fondazione evidence ONLUS

# Fondazione Evidence per Attività e Ricerche Cardiovascolari ONLUS
# Via Gaetano Donizzetti, 30, Milano
# P.IVA: 05074180968

# Politica generale sulla protezione dei dati personali

| | |
|---|---|
| Codice: | POL01 |
| Revisione: | 1 |
| Data della revisione: | 23/04/2019 |
| Redatta da: | Luca Oldrini |
| Approvata da: | Marina Cornacchia Schenetti |

**STATO DELLE REVISIONI**

| Rev. | Data | Descrizione delle modifiche | Approvazione |
|---|---|---|---|
| 01 | 23/04/2019 | Prima redazione del documento | Marina Cornacchia Schenetti |
| | | | |
| | | | |

# Indice

# 1. Scopo, campo di applicazione e destinatari

Fondazione Evidence, da ora in poi definita come “Fondazione”, si impegna a essere conforme alle leggi e ai regolamenti applicabili relativi alla protezione dei dati personali nei paesi dove questa opera.

La presente procedura definisce i principi fondamentali secondo i quali la Fondazione tratta i dati personali di clienti, fornitori, business partner, dipendenti ed altri individui, ed indica le responsabilità dei propri servizi e dei propri dipendenti nel trattamento dei dati personali.

La presente procedura si applica alla Fondazione e alle sue controllate (direttamente o indirettamente) che svolgono la propria attività all’interno dell’Area Economica Europea o trattano dati personali di interessati in tale area.

I destinatari della presente procedura sono tutti i dipendenti, temporanei o permanenti, e tutti i collaboratori che operano per conto della Fondazione.

# 2. Riferimenti normativi

- GDPR 2016/679 (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche in materia di trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la Direttiva 95/46 / CE)
- Leggi nazionali o regolamenti rilevanti per l’implementazione del Regolamento
- Politica di conservazione dei dati
- Registro dei trattamenti
- Procedura di richiesta di accesso e manutenzione dei dati
- Procedura trasferimento transfrontaliero dei dati
- Procedura di risposte agli interessati

# 3. Definizioni

Le definizioni utilizzate nel presente documento sono tratte dall’articolo 4 del Regolamento Europeo:

**«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 sensibili**: dati personali che, per loro natura, sono particolarmente sensibili in relazione ai diritti e alle libertà fondamentali e meritano una protezione specifica in quanto il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Questi dati personali includono dati personali che rivelano origine razziale o etnica, opinioni

politiche, credenze religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici che identificano in modo univoco una persona fisica, dati sulla salute o dati relativi all'orientamento sessuale della persona.

**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;

**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;

**Anonimizzazione:** de- identificazione irreversibile dei dati personali in modo tale che la persona non può essere identificata tramite tecnologie e in tempi e costi ragionevoli né dal titolare né da altra persona. I principi di trattamento dei dati personali non si applicano ai dati anonimi in quanto questi non sono considerati dati personali.

**Pseudonimizzazione**: 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; la pseudonimizzazione riduce, ma non elimina del tutto, la possibilità di collegare un dato personale a un interessato. Tenendo conto che i dati che hanno subito il processo di pseudonimizzazione sono ancora dati personali, tale processo deve essere conforme ai principi di trattamento dei dati personali.

**Trattamento transfrontaliero**: trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

**Autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

**Autorità di controllo principale**: l'autorità di vigilanza con la responsabilità primaria di occuparsi di un'attività di trattamento di dati transfrontaliera, ad esempio quando un interessato presenta un reclamo in merito al trattamento dei propri dati personali; è responsabile, tra l'altro, di ricevere le notifiche di violazione dei dati, di essere informato sulle

attività di trattamento rischiose e avrà piena autorità per quanto riguarda i suoi obblighi di garantire l'osservanza delle disposizioni del GDPR;

Ciascuna "**autorità di vigilanza locale**" manterrà comunque la sua attività nel proprio territorio e monitorerà qualsiasi trattamento di dati a livello locale che riguarda gli interessati o che viene effettuato da un titolare o un responsabile UE o non UE quando il loro trattamento si rivolge agli interessati che risiedono sul suo territorio. I loro compiti e poteri comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni, la promozione a livello generale della consapevolezza dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati personali, nonché l'accesso a qualsiasi sede del responsabile del titolare e del responsabile, compresi eventuali strumenti e mezzi per il trattamento dei dati.

