FONDAZIONE CASA DI RIPOSO SAN GIUSEPPE O.N.L.U.S.

PROCEDURA PER LA GESTIONE DEI TEMPI DI CONSERVAZIONE

E CANCELLAZIONE DEI DOCUMENTI

INDICE SOMMARIO

1. PREMESSA

Al fine di garantire che lo svolgimento dei trattamenti di dati personali effettuati nel corso della propria attività di business avvenga ai sensi ed in conformità del Regolamento UE 679/2016 ("**Regolamento**" o "**GDPR**") e di eventuali altre normative applicabili in materia di protezione dei dati personali, **FONDAZIONE CASA DI RIPOSO SAN GIUSEPPE O.N.L.U.S**. ha predisposto una procedura finalizzata a definire i tempi di conservazione dei dati personali e ad assicurarne la cancellazione conformemente ai principi previsti dalla citata normativa, nel rispetto del principio di "*accountability*" previsto dal Regolamento.

2. AMBITO DI APPLICAZIONE

La presente procedura si applica:

- a tutto il personale in forza presso la Struttura, senza eccezione alcuna, ai collaboratori (a mero titolo esemplificativo, ai consulenti, ai rappresentanti, etc.) e a tutto il personale di strutture terze che, nell'ambito dei contratti di fornitura sottoscritti con la Struttura, a vario titolo accedono ai dati personali di cui la stessa è titolare (es. responsabili esterni del trattamento, subappaltatori, etc.);
- a tutti i documenti, le informazioni e/o i file contenenti dati personali (es. di dipendenti, collaboratori, pazienti, fornitori o altri soggetti terzi) di cui la Struttura è titolare o che la stessa tratta a vario titolo per conto di altri soggetti (es. altre strutture del Gruppo GHC), creati, utilizzati, archiviati ed elaborati in tutti i formati e mezzi, sia cartacei che elettronici (quando collettivamente richiamati, "**Documenti**"), così come meglio definiti al successivo art. 5.

Questa procedura va letta congiuntamente con le altre procedure eventualmente predisposte dalla Struttura in relazione alla sicurezza, alla protezione ed al corretto trattamento dei dati personali, che saranno rese disponibili agli interessati.

3. OBIETTIVO

La presente procedura ha l'obiettivo di definire gli indirizzi, i principi, le modalità ed i tempi di conservazione e cancellazione dei Documenti, nonché di individuare i soggetti responsabili della gestione dei processi di conservazione e cancellazione dei Documenti descritti nella presente procedura.

La conservazione dei Documenti (cd. "*Data Retention Management*") dovrà essere effettuata nel rispetto dei criteri indicati al successivo art. 6. La cancellazione dei Documenti (cd. "*Data Destruction Management*"), invece, dovrà rispettare quanto previsto dal successivo art. 7.

In ogni caso, dovranno essere rispettati tutti i tempi di conservazione dei Documenti previsti dalla tabella inserita in calce alla presente procedura ("**Tabella**"). Tale Tabella, ha lo scopo di descrivere ed elencare, in maniera schematica, i tempi di conservazione di ciascun documento, in quanto i dati personali trattati dalla Struttura (es. dati dei pazienti, dati relativi al personale dipendente, etc.) possono richiedere tempi di conservazione differenti nonché, in alcuni casi, essere necessari per finalità diverse da quelle per cui sono stati raccolti che richiedono l'eccezionale allungamento dei tempi di conservazione stabiliti (es. in caso di contenzioso, accertamenti delle Autorità, etc.).

4. LEGAL BACKGROUND

Il Regolamento prevede che il titolare del trattamento dei dati personali debba:

(i) conservare i dati personali 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;

(ii) assicurarsi che tale periodo di conservazione sia limitato al minimo necessario per perseguire le specifiche, legittime e predeterminate finalità del trattamento;

(iii) stabilire un termine per la cancellazione o la verifica periodica dei dati personali trattati e dei relativi tempi di conservazione, al fine di assicurare che i dati non siano conservati più a lungo del necessario.

I dati personali presenti nei Documenti, inoltre, potranno essere conservati per periodi di tempo più lunghi rispetto a quanto necessario per il conseguimento delle finalità per le quali sono stati raccolti solo laddove ricorra una delle eccezioni prevista al successivo art. 7.2.3.

