o per una riunione): è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, ecc.).

d) Al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate (in particolare in presenza di dati di natura sensibile).

e) L'incaricato deve adottare ogni opportuna cautela affinché persone non autorizzate non vengano a conoscenza del contenuto dei suddetti documenti.

f) Per evitare il rischio di diffusione o comunicazione non autorizzata dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche; il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro; particolare cautela deve, inoltre, essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato.

g) É vietato utilizzare copie fotostatiche di documenti contenenti dati personali, e in particolare dati sensibili, come carta da riciclo o da appunti.

h) I documenti contenenti dati "sensibili" (ad esempio i dati riguardanti lo stato di salute o i dati sanitari) o dati che, per una qualunque ragione, siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura o in contenitori ed appositi armadi muniti di serratura, ove previsto.

i) Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.

l) L'incaricato del trattamento deve evitare che un soggetto terzo non autorizzato al trattamento possa esaminare anche solo la copertina del documento in questione.

Infine, a seguito di una cessazione del rapporto lavorativo o di consulenza o, comunque, al venir meno, ad insindacabile giudizio della Fondazione Sant'Erasmo, della permanenza dei presupposti per l'utilizzo dei dati cartacei, gli incaricati hanno i seguenti obblighi:

- procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
- divieto assoluto di copiare, alterare, manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili, tramite qualsiasi processo.

7.4 Distruzione delle copie cartacee

Qualora sia necessario distruggere i documenti contenenti dati personali (e, in particolar modo, quelli contenenti dati "sensibili"), l'operazione deve, se possibile, essere compiuta utilizzando gli appositi apparecchi "trita documenti". In alternativa, i documenti devono essere sminuzzati in modo da non essere più ricomponibili.

7.5 Utilizzo del telefono e del telefax

Sono raccomandate le seguenti modalità operative, in riferimento all'utilizzo, durante lo svolgimento dell'attività lavorativa, di apparecchiature come telefono e telefax:

- L'apparecchio "telefax" deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.
- È comunque necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
- In caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza.
- É proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia il soggetto a cui si riferiscono i dati o un incaricato autorizzato a poter trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce trattando dati personali per telefono (soprattutto utilizzando cellulari), per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente. Tali precauzioni diventano particolarmente importanti, qualora il telefono sia utilizzato in luogo pubblico o aperto al pubblico.

7.6 Trattamenti dei dati con l'ausilio di strumenti elettronici

L'incaricato del trattamento è autorizzato ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.

L'accesso al PC è protetto da un sistema di autenticazione che richiede all'incaricato di inserire sulla schermata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione e l'utilizzo di tale combinazione è fondamentale per il corretto utilizzo del PC, in quanto tutela l'utilizzatore ed in generale la Fondazione Sant'Erasmo da accessi illeciti e, comunque, da violazioni e danneggiamenti del patrimonio informativo, oltre a tutelare l'incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che dunque, con il suo profilo, solo il suddetto possa svolgere determinate azioni e operazioni.

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione. Avere cura del computer e degli accessori in affidamento consente di conservare l'efficienza dei sistemi di sicurezza.

È, innanzitutto, importante che ogni computer, relativo monitor e stampanti, siano spenti in caso di inattività prolungata (di sera, oppure durante i weekend).

Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei o non specificamente autorizzati.

Per la gestione del lavoro sui computer si applicano le seguenti istruzioni:

a) L'incaricato che ha ricevuto le credenziali di autenticazione per il trattamento dei dati personali, deve conservare con la massima segretezza le componenti riservate ("parola chiave" o "password") e i dispositivi di autenticazione in loro possesso ed uso esclusivo.

b) La "parola chiave", quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

c) La "parola chiave" deve essere composta da una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali, non potendo contenere riferimenti agevolmente riconducibili all'incaricato o ai suoi familiari.

d) L'incaricato deve modificare la componente riservata della "parola chiave" al primo utilizzo e, successivamente, almeno ogni sei mesi, non dovendo mai essere uguale alle precedenti. In caso di trattamento di dati sensibili la "password" deve essere modificata almeno ogni tre mesi.

e) La "password" deve essere conservata in un luogo sicuro; è vietato indicare la password su supporti facilmente intercettabili da altre persone (quali, ad esempio, biglietti sulla scrivania, "post-it" sul monitor o sotto la tastiera del computer); inoltre

non deve mai essere rivelata o condivisa con i colleghi di lavoro, con familiari o con amici.

f) L'incaricato deve evitare di digitare la propria "password" in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti della Fondazione Sant'Erasmo.

g) Occorre cambiare immediatamente la "password", qualora vi sia il dubbio o il sospetto che sia diventata poco "sicura".

