**Sommario**

[1. Campo d’applicazione, scopo e destinatari 2](#_Toc513191978)

[2. Documenti di Riferimento 2](#_Toc513191979)

[3. Definizioni 2](#_Toc513191980)

[4. Principi Applicabili al Trattamento dei Dati Personali 4](#_Toc513191981)

[4.1 Liceità, Correttezza e Trasparenza 4](#_Toc513191982)

[4.2 Limitazione delle Finalità 4](#_Toc513191983)

[4.3 Minimizzazione dei Dati 4](#_Toc513191984)

[4.4 Esattezza 5](#_Toc513191985)

[4.5 Limitazione del Periodo di Conservazione 5](#_Toc513191986)

[4.6 Integrità e riservatezza 5](#_Toc513191987)

[4.7 Responsabilizzazione 5](#_Toc513191988)

[5 Costruire la protezione dei dati nelle attività commerciali 5](#_Toc513191989)

[5.1 Notifica agli Interessati 5](#_Toc513191990)

[5.2 Scelta e Consenso dell’Interessato 5](#_Toc513191991)

[5.3 Raccolta 5](#_Toc513191992)

[5.4 Uso, Conservazione e Smaltimento 5](#_Toc513191993)

[5.5 Divulgazione a terzi 6](#_Toc513191994)

[5.6 Trasferimento Transfrontaliero dei Dati Personali 6](#_Toc513191995)

[5.7 Portabilità dei Dati 6](#_Toc513191996)

[5.8 Diritto all’oblio 6](#_Toc513191997)

[6 Linee guida sul Corretto Trattamento 6](#_Toc513191998)

[6.1 Comunicazioni agli Interessati 6](#_Toc513191999)

[6.2 Ottenere i Consensi 7](#_Toc513192000)

[7 Organizzazione e Responsabilità 7](#_Toc513192001)

[8 Risposta agli incidenti di Violazione dei Dati Personali 9](#_Toc513192002)

[9 Audit e Responsabilizzazione 9](#_Toc513192003)

[10 Conflitti con la Legge 9](#_Toc513192004)

[11 Gestione delle registrazioni sulla base di questo documento 9](#_Toc513192005)

[12 Validità e gestione del documento 10](#_Toc513192006)

1. **Campo d’applicazione, scopo e destinatari**

L’Associazione della Croce Rossa Italiana, in seguito denominata "CRI", si impegna a rispettare le leggi e i regolamenti applicabili relativi alla protezione dei dati personali nei paesi in cui CRI opera. Questa Politica stabilisce i principi di base con cui CRI tratta i dati personali di consumatori, clienti, fornitori, partner commerciali, dipendenti e altre persone e indica le responsabilità dei propri dipartimenti aziendali e dipendenti durante il trattamento dei dati personali.

La presente politica si applica alla CRI e alle aziende che controlla direttamente o indirettamente che svolgono attività all'interno dello Spazio Economico Europeo (SEE) o che trattano i dati personali degli interessati all'interno del SEE.

I destinatari di questo documento sono tutti i dipendenti, permanenti o temporanei, e tutti i collaboratori che lavorano per conto della CRI.

# **Documenti di Riferimento**

* 1. Il GDPR dell’UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
  2. D.Lgs 196/2003
  3. altre leggi e regolamenti locali]
  4. Elenco dei trattamenti
  5. Descrizione dei Ruolo del Titolare
  6. Descrizione dei Ruolo del Responsabile della Protezione dei Dati
  7. Descrizione dei Ruolo del Responsabile esterno
  8. Descrizione dei Ruolo degli Addetti
  9. Informativa Privacy per il sito internet
  10. Informativa Provacy per i Dipendenti
  11. Politica di Conservazione dei Dati
  12. Metodologia di Valutazione d'Impatto sulla Protezione dei Dati
  13. DPIA - Data Privacy Impact Assessment
  14. Politica conservazione dei dati
  15. Procedura di Comunicazione di una Violazione di Dati

# **Definizioni**

Le seguenti definizioni di termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (o 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.

**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.

**le cc.dd. categorie particolari di dati personali**: i dati personali inerenti l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona. Nello specifico:

\* **“dati genetici”**: i dati personali elativi alle caratteristiche genetiche ereditarie o acquisite di una persona 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 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;

\* **“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.

**Titolare** : 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 dei dati**: una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare.

**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**: Deidentificazione irreversibile dei dati personali in modo tale che la persona non possa essere identificata utilizzando tempi, costi e tecnologie ragionevoli da parte del Titolare o di qualsiasi altra persona per identificare l’interessato. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile.

**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 completamente, la possibilità di collegare il dato personale all’interessato. Poiché i dati pseudominizzati sono comunque dati personali, il trattamento dei dati pseudonimizzati dovrebbe essere conforme ai principi del Trattamento dei Dati Personali.