5. DATI PERSONALI E INFORMAZIONI COPERTI DALLA PRESENTE PROCEDURA

La presente procedura si applica a tutti i dati personali presenti nei Documenti, ivi inclusi, a titolo meramente esemplificativo e non esaustivo:

- i dati personali raccolti e trattati sui database e i gestionali di funzione (es. pazienti, HR, IT, etc.) e archivi (inclusi gli archivi cartacei, di back-up, etc.) utilizzati dalla Struttura o comunque controllati o nella custodia della Struttura, su qualsivoglia mezzo in cui i dati sono conservati (es. desktop/laptop, server, sistemi di *storage* di rete, *smartphone*, *tablet*, dischi rigidi portatili, supporti rimuovibili, dispositivi di memoria flash, servizi di *storage* in cloud, etc.);
- i dati personali contenuti nei messaggi di posta elettronica e nella corrispondenza aziendale, negli elementi del calendario di Outlook, nei messaggi inviati e/o ricevuti via fax, nelle immagini raccolte tramite i sistemi di videosorveglianza, sul badge personale dei dipendenti/collaboratori, nelle copie cartacee e/o elettroniche di contratti, nei *sales records*, nei file di log e/o di back-up e nei documenti relativi ai pagamenti ricevuti o effettuati (es. contenenti dati bancari, numeri di carte di credito, etc.).

I principi e le regole stabiliti in questa procedura si riferiscono tanto ai Documenti cartacei quanto a quelli elettronici contenenti dati personali di titolarità della Struttura.

6. DATA RETENTION MANAGEMENT

6.1 I criteri per la conservazione

I termini di conservazione dei dati sono determinati dai soggetti indicati al successivo art. 6.2:

(i) sulla base di esigenze aziendali connesse alle originarie finalità del trattamento, per le quali i dati sono stati raccolti (c.d. "*finalità principale*");

(ii) sulla base di esigenze aziendali collegate a finalità secondarie del trattamento (c.d. "*secondary use*") per le quali vi sia un espresso consenso dell'interessato o la sussistenza di un legittimo interesse della Struttura o di un terzo (es. tutela di un diritto in sede giudiziaria, etc.);

(iii) sulla base di eventuali obblighi normativi che impongono la conservazione dei dati per un periodo di tempo successivo al termine del trattamento;

(iv) sulla base di esigenze di analisi e statistiche che richiedono necessariamente la conservazione dei dati per un periodo di tempo ulteriore rispetto a quanto previsto ai punti che precedono, solo se i dati sono previamente anonimizzati e/o sono state adottate le misure di sicurezza previste al successivo art. 7.2.3.

6.2 I soggetti competenti e le procedure

In ottemperanza ai c.d. principi fondamentali di "*Protezione dei dati fin dalla progettazione*" (c.d. "*Privacy by Design*") e "*Privacy come impostazione predefinita*" (c.d. "*Privacy by Default*") previsti dal Regolamento[1], la Struttura è tenuta a:

- effettuare un'analisi dei tempi di conservazione dei dati personali trattati;
- tenendo conto dei criteri di cui al precedente art. 6.1, individuare i tempi di conservazione ritenuti adeguati, valutando, ove necessario, le misure di sicurezza tecniche ed organizzative da adottare per la conservazione sicura dei dati, avuto altresì riguardo alle misure già presenti all'interno della Struttura e dei relativi costi di attuazione ("**Proposta**");
- verificare, con cadenza almeno annuale, i dati personali trattati, i loro tempi di conservazione (come indicati nella Tabella), il rispetto (o meno) dei criteri di cui al precedente 6.1, la presenza di "*eccezioni*" (come indicate al successivo art. 7.2.3).

6.3 Obblighi del personale

La Struttura ha il dovere di assicurare e verificare la corretta applicazione di questa procedura; il personale e i collaboratori hanno il dovere di segnalare alla Struttura ogni eventuale violazione della stessa.

Se, nell'ambito dell'attività lavorativa, dovessero essere rinvenuti Documenti contenenti dati personali che non rientrino nelle regole di conservazione stabilite è fatto dovere al personale e ai collaboratori della Struttura di rivolgersi immediatamente alla stessa.

7. DATA DESTRUCTION MANAGEMENT

7.1 Procedure di cancellazione e autorizzazioni

La cancellazione di determinati Documenti contenenti dati personali può essere effettuata:

1. in seguito al venir meno dei tempi di conservazione previsti;
2. per far fronte ad una richiesta di cancellazione dei dati pervenuta dagli interessati;
3. da uno o più dipendenti/collaboratori della Struttura, nel corso dello svolgimento della loro normale attività lavorativa.

7.1.1 *Gestione delle richieste di cancellazione pervenute dagli interessati*

Le richieste di cancellazione dei dati pervenute dagli interessati saranno gestite secondo la procedura che segue.