h) L'incaricato non deve lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali. Se l'incaricato ha necessità di assentarsi momentaneamente dalla propria postazione, deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone.

i) Lo "screen-saver" ("salva schermo"), attivo su ogni computer e protetto da password che, dopo 10 minuti di inattività della workstation, ne blocca l'utilizzo, non deve mai essere disattivato da parte dell'incaricato.

j) Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Ente è stato installato un "antivirus" aziendale che si aggiorna automaticamente all'ultima versione disponibile. L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito. Nel caso in cui il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario darne immediatamente segnalazione al titolare o all'Amministratore di Sistema. Si raccomanda di non scaricare, né tantomeno aprire *files* provenienti via email da mittenti sconosciuti. Tali *files* possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

k) Deve sempre essere prestata la massima attenzione all'utilizzo, solo se davvero necessario per lo svolgimento della propria attività, dei supporti di origine esterna (per esempio: chiavi USB, dischi esterni, CD riscrivibili, ecc.), avvertendo immediatamente il tecnico informatico / Amministratore di Sistema nel caso in cui siano rilevati virus; tali supporti devono comunque essere custoditi in cassetti o archivi muniti di serratura; quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati ad opera del tecnico informatico dell'Ente.

l) Al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave.

Per gli incaricati vige, inoltre, il divieto di:

- modificare le configurazioni già impostate sul personal computer senza espressa autorizzazione e senza il supporto di personale tecnico qualificato;
- utilizzare programmi senza la preventiva autorizzazione scritta dell'Ente;
- installare software di qualsiasi tipo, scaricati da internet o di cui l'Ente non possiede la licenza, oppure giochi, screen saver o qualsiasi altra utility non preventivamente autorizzata dalla Fondazione Sant'Erasmo;
- fare copia del software installato al fine di farne un uso personale;
- effettuare in proprio attività manutentive degli strumenti elettronici o permettere attività manutentive da parte di soggetti non espressamente autorizzati dall'Ente.

7.7 Servizio di internet e posta elettronica

Gli strumenti di comunicazione telematica (Internet e posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative, salvo casi eccezionali di comprovate urgenza e necessità. Occorre essere sempre consapevoli che la posta elettronica e la navigazione in Internet sono veicoli che comportano il rischio di introduzione sul proprio strumento elettronico (e, dunque, nell'Ente) di virus o altri elementi potenzialmente dannosi. Sono vietati comportamenti che possono recare danno all'Ente.

In particolare, l'incaricato dovrà osservare le seguenti regole:

a) Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'ente e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

b) É consentita la navigazione Internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate; in particolare è sempre vietato accedere ai siti i cui contenuti non siano adeguati alla serietà e al decoro richiesti nei luoghi di lavoro.

c) É vietato scaricare files e software anche gratuiti, prelevati da siti internet, se non a seguito di espressa autorizzazione da parte del titolare o del responsabile. Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza.

d) È vietato utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o sopprimere per finalità illecite il contenuto di comunicazioni e/o documenti informatici.

e) Si ricorda che le unità di rete sono aree destinate alla condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto si raccomanda di non collocare, anche temporaneamente, in queste aree qualsiasi files che non sia attinente allo svolgimento dell'attività lavorativa.

f) Si ricorda che non è permessa la partecipazione, per motivi non professionali, a Forum di discussione, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi; l'accesso a tali fonti di informazioni, esclusivamente per motivi professionali, potrà avvenire solo previa autorizzazione scritta da parte del titolare o del responsabile.

g) In riferimento alla posta elettronica, non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto, in quanto tale atto assicura al mittente l'esistenza del destinatario.

h) Occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare.

i) Nell'ipotesi in cui la mail debba essere utilizzata per la trasmissione di dati particolari (dati sensibili), si raccomanda di prestare attenzione sul fatto che l'indirizzo del destinatario sia stato correttamente digitato e che l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile.

j) In caso di errore nella spedizione o ricezione di un messaggio di posta elettronica, è opportuno contattare il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi eventuali allegati) senza effettuare copia.

k) Si ricorda che l'incaricato è invitato a fare una chiara distinzione tra i documenti o email considerati personali e quelli professionali; un qualsiasi documento che non comporterebbe questa distinzione sarebbe considerato come professionale.

7.8 Utilizzo dei PC portatili

Il computer portatile può venir concesso in uso dal titolare a singoli incaricati, volontari o soggetti espressamente autorizzati qualora, nello svolgimento della propria attività, necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Ente.