**Autorità di Controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell’UE;

**Autorità di Controllo Capofila**: L’autorità di controllo con la responsabilità primaria di gestire 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 notificato su attività di trattamento rischiose e avrà piena autorità per quanto riguarda le sue funzioni per garantire l'osservanza delle disposizioni del GDPR dell'UE;

Ogni “**autorità di controllo locale**” manterrà comunque nel proprio territorio e monitorerà qualsiasi trattamento di dati locale che incide sugli interessati o che viene effettuato da un Titolare o un processore all’interno dell’Unione oppure all’esterno dell’Unione in caso il loro trattamento si rivolge a interessati residenti sul proprio territorio. I loro compiti e poteri comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni, la promozione della consapevolezza da parte del pubblico dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati personali, nonché l'accesso a qualsiasi sede del Titolare e del processore dei dati, compresi eventuali strumenti e mezzi per il trattamento.

“**Sede principale per quanto riguarda un Titolare**” 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 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;

“**Sede principale con riferimento a un responsabile**” 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.

# **Principi Applicabili al Trattamento dei Dati Personali**

I principi applicabili alla protezione dei dati delineano le responsabilità delle organizzazioni nella gestione dei dati personali. L’articolo 5(2) del GDPR enuncia che “il Titolare è competente per il rispetto dei principi, e in grado di comprovarlo.”

## **Liceità, Correttezza e Trasparenza**

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

## **Limitazione delle Finalità**

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

## **Minimizzazione dei Dati**

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. CRI deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

## **Esattezza**

I dati personali devono essere 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.

## **Limitazione del Periodo di Conservazione**

I dati personali devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

## **Integrità e riservatezza**

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, CRI deve mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali , inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

## **Responsabilizzazione**

I Responsabili dei dati sono competenti per il rispetto dei principi sopra descritti devono essere in grado di comprovarlo.

# **Costruire la protezione dei dati nelle attività commerciali**

Al fine di dimostrare la conformità con i principi della protezione dei dati, un'organizzazione dovrebbe creare protezione dei dati nelle sue attività di servizio.

## **Notifica agli Interessati**

(Vedi la sezione Linee guida sul Corretto Trattamento.)

## **Scelta e Consenso dell’Interessato**

(Vedi la sezione Linee guida sul Corretto Trattamento.)

## **Raccolta**

CRI deve sforzarsi di raccogliere il minor numero di dati personali possibili. Se i dati personali sono raccolti da terzi, il Responsabile del trattamento deve garantire che i dati personali siano raccolti legalmente.

## **Uso, Conservazione e Smaltimento**

Le finalità, i metodi, il limite di registrazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'Informativa sulla Privacy. CRI deve mantenere l'esattezza, 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, utilizzati in modo improprio o abusati e prevenire le violazioni dei dati personali. Il Responsabile del Trattamento dei Dati è responsabile della conformità con i requisiti elencati in questa sezione.

## **Divulgazione a terzi**

Ogni volta che CRI utilizza un fornitore o un partner terzo per il trattamento dei dati personali per suo conto, il Responsabile della Protezione dei Dati deve garantire che questo Responsabile al Trattamento fornisca misure di sicurezza per salvaguardare i dati personali adeguate ai rischi associati.

CRI deve richiedere contrattualmente al fornitore o partner commerciale di fornire lo stesso livello di protezione dei dati. Il fornitore o il partner commerciale deve trattare i dati personali solo per adempiere ai propri obblighi contrattuali nei confronti di CRI o dietro istruzioni di CRI e non per altri scopi. Quando CRI tratta i dati personali congiuntamente con un terzo indipendente, CRI deve specificare esplicitamente le responsabilità proprie e quelle del terzo nel relativo contratto o qualsiasi in altro documento legale vincolante, come esplicitato nelle Nomine degli Incaricati e Nomine di Responsabile esterno .

## **Trasferimento Transfrontaliero dei Dati Personali**

Prima di trasferire i dati personali dallo Spazio Economico Europeo (SEE) devono essere utilizzate misure di protezione adeguate, (come documento: Misure consigliate) compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione Europea e, se necessario, deve essere ottenuta l'autorizzazione della relativa Autorità per la Protezione dei Dati. L'entità che riceve i dati personali deve rispettare i principi del trattamento dei dati personali stabiliti nella Procedura di Trasferimento Transfrontaliero di Dati Personali.

## **Portabilità dei Dati**

Gli interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che ci hanno fornito in un formato strutturato e di trasmettere tali dati a un altro Titolare, gratuitamente. Il Responsabile al Trattamento è responsabile di garantire che tali richieste vengano elaborate entro un mese, non siano eccessive e non incidano sui diritti relativi ai dati personali di altre persone .

## **Diritto all’oblio**

Su richiesta, gli interessati hanno il diritto di ottenere da CRI la cancellazione dei propri dati personali. Quando CRI agisce come Titolare, il Responsabile della Protezione dei Dati deve intraprendere le azioni necessarie (comprese le misure tecniche) per informare i terzi che utilizzano o trattano tali dati per conformarsi alla richiesta.