Ai sensi dell'art. 17 del Regolamento, l'interessato (es. il paziente, il dipendente, il fornitore, ecc.) ha il diritto di richiedere e ottenere senza ritardo (e in ogni caso entro 30 giorni – o 3 mesi, in ipotesi di complessità della richiesta o elevato numero di richieste) la cancellazione dei propri dati personali raccolti, trattati e conservati dalla Struttura, se ricorre una delle seguenti circostanze:

---

1 Ai sensi dei quali la Struttura è tenuta, da un lato, "*sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, a mettere in atto misure tecniche e organizzative adeguate, quali la pseudo-anonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati*" e, dall'altro, "*a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento*".

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati dalla Struttura (es. per obblighi di legge, per finalità primarie, per *secondary use*, etc.);

b) l'interessato revoca il consenso su cui si basa il trattamento dei propri dati personali;

c) l'interessato si oppone al trattamento dei propri dati personali e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

d) i dati personali sono stati trattati illecitamente da parte della Struttura (o da terzi, anche per conto della Struttura);

e) i dati personali devono essere cancellati per adempiere un obbligo di legge, regolamento, normativa applicabile nazionale o Europea.

In caso di ricezione di una richiesta da parte dell'interessato, il soggetto ricevente è tenuto a trasmettere senza indugio la comunicazione ricevuta alla Struttura che a sua volta procederà, nell'ordine, a:

1. verificare la sussistenza di uno o più requisiti previsti alle precedenti lettera da a) a e);
2. in caso di sussistenza di o più dei predetti requisiti, cancellare senza ritardo i dati personali degli interessati, rispettando le modalità di cancellazione indicate nella presente procedura ed avvalendosi, in caso di documenti elettronici, anche di personale IT specializzato;
3. comunicare le cancellazioni effettuate a ciascuno dei destinatari cui i dati personali siano stati trasmessi, salvo che ciò si riveli impossibile od implichi uno sforzo sproporzionato (ad es. per il numero elevato di destinatari in questione);
4. nel caso in cui i dati siano cancellati stati resi pubblici, informare i titolari del trattamento che li stanno trattando della richiesta ricevuta.

7.1.2 *Cancellazione dei dati da parte dei dipendenti/collaboratori*

Infine, la cancellazione dei Documenti (sia cartacei che informatici) contenenti dati personali può essere effettuata anche dai dipendenti/collaboratori della Struttura, nel corso dello svolgimento della loro normale attività lavorativa. Tuttavia, al fine di delineare una procedura volta alla gestione ordinata e controllata della cancellazione dei dati personali da parte dei predetti soggetti, occorre, in via preliminare, distinguere tra:

- documenti ufficiali della Struttura: con tale definizione si intendono tutti quei Documenti che hanno specifica rilevanza per l'attività di impresa della Struttura e che devono essere necessariamente custoditi e conservati con attenzione, anche al fine di essere prodotti in giudizio in caso di contenziosi e/o precontenziosi in cui la Struttura è parte - quali, a titolo esemplificativo e non esaustivo, documentazione clinica dei pazienti, delibere delle riunioni della Struttura, copie originali dei contratti con i fornitori, ecc.;
- documenti non ufficiali della Struttura: con tale definizione si intendono tutti quei Documenti contenenti dati personali utilizzati dai dipendenti/collaboratori della Struttura nel corso del normale svolgimento dell'attività lavorativa che costituisco mere copie di Documenti ufficiali – quali, a titolo esemplificativo e non esaustivo, copie non originali dei contratti con i fornitori, delle fatture emesse, duplicati di e-mail inviate e/o ricevute.

L a cancellazione dei documenti non ufficiali può essere richiesta dal personale e/o dai collaboratori della Struttura, previa verifica della conservazione dei rispettivi Documenti ufficiali e purché siano rispettate eventuali indicazioni e/o istruzioni ricevute dalla Struttura stessa, se necessario.

L a cancellazione dei documenti ufficiali, invece, potrà essere effettuata esclusivamente nel rispetto della seguente procedura:

- il dipendente/collaboratore inoltra alla Struttura, *via e-mail,* il documento ufficiale da cancellare e la informa della volontà di procedere alla cancellazione dello stesso, illustrandone in modo circostanziato le ragioni;
- la Struttura esamina senza indugio la richiesta ricevuta, anche alla luce dei criteri di conservazione indicati al precedente art. 6.1, e:
  - autorizza la cancellazione del documento ufficiale in questione, ordinando la cancellazione al personale autorizzato ad effettuare tali operazioni; o, in alternativa,
  - rigetta la richiesta con comunicazione motivata nei confronti del richiedente.

