FONDAZIONE SODALIZIO DI SAN MARTINO

Perugia

REGOLAMENTO INTERNO IN MATERIA DI PRIVACY

REGOLAMENTO INTERNO PRIVACY: premessa

Le seguenti prescrizioni sono da intendersi VINCOLANTI per i dipendenti della Fondazione che sono preposti in qualità di autorizzati al trattamento e per tutti i preposti che a vario titolo, hanno accesso ai dati personali trattati dalla Fondazione. L'eventuale violazione delle disposizioni di seguito riportate costituisce un illecito, che può comportare l'applicazione di sanzioni di natura disciplinare ma anche di natura civile e penale, secondo quanto previsto dalle norme vigenti. Si auspica, pertanto, una responsabile e consapevole collaborazione da parte di tutti gli operatori, nella diligente osservanza delle disposizioni di legge e nelle prescrizioni contemplate all'interno del presente Regolamento Interno Privacy, nonché del Regolamento europeo "GDPR" e delle norme previste dal D.Lgs n. 101/2018.

Il presente Regolamento è approvato con atto del Consiglio di Amministrazione al fine di individuare le norme comportamentali e le procedure tecnico-organizzative cui è necessario attenersi in materia di trattamento di dati personali e di sicurezza nello svolgimento di tutte le attività istituzionali della Fondazione Sodalizio di San Martino (di seguito anche "Fondazione"). In particolare, si ritiene necessario definire una chiara disciplina interna atta a garantire che il trattamento dei dati personali, svolto nell'ambito delle mansioni lavorative, avvenga - come espressamente previsto dal regolamento UE n. 679/20162 GDPR art. 5, par.1, lettera f) "in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)".

Secondo il suddetto articolo, inoltre, i dati personali oggetto del trattamento devono essere altresì:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste

dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

Il titolare del trattamento è competente per il rispetto di tali principi e dovrà essere in grado di comprovarne suddetto rispetto («responsabilizzazione»). I dati personali trattati in violazione dei succitati principi, NON POTRANNO ESSERE UTILIZZATI O ESSERE DIFFUSI.

REGOLAMENTO INTERNO PRIVACY: definizioni

a) **«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;

b) **«trattamento»:** 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;

c) **«limitazione di trattamento»:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) **«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) **«pseudonimizzazione o anonimizzazione»:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

g) **«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

h) **«Incaricati o Autorizzati del trattamento»:** è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali. L'autorizzato può operare alle dipendenze del Titolare. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega. Gli Incaricati saranno designati con apposita lettera di nomina;

i) **«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;

j) **«destinatario»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

k) **«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;

l) **«consenso dell'interessato»:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

m) **«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;

n) **«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;

o) **«dati biometrici»:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

p) **«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

q) **«autorità di controllo»:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;

r) **«autorità di controllo interessata»:** un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo

sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo.

REGOLAMENTO INTERNO PRIVACY: ambito di applicazione

Il presente regolamento si applica a tutte le persone fisiche che, nell'esercizio delle proprie mansioni/attività ed a qualsiasi titolo, svolgono attività in qualità di "incaricato o autorizzato del trattamento dei dati personali", di "responsabili del trattamento" o di addetti alla gestione o alla manutenzione degli strumenti elettronici e comunque tutti coloro, incluse le persone giuridiche, che trattano, in qualsiasi ruolo, dati personali e sensibili di titolarità della Fondazione e/o che la Fondazione tratta in qualità di Responsabile del trattamento. Suddetti soggetti, sono tenuti al rispetto delle regole di seguito elencate.