**Stabilimento principale**: per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

**Stabilimento principale**: con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

**Gruppo imprenditoriale:** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

# 4. Principi base del trattamento dei dati personali

I principi sulla protezione dei dati delineano le responsabilità base per le organizzazioni che si occupano del trattamento dei dati personali. L'articolo 5, punto 2 del Regolamento stabilisce che "*il titolare del trattamento è responsabile e deve dimostrare la conformità a tali principi".*

## 4.1. Legalità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, equo e trasparente in relazione all'interessato.

## 4.2. Limitazione dello scopo

I dati personali devono essere raccolti per scopi specifici, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi.

### 4.3. Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per i quali sono trattati. Se possibile per ridurre i rischi per gli interessati la Fondazione deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali.

### 4.4. Precisione

I dati personali devono essere accurati e, ove necessario, aggiornati; misure ragionevoli devono essere prese per garantire che i dati personali inaccurati, in relazione alle finalità per cui sono trattati, siano cancellati o rettificati in modo tempestivo.

### 4.5. Limitazione del periodo di conservazione

I dati personali devono essere conservati per un periodo non superiore a quello necessario agli scopi per i quali i dati personali sono trattati.

### 4.6. Integrità e confidenzialità

Tenendo conto dello stato della tecnologia e di altre misure di sicurezza disponibili, dei costi di implementazione e della probabilità e della gravità dei rischi dei dati personali, la Fondazione deve utilizzare misure tecniche o organizzative adeguate per trattare i dati personali in modo tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro la distruzione, la perdita, l'alternanza o la divulgazione accidentale o illecita o l'accesso non autorizzato.

### 4.7. Responsabilità

I responsabili del trattamento dei dati sono responsabili di dimostrare la conformità ai principi sopra descritti.

## 5. Integrare la protezione dei dati nelle attività commerciali

Al fine di dimostrare la conformità ai principi della protezione dei dati, l’organizzazione deve integrare la protezione dei dati nelle attività commerciali.

### 5.1. Informativa agli interessati

(Vedi la sezione Linee Guida sul corretto trattamento)

### 5.2. Scelta e consenso dell’interessato

(Vedi la sezione Linee Guida sul corretto trattamento)

### 5.3. Raccolta

La Fondazione deve cercare di raccogliere il minor numero possibile di dati personali. Se i dati personali sono raccolti da una terza parte, il Titolare deve assicurarsi che i dati personali siano raccolti secondo le previsioni di legge.

## 5.4. Utilizzo, conservazione e smaltimento

Gli scopi, i metodi, i limiti di archiviazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'informativa sulla protezione dei dati generali.

La Fondazione deve mantenere l'accuratezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base allo scopo del trattamento. È necessario utilizzare adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati o utilizzati in modo improprio e prevenire le violazioni dei dati personali. il Titolare è responsabile della conformità ai requisiti elencati in questa sezione.

## 5.5. Divulgazione a terzi

Ogni volta che la Fondazione utilizza un fornitore di terza parte o un partner commerciale per trattare i dati personali per suo conto, il referente privacy deve garantire che questo processore fornisca misure di sicurezza per salvaguardare i dati personali appropriate ai rischi associati. A tal fine, è necessario utilizzare apposito questionario di conformità.

La Fondazione deve richiedere contrattualmente al fornitore o al partner commerciale di fornire lo stesso livello di protezione dei dati. Il fornitore o il partner commerciale deve elaborare i dati personali solo per adempiere ai propri obblighi contrattuali nei confronti della Fondazione o dietro istruzioni della Fondazione e non per altri scopi. Quando l'Azienda tratta i dati personali congiuntamente con una terza parte indipendente, la Fondazione deve specificare esplicitamente le rispettive responsabilità e la terza parte nel rispettivo contratto o in qualsiasi altro documento legalmente vincolante, come il Contratto di trattamento dei dati del fornitore.

## 5.6. Trasferimento transfrontaliero dei dati personali

Prima di trasferire i dati personali dallo Spazio economico europeo (SEE) devono essere utilizzate misure di salvaguardia adeguate, compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione europea e, se necessario, deve essere ottenuta l'autorizzazione da parte della autorità di protezione dei dati. L'entità che riceve i dati personali deve rispettare i principi del trattamento dei dati personali stabiliti nella Procedura di trasferimento dei dati transfrontalieri.