I documenti ufficiali pertanto non potranno, in nessun caso, essere cancellati dai dipendenti/collaboratori e/o, in generale, dal personale della Struttura senza aver ottenuto la previa autorizzazione della stessa.

7.2 Istruzioni per la cancellazione e distruzione

La cancellazione e la distruzione dei Documenti, cartacei ed informatici, contenenti dati personali deve essere effettuata nel rispetto delle modalità indicate ai successivi paragrafi 7.2.1 e 7.2.2, volte a rendere inintelligibili o irreperibili in maniera irreversibile i dati personali.

Tali modalità si applicano a qualunque supporto e/o sistema di memorizzazione in cui i Documenti contenenti dati personali sono trattati e/o conservati (quali, ad esempio, format *online*, supporti elettronici, stampanti, CD, memorandum e documenti interni, ecc.).

7.2.1. Documenti cartacei (ufficiali e non ufficiali)

I dati personali trattati e/o conservati su documenti cartacei devono essere distrutti attraverso gli appositi distruggi-documenti (c.d. *shredding*), affinché i documenti siano distrutti in modo tale da rendere ragionevolmente impossibile il loro riassemblaggio e di conseguenza la ricostruzione (anche solo parziale) delle informazioni in essi contenute.

In particolare, per rendere efficiente questo processo, si forniscono di seguito alcune linee guida e *best practice* che devono essere osservate in relazione alla distruzione dei Documenti cartacei contenenti dati personali:

- la distruzione dei Documenti contenenti dati personali deve coinvolgere non solo il documento "principale", ma anche le sue eventuali ulteriori copie e precedenti versioni stampate, copie locali, versioni non ufficiali (c.d. *drafts*);
- è importante evitare di lasciare i Documenti contenenti dati personali incustoditi nei pressi dei distruggi-documenti, nell'attesa di provvedere alla loro distruzione (ciò, infatti, potrebbe consentire a soggetti non autorizzati di averne visione o di acquisirli);
- occorre altresì evitare di distruggere i Documenti cartacei contenenti dati personali senza avvalersi dei distruggi-documenti (per esempio, strappando il documento e gettandolo nel cestino).

7.2.2. Documenti elettronici (ufficiali e non ufficiali)

I Documenti contenenti dati personali trattati e/o conservati per mezzo di uno strumento elettronico (i.e. qualsiasi mezzo utilizzato per raccogliere, creare, trattare, conservare e trasmettere dati personali, inclusi, senza limitazione, *hard disk*, nastri magnetici, *desktop/laptop*, *server*, sistemi di *storage* di rete, *smartphone*, *tablet*, supporti rimuovibili, dispositivi di memoria flash, servizi di *storage* in *cloud*, *zip*, nonché le relative copie di *backup* dei dati) devono essere cancellati e distrutti (o trasformati in forma non intelligibile) secondo le modalità di seguito descritte.

1. Cancellazione sicura delle informazioni, ottenibile con software e programmi informatici (quali "*wiping program"* o *"file shredder"*) che provvedono, una volta che l'utente abbia eliminato un *file* da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi (ad es., con l'uso del "cestino" o con comandi di cancellazione), a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

2. Demagnetizzazione ("*degaussing*") dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, *floppy-disk*, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione *software* (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

3. In determinati casi:

    a. anonimizzazione permanente dei dati personali, quale tecnica con cui i dati sono modificati irreversibilmente in modo tale che l'interessato a cui essi si riferiscono non possa più essere identificato direttamente o indirettamente, né dalla Struttura autonomamente né in collaborazione con altri soggetti. L'elemento fondamentale dell'anonimizzazione è l'irreversibilità delle modifiche subite dai dati personali per consentirne il recupero diretto o indiretto;

b. distruzione fisica degli strumenti elettronici, praticabile con i supporti ottici a sola lettura (es. CD-ROM, DVD-R), che possono essere distrutti o polverizzati con appositi macchine analoghe ai distruggi-documenti in uso negli uffici.

Tali misure tecniche, suscettibili di aggiornamento alla luce dell'evoluzione tecnologica, hanno lo scopo di evitare che i Documenti e i relativi dati personali siano reperibili reversibilmente e di impedire a soggetti non autorizzati, che abbiano a vario titolo la disponibilità materiale dei supporti di elettronici di memorizzazione, di venirne a conoscenza.