Il regolamento si applica, altresì, alle attività che comportano il trattamento dei dati personali di titolarità della Fondazione (quali, ad es. attività connesse alla gestione del personale, agli organi societari e agli adempimenti relativi ai propri clienti, fornitori ed eventuali consulenti, manutentori, servizi esterni) ovvero alle attività che comportano il trattamento dei dati personali per le quali la Fondazione Sodalizio di San Martino sia stata individuata, ai sensi dell'art. 28 GDPR, in qualità di Responsabile Esterno del trattamento (quali, ad es. attività oggetto di convenzioni di servizio sottoscritte per le quali ha ricevuto apposita nomina) nel rispetto delle finalità determinate dai committenti e secondo le modalità previste dalla convenzione di servizio e dalla nomina ricevuta. Le nomine della Fondazione Sodalizio di San Martino in qualità di Responsabile Esterno del trattamento definiscono l'ambito del trattamento autorizzato da parte dei Titolari e vengono descritte ed elencate nel Registro dei Trattamenti della Fondazione. Nessun trattamento ulteriore è consentito, se non previa autorizzazione dei titolari a cui compete in via esclusiva la verifica della compatibilità dei trattamenti effettuati rispetto alle informative rilasciate (art.12 GDPR) ed ai consensi acquisiti dagli interessati.

REGOLAMENTO INTERNO PRIVACY: principi generali

1. Dovrà essere mantenuto il più assoluto riserbo su tutte le informazioni di cui si viene a conoscenza nello svolgimento del lavoro.

2. Le pratiche di lavoro dovranno essere sempre trattate secondo gli indirizzi della legge e le indicazioni della prassi. In particolare, per quanto attiene al Trattamento di Dati Personali, dovrà essere sempre effettuata la raccolta, la elaborazione, la registrazione, esclusivamente per gli scopi assegnati.

3. Ogni Incaricato potrà accedere alle procedure di elaborazione per le quali è stato espressamente autorizzato, e inoltre dovrà custodire con la massima riservatezza, anche nei confronti degli altri colleghi di lavoro, le credenziali di autenticazione per l'accesso alle procedure necessarie per il trattamento da svolgere.

4. Ogni Incaricato dovrà osservare scrupolosamente le procedure di sicurezza indicate nel Registro del Trattamento Dati e nel presente Regolamento.

5. Al termine del lavoro tutti i documenti cartacei dovranno essere riposti negli armadi possibilmente chiusi a chiave, e, relativamente ai dati in trattamento, dovrà essere disattivata la procedura di elaborazione informatica eventualmente utilizzata.

6. L'accesso al lavoro fuori dal normale orario, dovrà essere autorizzato dal Titolare.

7. Tutti i rapporti con i clienti, ospiti o visitatori (colloqui, anche telefonici, scambio di documenti, o informazioni anche verbali ecc.) dovranno avvenire sempre nel rispetto delle procedure di riservatezza.

8. I documenti cartacei fotocopiati ed i contenuti copiati su supporti rimovibili (chiavette, cd e simili) eventualmente utilizzati per il trattamento di dati personali, sensibili e giudiziari, devono essere distrutti o cancellati se copiati su supporti rimovibili, una volta terminato il trattamento.

9. Il sistema antivirus di cui sono dotati i computer deve essere aggiornato con continuità.

10. Le credenziali di autenticazione dovranno essere rinnovate ogni 6 mesi. Se il Trattamento Dati comprende anche dati sensibili o giudiziari, dovranno essere rinnovate ogni 3 mesi.

11. Dovrà essere data immediata comunicazione al Titolare del trattamento o suo rappresentante di qualsiasi violazione, perdita o danneggiamento dei dati di cui si venga a conoscenza o di cui si abbia anche sola semplice supposizione.

12. Il trattamento di dati personali deve essere effettuato in misura pertinente e non eccedente. Dovrà essere svolto esclusivamente per le finalità per le quali i dati sono stati raccolti e nella misura in cui queste sono state oggetto di apposita informativa fornita agli interessati.

13. Il trattamento di dati personali non deve essere effettuato qualora sia possibile realizzare le finalità per cui è attuato, attraverso l'uso di dati anonimi.

14. Le attività di trattamento dei dati personali e sensibili devono essere limitate al tempo strettamente necessario al raggiungimento degli scopi per cui i dati medesimi sono stati raccolti.