## 5.7. Diritti di accesso degli interessati

Quando agisce come titolare del trattamento dei dati, la Fondazione è tenuta a fornire agli interessati un ragionevole meccanismo di accesso che consenta loro di accedere ai propri dati personali e deve consentire loro di aggiornare, correggere, cancellare o trasmettere i propri dati personali, se del caso o richiesto dalla legge. Il meccanismo di accesso sarà ulteriormente dettagliato nella Procedura di richiesta di accesso ai dati dell'interessato.

## 5.8. Portabilità dei dati

Gli interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che hanno fornito in un formato strutturato e di trasmettere gratuitamente tali dati a un altro titolare. il Titolare è

responsabile di garantire che tali richieste vengano elaborate entro un mese, non siano eccessive e non pregiudichino i diritti sui dati personali di altre persone.

### 5.9. Diritto all'oblio

Su richiesta l'interessato ha il diritto di ottenere dalla Fondazione la cancellazione dei suoi dati personali. Quando la Fondazione agisce in qualità di titolare del trattamento, il referente privacy deve intraprendere le azioni necessarie (comprese le misure tecniche) per informare le terze parti che usano o trattano quei dati di adeguarsi alla richiesta.

## 6. Linee guida sul corretto trattamento

I dati personali possono essere trattati solo se esplicitamente autorizzati dal titolare.

La Fondazione deve decidere se effettuare una valutazione di impatto sulla protezione dei dati per ogni attività di trattamento dei dati secondo quanto definito dalle Linee guida sulla valutazione dell'impatto sulla protezione dei dati dati personali.

### 6.1. Informativa agli interessati

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento incluso ma non limitato alla vendita di prodotti, servizi o attività di marketing, il Titolare è responsabile di informare adeguatamente gli interessati di quanto segue: la tipologia di dati personali raccolti, le finalità del trattamento, i metodi di trattamento, i diritti degli interessati in relazione ai loro dati personali, il periodo di conservazione, i potenziali trasferimenti internazionali di dati, se i dati saranno condivisi con terzi e le misure di sicurezza della Fondazione per proteggere i dati personali. Queste informazioni sono fornite tramite un'informativa generale sulla protezione dei dati.

Se l'azienda ha molteplici attività di trattamento dei dati, occorrerà sviluppare diverse comunicazioni che saranno diverse a seconda dell'attività di trattamento e delle categorie di dati personali raccolti, ad esempio, un'informativa potrebbe essere scritta per le spedizioni via mail e una diversa per la spedizione via posta ordinaria.

Laddove i dati personali siano condivisi con terzi, il Titolare deve garantire che gli interessati siano stati informati di ciò tramite un'informativa generale sulla protezione dei dati

Laddove i dati personali siano trasferiti in un paese terzo in base alla politica di trasferimento dei dati transfrontalieri, l'informativa generale sulla protezione dei dati dovrebbe specificarlo, indicando chiaramente dove e a quale entità vengono trasferiti i dati personali.

Nel caso in cui vengano raccolti dati personali sensibili, il Data Protection Officer deve assicurarsi che l'informativa generale sulla protezione dei dati chiarisca espressamente lo scopo per il quale tali dati sensibili vengono raccolti.

La modalità per l'esercizio dei diritti degli interessati è definita mediante comunicazione all'indirizzo di posta: fondevidence@gmail.com.

### 6.2. Ottenimento dei consensi

Ogni qualvolta il trattamento dei dati personali è basato sul consenso dell'interessato, o su altri motivi legittimi, il Titolare è responsabile di conservare una registrazione di tale consenso. Il Titolare è responsabile di presentare alle persone interessate le diverse opzioni per fornire il consenso e deve informare e garantire che il loro consenso (ogni volta che viene utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento.

Quando viene richiesto di correggere, modificare o distruggere registrazioni di dati personali, il Referente Privacy deve garantire che tali richieste siano gestite entro un ragionevole lasso di tempo. Il Referente Privacy deve anche registrare le richieste e tenere un apposito registro.