E' importante, pertanto:

- che il processo di distruzione/cancellazione dei Documenti elettronici contenenti dati personali non si esaurisca nel semplice sposamento del file e/o documento (elettronico o cartaceo) nel "cestino";
- che non siano utilizzate modalità di cancellazione dei dati non previste dal presente paragrafo (es. formattazione del disco, cifratura unidirezionale, in grado di mantenere parte dei dati personali intatta ed eventualmente accessibile o ripristinabile da soggetti non autorizzati);
- che anche in caso di riutilizzo, trasferimento, ricollocamento presso altri soggetti/funzioni (anche all'esterno), riciclo o dismissione di strumenti elettronici contenenti dati personali, sia rispettata la procedura di *Data Destruction Management* descritta in questa procedura.

7.2.3 *Eccezioni alla cancellazione dei dati personali*

Come detto al precedente art. 6.1, i tempi di conservazione dei dati sono determinati sulla base dei criteri ivi indicati. Tuttavia, tali termini di conservazione - e, quindi, la cancellazione/distruzione dei dati personali -possono essere soggetti a specifiche eccezioni allorquando la conservazione dei dati sia necessaria per:

a) esigenze di analisi e statistiche che richiedono necessariamente la conservazione dei dati per un periodo di tempo ulteriore rispetto a quanto necessario per il perseguimento delle finalità del trattamento. In tali circostanze, in ossequio all'art. 89 del Regolamento, saranno adottate misure tecniche e organizzative adeguate al fine di garantire il rispetto dei diritti e delle libertà degli interessati, quali, a titolo esemplificativo e non esaustivo, la pseudo-anonimizzazione dei dati;

b) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria da parte della Struttura[2];

c) dare esecuzione ad una richiesta di esercizio del diritto di accesso ai dati, di rettifica dei dati, di limitazione del trattamento (c.d. "*congelamento*" dei dati) e di portabilità dei dati rivolta alla Struttura dagli interessati che rende necessario il trattamento degli stessi;

d) dare esecuzione ad una comunicazione di avviso (c.d. "*Stop Notice*") da parte della Struttura che identifichi i Documenti contenenti dati personali che dovranno essere oggetto di ulteriore conservazione.

In nessun caso, pertanto, potrà essere proseguita la conservazione dei Documenti contenenti dati personali oltre i termini indicati nella Tabella senza aver ottenuto la previa autorizzazione dei soggetti indicati nella precedente procedura.

Concluso il processo sopra delineato, la Struttura, in caso di modifica/aggiornamento dei termini di conservazione, provvede all'aggiornamento/modifica della Tabella.

8. VIOLAZIONI DI QUESTA PROCEDURA E SEGNALAZIONI

La Struttura vieta a tutto il proprio personale (e.g. dipendenti, collaboratori, consulenti) e ad altre terze parti di conservare e procedere alla cancellazione/distruzione di Documenti contenenti dati personali in violazione della presente procedura e dei tempi di conservazione previsti dalla Tabella presente in calce alla stessa.

La Struttura, pertanto, invita tutto il proprio personale a segnalare prontamente qualsiasi evento e/o condotta che potrebbe portare alla violazione delle regole previste da questa procedura, inviando una *e-mail* all'indirizzo ***privacy@fondazionesangiuseppebordighera.it***

---

2 In talune circostanze, infatti, la Struttura può essere coinvolta in eventi inaspettati quali, ad esempio, contenziosi legali (o procedure pre-contenziose), richieste/investigazioni delle Autorità competenti (e.g. autorità giudiziaria, polizia postale, Garante Privacy, etc.), che richiedano l'accesso e il mantenimento di specifici Documenti contenenti dati personali al fine di accertare o tutelare i propri diritti o perseguire propri legittimi interessi o legittimi interessi di terzi (es. pazienti, fornitori, etc.). In questi casi, eccezionalmente, tali Documenti non possono essere cancellati secondo i tempi di conservazione previsti, che pertanto ricominciano a decorrere alla cessazione dell'evento (es. chiusura del contenzioso legale, etc.).

Qualsiasi violazione di questa procedura, infatti, può avere conseguenze legali e reputazionali anche gravi per l a Struttura, oltre che provocare danni materiali alla Struttura stessa e al proprio business, costituire inadempimento delle obbligazioni previste dal Regolamento ed esporre la stessa alle sanzioni ivi previste.

L a Struttura si riserva il diritto di intervenire sul piano disciplinare nei confronti del personale e/o dei propri collaboratori nei casi più gravi di mancato rispetto delle regole previste nella presente procedura.