15. Ciascun soggetto preposto allo svolgimento delle operazioni di trattamento ha l'obbligo di mantenere il segreto sui dati raccolti o di cui venga a conoscenza nel corso della propria attività lavorativa, evitando di diffonderli o di comunicarli a terzi o comunque a soggetti non legittimati al trattamento di tali informazioni. Non è pertanto autorizzato a fornire riscontro diretto a richieste, verbali o scritte, di estrazione o di comunicazione di dati di titolarità della Fondazione ovvero di titolarità di terzi, anche qualora tali richieste pervengano da uffici o strutture aziendali della stessa Fondazione, se non autorizzate all'accesso ai dati medesimi dal Titolare

16. In caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, ciascun soggetto preposto allo svolgimento delle operazioni di trattamento deve adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza o non specificamente autorizzato.

17. Qualora, nello svolgimento delle proprie mansioni, l'incaricato utilizzi atti o documenti contenenti dati personali o sensibili, questi non devono essere lasciati incustoditi. Occorre, inoltre, che siano evitati eventuali accessi da parte di soggetti non autorizzati. Alla fine delle proprie attività lavorative, la documentazione deve essere SEMPRE riposta negli archivi ad accesso controllato.

18. Al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione delle anagrafiche e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento.

ORGANIGRAMMA PRIVACY

La Fondazione Sodalizio di San Martino, in qualità di Titolare del trattamento di dati personali, al fine di facilitare l'adeguamento al regolamento europeo GDPR e al D.Lgs. n. 101/2018 e con lo scopo di garantire il rispetto dei principi previsti da suddette norme, individua la propria struttura di presidio della privacy in un "Organigramma Privacy" così come di seguito descritto.

Titolare del trattamento

Il Titolare del trattamento ai sensi dell'art. 4 par. 7 GDPR è la Fondazione nel suo complesso, che è rappresentata dal Presidente pro-tempore, in qualità di Legale Rappresentante. Il Legale Rappresentante può delegare con apposita deliberazione del Consiglio di Amministrazione un Consigliere con le funzioni di rappresentare la Fondazione in materia di privacy.

Delegato alla gestione della privacy: il Referente Privacy Interno

Con deliberazione del Consiglio di Amministrazione, al Direttore Amministrativo è delegata l'organizzazione e la supervisione interna della tutela della privacy, con la facoltà di nominare uno o più sub-responsabili interni nell'ambito delle aree di attività (Servizio dell'Amministrazione Centrale, Servizio della Farmacia, Servizio dell'Azienda Agraria, Servizio delle Residenze per anziani), attraverso la sottoscrizione di una nomina formale. La struttura, è rappresentata graficamente in un organigramma allegato al presente regolamento.

Funzionamento della struttura di presidio privacy

Il "Referente Privacy Interno" è supportato dai sub-responsabili interni nelle attività di organizzazione e gestione della privacy aziendale. Assiste il Titolare nei seguenti processi: coordinamento della gestione operativa degli adempimenti in materia di privacy, eventuale istruttoria sulle richieste di accesso o estrazione dati provenienti da soggetti terzi (ad esempio per indagini di polizia giudiziaria ovvero per istanze di accesso ai sensi dell'art. 6 del GDPR), cura degli approfondimenti normativi, organizzazione delle sessioni di formazione verso il personale interno, verifica dell'applicazione del presente regolamento e di ogni ulteriore disposizione aziendale in materia di privacy, ivi inclusa la corretta preposizione di incaricati ed addetti alla manutenzione, le eventuali comunicazioni con il Garante, le segnalazioni e la gestione di casi di Data Breach, la corretta applicazione dei principi della tutela dei dati personali in ambito sanitario, l'aggiornamento delle credenziali assegnate a ciascun preposto per l'accesso agli strumenti elettronici, la tenuta e l'aggiornamento del Registro dei Trattamenti, l'aggiornamento di informative e consensi, l'invio di nomine verso i Responsabili esterni, l'invio di lettere di autorizzazione verso i dipendenti e i neo assunti e il rispetto di tutte le altre norme del GDPR e dei principi vigenti in

materia di tutela dei dati personali. Qualora lo ritenga opportuno, Il Referente Privacy Interno avanza verso il Titolare, formale proposta di nomina di un DPO esterno (Responsabile Protezione Dati o Data ProtectionOfficer) al quale affidare in tutto o in parte, la gestione della privacy all'interno della Fondazione.