In riferimenti all'utilizzo dei PC portatili valgono le medesime regole elencate per i PC connessi alla rete, oltre alle seguenti ulteriori raccomandazioni:

- il soggetto autorizzato è responsabile dei dispositivi mobili assegnatigli dall'Ente e deve custodirli con diligenza durante l'utilizzo sia se questo avvenga nel luogo di lavoro sia fuori sede (in tal caso, se espressamente autorizzato dal titolare); in ogni caso non è consentito lasciare incustoditi i dispositivi mobili;
- sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dal Titolare;
- prima della riconsegna l'incaricato deve rimuovere eventuali files ivi elaborati;
- in caso di furto o smarrimento di un portatile è necessario avvertire tempestivamente il Titolare o il responsabile del sistema informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
- è opportuno eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

8. Formazione ed informazione

In base all'articolo 29 del GDPR, "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*".

La centralità della formazione in materia di "privacy" è ancor più evidenziata dall'art. 32, paragrafo quarto, del GDPR ("Sicurezza del trattamento"), secondo cui "*il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

Inoltre, ai sensi dell'art. 39 del GDPR, il Responsabile della Protezione dei Dati (DPO) deve occuparsi di sorvegliare l'osservanza della normativa in materia di "privacy", compresi "*la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo*", nonché supportare il titolare nella programmazione di piani formativi inerenti la materia.

L'obbiettivo di garantire un corretto trattamento dei dati personali, conforme ai requisiti previsti dalla normativa europea ed italiana, viene raggiunto dalla Fondazione Sant'Erasmo, oltre che per mezzo della comunicazione di tale Regolamento interno a tutti i soggetti coinvolti, anche, e soprattutto, grazie alla particolare attenzione riposta nei confronti della formazione del proprio personale.

La previsione di eventi formativi diretti ai dipendenti dell'Ente ed ai collaboratori che trattano dati personali, nell'ottica di un miglioramento continuo delle attività lavorative, concretizza il principio di "*accountability*", ossia di responsabilizzazione del Titolare del trattamento, previsto dal GDPR.

Tale processo di formazione e di "sensibilizzazione", programmato annualmente, sarà svolto in orario lavorativo, coinvolgendo tutto il personale incaricato al trattamento dei dati personali (fin dal momento di ingresso in struttura di una nuova risorsa), e, in particolare, le figure professionali che, all'interno del proprio ufficio o reparto, rivestono un ruolo "apicale" o di particolare responsabilità. Per quanto riguarda i responsabili esterni del trattamento, Fondazione Sant'Erasmo fornisce delle direttive formulate specificatamente per le attività di loro competenza.

La formazione è finalizzata ad assicurare la corretta comprensione ed applicazione dei principi su cui si basa la *Policy Privacy* e ad illustrare i rischi generali e specifici dei trattamenti dei dati, le misure organizzative, tecniche e informatiche adottate, nonché le responsabilità e le sanzioni. Inoltre, prevede delle sessioni di aggiornamento in caso di modifiche normative, organizzative e tecniche.

La formazione sarà documentabile mediante opportuna modulistica attestante la partecipazione agli eventi formativi.

9. Responsabilità e sanzioni

I soggetti autorizzati al trattamento, al fine di non esporre sé stessi e l'Ente a rischi sanzionatori, sono tenuti ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione interna.

Tutti gli incaricati sono tenuti ad osservare e fare osservare le disposizioni e le istruzioni contenute nel presente Regolamento. Il mancato rispetto o la violazione delle regole contenute sono perseguibili con provvedimenti disciplinari nonché con le azioni civili e penali previsti *ex lege*.

In particolare:

- per il personale dipendente, il mancato rispetto o la violazione delle regole potranno comportare, l'adozione di provvedimenti disciplinari previsti dal Contratto Collettivo Nazionale di Lavoro (C.C.N.L.), oltre alle azioni civili e penali previste *ex lege*;
- per i collaboratori esterni, il mancato rispetto o la violazione delle regole potranno comportare la risoluzione del contratto, oltre alle azioni civili e penali previste *ex lege*.

10. Aggiornamento e revisione

Il presente Regolamento interno è soggetto ad aggiornamento e/o revisione con frequenza annuale.

Il DPO, in quanto figura deputata anche all'aggiornamento della documentazione interna in materia di privacy, verifica costantemente la complessiva idoneità delle procedure predisposte al fine di assicurare il conseguimento degli obiettivi posti dalla disciplina vigente in materia, tenendo conto, in particolare, delle modifiche eventualmente intervenute nella normativa di riferimento, negli assetti organizzativi del Titolare nonché dell'efficacia dimostrata dalle procedure nella prassi applicativa.

Tutti gli incaricati del trattamento possono, inoltre, proporre, se ritenuto necessario, integrazioni o specificazioni al presente documento. Le proposte verranno esaminate dal Titolare del trattamento, con la consulenza del DPO.