I dati personali devono essere trattati solo per lo scopo per il quale sono stati originariamente raccolti. Nel caso in cui la Fondazione desideri trattare i dati personali raccolti per un altro scopo, la Fondazione deve richiedere il consenso dei suoi interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo dovrebbe includere lo scopo originale per cui sono stati raccolti i dati e anche gli scopi nuovi o aggiuntivi. La richiesta deve includere anche il motivo del cambiamento di scopo / i. Il Referente Privacy è responsabile del rispetto delle regole in questo paragrafo.

Ora e in futuro, il Referente Privacy deve garantire che i metodi di raccolta siano conformi alla legge, alle buone pratiche e agli standard industriali pertinenti.

Il Referente Privacy è responsabile della creazione e della manutenzione di un registro delle informative generali sulla protezione dei dati.

## 7. Organizzazione e responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori all'interno della Fondazione o per suo conto e abbia accesso ai dati personali da essa trattati.

Le principali aree di responsabilità per il trattamento dei dati personali sono riferibili ai seguenti ruoli organizzativi:

Il **Consiglio di Amministrazione** o altro organo decisionale competente prende decisioni e approva le strategie generali della Fondazione in materia di protezione dei dati personali.

Il **referente Privacy** è responsabile della gestione del programma di protezione dei dati personali e dello sviluppo e della promozione delle procedure end-to-end di protezione dei dati personali;

Il **Referente Privacy** monitora e analizza le leggi sui dati personali e le modifiche alle normative, sviluppa i requisiti di conformità e assiste i reparti aziendali nel raggiungimento dei loro obiettivi relativi ai dati personali.

Egli è responsabile di:

- Approvare di qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni quali e-mail e lettere.
- Affrontare qualsiasi quesito in merito alla protezione dei dati da parte di giornalisti o altri mezzi di informazione come giornali.
- Ove necessario, collaborare con il Data Protection Officer per garantire che le iniziative di marketing rispettino i principi di protezione dei dati.
- Migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti.
- Organizzare per i dipendenti che lavorano con dati personali formazione per aumentare la competenza in materia di protezione dei dati personali e la consapevolezza.
- Garantire la protezione end-to-end dei dati personali dei dipendenti. Deve garantire che i dati personali dei dipendenti vengano elaborati in base a finalità legittime e alle necessità aziendali del datore di lavoro.

L'**IT manager (in outsourcing)** è responsabile di:

- garantire che tutti i sistemi, i servizi e le attrezzature utilizzate per l'archiviazione dei dati abbiano standard di sicurezza adeguati
- effettuare controlli periodici ed esami per verificare il livello di sicurezza dell'hardware e il funzionamento corretto del software.

Il **Titolare del Trattamento** è responsabile del trasferimento delle responsabilità di protezione dei dati personali ai fornitori e del miglioramento dei livelli di consapevolezza dei fornitori in materia di protezione dei dati personali, nonché della trasmissione dei requisiti dei dati personali a qualsiasi fornitore terzo che utilizza. Il Titolare deve garantire che la Fondazione si riserva il diritto di controllare i fornitori mediante audit.

## 8. Risposta agli incidenti di violazione dei dati personali

Quando la Fondazione viene a conoscenza di una sospetta o reale violazione dei dati personali, Il Referente Privacy deve condurre un'indagine interna e prendere appropriati provvedimenti in maniera tempestiva, secondo quanto previsto dalla procedura per la violazione dei dati. Se ci sono delle minacce ai diritti e alle libertà degli interessati, la Fondazione deve notificarle alle autorità per la protezione dei dati senza alcun ritardo, e se possibile, entro 72 ore.

## 9. Audit e responsabilità

L'ufficio audit o altri uffici rilevanti sono responsabili di verificare la corretta applicazione della presente procedura da parte delle altre aree aziendali.

Chiunque violerà la presente procedura sarà oggetto di un'azione disciplinare, e se la violazione commessa infrangerà leggi o regolamenti la persona sarà soggetta anche a responsabilità civili e penali.

## 10. Conflitti di legge

Tale procedura intende essere conforme con le leggi ed i regolamenti vigenti nei paesi dove è ubicata e dove opera la Fondazione. In caso di conflitto tra questa procedura e le leggi ed i regolamenti applicabili, prevalgono questi ultimi.

## 11. Gestione e validità del documento

Il responsabile del documento è il Referente Privacy, che ha il compito di controllarlo e, se necessario, aggiornarlo, almeno annualmente.