DATI DI TITOLARITÀ DELLA FONDAZIONE SODALIZIO DI SAN MARTINO

Il trattamento dei dati personali e sensibili di titolarità della Fondazione Sodalizio di San Martino viene effettuato nel rispetto delle finalità e con le modalità indicate nell'informativa ai sensi dell'art. 12 del GDPR preliminarmente rilasciata agli interessati ai fini dell'acquisizione del relativo consenso. L'informativa viene aggiornata periodicamente ed in ogni caso in coerenza con le raccomandazioni del Garante e le vigenti norme di legge. L'informativa al personale dipendente viene rilasciata al momento della consegna della lettera di assunzione; l'informativa aggiornata viene pubblicata nella sezione privacy del sito istituzionale della Fondazione. L'informativa destinata ai fornitori/consulenti viene inserita, con apposita clausola, nel testo del relativo contratto; il testo esteso dell'informativa viene pubblicato nella sezione privacy del sito istituzionale della Fondazione.
Ai sensi dell'art. 28 del GDPR, i soggetti esterni che, in qualità di fornitori, consulenti o comunque contraenti, per esigenze organizzative della Fondazione, gestiscono specifici servizi o svolgono attività connesse, strumentali o di supporto a quelle della Fondazione, e che pertanto effettuano attività di trattamento di dati personali di titolarità aziendale (ad es.: fornitura di prestazioni professionali, sanitarie o di prestazioni e servizi anche in convenzione quali consulenti, istituti di credito ed assicurativi, cliniche, aziende ospedaliere, ecc.), sono di norma individuati in qualità di Responsabili del trattamento, sempreché in possesso dei requisiti previsti dall'art. 28 comma 1 GDPR. In alternativa ovvero nel caso in cui i fornitori/consulenti trattino dati di titolarità dei soci/committenti della Fondazione Sodalizio di San Martino dovrà essere richiesto l'elenco nominativo delle persone fisiche preposte dai fornitori/consulenti alle attività che comportano il trattamento di dati personali e copia delle relative istruzioni operative impartite ai fini delle necessarie verifiche ed integrazioni da parte della Fondazione.

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

L'art. 32 del GDPR stabilisce che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, tra le quali:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Le seguenti istruzioni devono essere osservate da ciascuna persona fisica autorizzata ad accedere ai dati personali o preposta allo svolgimento delle operazioni di trattamento relative a dati di titolarità della Fondazione Sodalizio di San Martino ovvero rispetto ai quali la Fondazione è stata nominata Responsabile Esterno dai soci committenti:

Trattamenti effettuati con strumenti elettronici

Il trattamento di dati personali con strumenti elettronici è consentito agli autorizzati/addetti o preposti, dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o ad un insieme di trattamenti.

Gestione degli strumenti elettronici in dotazione

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smartcard,...). Devono essere adottate le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.

Per monitorare il rispetto delle politiche e degli obblighi di sicurezza possono essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi.

L'uso della posta elettronica è autorizzato esclusivamente per finalità di lavoro; si raccomanda di non inviare comunicazioni a soggetti estranei agli scopi istituzionali o professionali. In caso di assenza prolungata può essere richiesto all'incaricato di individuare un proprio fiduciario autorizzato ad accedere alla casella assegnata. Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati sensibili, si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

Coloro che eseguono duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) o che utilizzano strumenti per la riproduzione cartacea di documenti digitali, dovranno procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli per eventuali appunti o brutte copie. La documentazione riprodotta, dovrà invece essere distrutta immediatamente quando non più necessaria.

Antivirus e protezione dei dati

Qualora non siano attivi sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli autorizzati devono procedere all'effettuazione delle operazioni di aggiornamento, di volta in volta richieste dal sistema, secondo le istruzioni visualizzate sullo schermo; tutti i supporti di memorizzazione devono essere sottoposti a scansione antivirus.

Gestione organizzativa e tecnica dei supporti di memorizzazione dei dati

I supporti informatici che contengono dati sensibili o giudiziari sono distrutti/resi inutilizzabili ovvero possono essere riutilizzati solo dopo avere provveduto a cancellare i dati e le informazioni contenute in modo tale che questi non siano tecnicamente in alcun modo recuperabili.

Trattamento di dati effettuati con documenti cartacei o strumenti non elettronici

Nel caso in cui il trattamento sia effettuato con strumenti diversi da quelli elettronici, gli autorizzati dovranno verificare che siano rispettati i criteri di controllo e custodia per tutto il ciclo di lavorazione necessario allo svolgimento delle operazioni di trattamento. In particolare, l'autorizzato è tenuto a impedire l'accesso ai dati da parte di persone non autorizzate fino al termine delle operazioni di trattamento effettuate.

L'accesso agli archivi contenenti dati sensibili e giudiziari deve essere controllato. Chi vi accede dopo l'orario di lavoro a qualsiasi titolo, deve essere identificato e registrato. Qualora gli archivi siano sprovvisti di strumenti elettronici per il controllo degli accessi, la consultazione degli stessi sarà resa possibile solo previa autorizzazione del Titolare.

Nel caso in cui sia necessario effettuare trasmissioni o riproduzione di documenti contenenti dati personali devono essere adottate le successive cautele:

- NON lasciare incustoditi presso fax, stampanti e fotocopiatrici documenti contenenti dati personali;
- In caso di trasmissione via fax di documenti contenenti dati personali, verificare, eventualmente anche per via telefonica, l'avvenuta ricezione del fax.

Ciascun autorizzato al trattamento deve rispettare i principi generali previsti dall'art. 5 e 6 del GDPR (principi applicabili al trattamento di dati personali e Liceità del trattamento), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi, comunque connessi alla mansione e all'ambito di operatività assegnato. Si ricorda, altresì, che i dati devono essere trattati nei limiti della pertinenza, completezza e non eccedenza rispetto alle finalità per cui sono raccolti o successivamente trattati; rispettare l'obbligo di riservatezza e segretezza e

conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto; utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali.

L'incaricato o autorizzato, inoltre, deve:

- rispettare le misure di sicurezza previste nella sezione 2 del GDPR e le misure idonee adottate dalla Fondazione, atte a salvaguardare la riservatezza e l'integrità dei dati, ai sensi degli articoli 32 e seguenti del GDPR;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica);
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze.

In attuazione al presente regolamento, sono redatte le seguenti istruzioni operative

- **identificazione dell'interessato:** al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- **verifica del controllo dell'esattezza del dato e della corretta digitazione:** al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- **accesso fisico ai locali:** l'accesso ai locali ove i dati personali (ed in particolare quelli di natura sensibile) sono custoditi, dovrà essere disciplinato con il fine di evitare che durante l'orario di lavoro, possano essere resi accessibili a soggetti non autorizzati. Si raccomanda, 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 legittimato, soprattutto se esterno all'organizzazione di appartenenza.

ADDETTI ALLA MANUTENZIONE DEL SISTEMA INFORMATICO

Le seguenti istruzioni devono essere osservate dai preposti alla gestione dei servizi di manutenzione che trattano o hanno accesso ai dati di titolarità della Fondazione Sodalizio di San Martino e/o per i quali la Fondazione Sodalizio di San Martino è nominata Responsabile Esterno del trattamento, nonché dagli addetti di ditte specializzate che svolgono interventi tecnici di gestione e manutenzione degli strumenti elettronici su richiesta della Fondazione Sodalizio di San Martino:

- gestire le credenziali di autenticazione:

- gestire i profili di autorizzazione degli incaricati al trattamento dei dati/addetti alla manutenzione, su specifiche indicazioni impartite dal Titolare del trattamento o, comunque, previsti dalla Password Policy della Fondazione;
- provvedere alla disattivazione/variazione delle utenze assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica del Titolare o dei responsabili;
- pianificare la formazione del personale, in materia di soluzioni tecniche per la garanzia della sicurezza dei dati e della protezione degli strumenti elettronici;
- adottare i provvedimenti necessari ad evitare la perdita o la distruzione accidentale dei dati e provvedere al loro ricovero periodico con copie di back-up secondo i criteri di sicurezza stabiliti;
- assicurarsi che la conservazione delle copie di back-up dei dati avvenga in luogo adatto e sicuro;
- prevedere procedure operative per la disattivazione dei "codici identificativi personali" (User-ID), in caso di perdita della qualità di incaricato all'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per un periodo superiore a 3 mesi ;
- proteggere gli strumenti elettronici dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di programmi virus mediante idonee misure di sicurezza da aggiornare almeno ogni 6 mesi;
- mantenere un adeguato sistema di autorizzazione che, per ogni identificativo utente, riporti la data di attivazione, le funzioni del sistema alle quali l'utente è abilitato, la data di cessazione dell'identificativo stesso;
- provvedere al salvataggio dei dati presenti sui server e al loro ripristino in caso di necessità;
- registrare e archiviare tutte le attività eseguite sul sistema;
- garantire che le informazioni scambiate con soggetti interni ed esterni siano opportunamente protette da rischi di Data Breach.
- assicurarsi che l'hardware sia conforme alla normativa in materia di protezione dei dati personali;
- in occasione di ciascun intervento di manutenzione e di assistenza tecnica, i fornitori dovranno sottoscrivere un verbale sulla esecuzione dei lavori, che ne attesti lo stato di conformità;
- i software operativi e i programmi applicativi siano idonei ad assicurare la separazione tra dati anagrafici e dati sensibili, la tracciabilità delle attività degli utenti, un sistema di autenticazione e di autorizzazione conforme alla normativa in materia di protezione dei dati personali;
- effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- gestire le credenziali di autenticazione dei soggetti autorizzati del trattamento come previsto dalla Password Policy della Fondazione;
- provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica del Titolare ovvero della Direzione Risorse Umane e su indicazione del Titolare;

- custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
- l'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico;
- nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova;
- nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione;
- per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati;
- informare al più presto il Titolare del trattamento qualora si dovessero riscontrare malfunzionamenti, non conformità o episodi di Data Breach, anche solo se presunti.
- tutti i dati personali contenuti nei data base devono essere protetti da password;
- l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
- è assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla Fondazione, se non previa espressa comunicazione scritta.

NORME FINALI

ALLEGATI AL REGOLAMENTO

I seguenti documenti sono da intendersi parte integrante del presente Regolamento:

- Data Breach: Procedura Operativa di Segnalazione, Notifica e Valutazione
- Manuale per Trattamento Dati delle Persone Fisiche
- Password Policy

VIOLAZIONE DEL REGOLAMENTO

Fermi restando i profili di responsabilità civile e penale previsti dalla normativa vigente, con particolare riferimento a condotte di trattamento illecito dei dati, ovvero di omessa adozione delle misure tecniche e organizzative per la garanzia della tutela dei dati personali, in relazione ai dipendenti della Fondazione si precisa che il mancato rispetto del presente Regolamento costituisce un comportamento sanzionabile disciplinarmente in quanto grave violazione degli obblighi contrattualmente assunti, con conseguente applicabilità di sanzioni disciplinari.

RINVIO

Per quanto non espressamente disciplinato in questa sede, si rinvia ai principi ed alle disposizioni del GDPR, del D.Lgs n. 101/2018, ai Provvedimenti Generali, le Autorizzazioni

Generali ed alle Linee Guida emanate dall'Autorità Garante per la Protezione dei dati personali e, più in generale, alla normativa vigente in tema di protezione di dati personali, che qui deve intendersi integralmente richiamata.

DIFFUSIONE E AGGIORNAMENTO

Copia del presente Regolamento sarà esposto e reso accessibile a tutti gli operatori, collaboratori e autorizzati preposti al trattamento dei dati personali. Ne sarà curato l'aggiornamento periodico e sarà reso pubblico sul sito internet della Fondazione per una facile consultazione. Il presente regolamento potrà essere modificato o integrato qualora se ne ravvedesse la necessità da parte del Titolare del Trattamento.

Perugia lì 12/12/2018

Il Titolare del Trattamenti

Fondazione
SODALIZIO DI SAN MARTINO
IL PRESIDENTE
(Dott. Alfredo Arioti Branciforti)