# **Linee guida sul Corretto Trattamento**

I dati personali devono essere trattati solo se esplicitamente autorizzati dal Responsabile della Protezione dei Dati. CRI decide se eseguire la Valutazione d'Impatto sulla Protezione dei Dati per ciascuna attività di trattamento dei dati.

## **Comunicazioni agli Interessati**

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, inclusa ma non limitata a, la vendita di prodotti, servizi o attività di marketing, il Responsabile della Protezione dei Dati è responsabile di informare adeguatamente gli interessati di quanto segue: ***i tipi di dati personali raccolti, le finalità del trattamento, I metodi di trattamento, i diritti degli interessati riguardo 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 dell’CRI per proteggere i dati personali . Queste informazioni sono fornite tramite un’Informativa sulla Privacy***.

Laddove i dati personali siano condivisi con terzi, , il Responsabile della Protezione dei Dati deve garantire che gli interessati siano stati informati di ciò tramite un’Informativa sulla Privacy.

Laddove i dati personali siano trasferiti in un paese terzo in base alla politica di trasferimento transfrontaliero dei dati, l’Informativa sulla Privacy dovrebbe rispecchiare questo e indicare chiaramente dove e a quale soggetti i dati personali vengono trasferiti.

Nel caso in cui vengano raccolti dati personali sensibili, il Responsabile della Protezione dei Dati deve assicurarsi che l’Informativa sulla Privacy riporti esplicitamente lo scopo per il quale tali dati personali sensibili vengono raccolti.

## **Ottenere i Consensi**

Ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, il Responsabile della Protezione dei Dati è responsabile della conservazione di una registrazione di tale consenso. Il Responsabile della Protezione dei Dati è responsabile di fornire agli interessati le opzioni per dare il consenso e deve informarli e garantire che il loro consenso (ogni volta che il consenso venga utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 16 anni, il Responsabile della Protezione dei Dati deve garantire che il consenso del titolare della responsabilità genitoriale sia fornito prima della raccolta utilizzando il **Modulo di consenso del titolare della responsabilità genitoriale**.

Quando si richiede di correggere, modificare o distruggere le registrazioni dei dati personali, il Responsabile della Protezione dei Dati deve garantire che tali richieste siano gestite entro un ragionevole lasso di tempo. Il Responsabile della Protezione dei Dati deve anche registrare le richieste e tenere un registro di queste.

I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti. Nel caso in cui CRI desideri trattare i dati personali raccolti per un altro scopo, CRI richiede il consenso degli 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 Responsabile della Protezione dei Dati è responsabile del rispetto delle regole in questo paragrafo.

Ora e in futuro, il Responsabile della Protezione dei Dati deve garantire che i metodi di raccolta siano conformi alla legge, alle buone pratiche e alle norme industriali pertinenti.

Il Responsabile della Protezione dei Dati è responsabile della creazione e della manutenzione di un registro delle Informative sulla Privacy.

# **Organizzazione e Responsabilità**

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori per o con CRI e abbia accesso ai dati personali trattati dalla CRI.

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

**Il consiglio di amministrazione o altro organo decisionale** competente prende decisioni e approva le strategie generali della Società in materia di protezione dei dati personali.

**Il Responsabile della Protezione dei Dati o qualsiasi altro dipendente competente** , è responsabile della gestione del programma di protezione dei dati personali ed è responsabile dello sviluppo e della promozione delle politiche di protezione dei dati personali dall’inizio alla fine, come definito nella Descrizione del Ruolo del Responsabile della Protezione dei Dati ;

**Il Dipartimento Affari legali / il Consulente insieme al Responsabile della Protezione dei Dati** , 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.

**Il responsabile del dipartimento di Informatica** è responsabile di:

* Garantire che tutti i sistemi, i servizi e le attrezzature utilizzati per la registrazione dei dati soddisfino standard di sicurezza accettabili.
* Condurre controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.

**Il Responsabile del Marketing** , è responsabile di:

* Approvare qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni quali e-mail e lettere.
* Rispondere a qualsiasi domanda sulla protezione dei dati da parte di giornalisti o media come giornali.
* Se necessario, collaborare con il Responsabile della Protezione dei Sati per garantire che le iniziative di marketing rispettino i principi di protezione dei dati.

**Il Responsabile delle Risorse Umane** è responsabile di:

* Migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti.
* Organizzare la formazione per la competenza e la sensibilizzazione sulla protezione dei dati personali per i dipendenti che lavorano con dati personali.
* Protezione dei dati personali dei dipendenti dall’inizio alla fine. Deve garantire che i dati personali dei dipendenti vengano trattati in base alle legittime finalità e necessità CRIli del datore di lavoro.

**Il Responsabile degli Acquisti** 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 del flusso verso il basso dei dati personali richiesti a qualsiasi fornitore terzo che l’CRI utilizzi. Il reparto Acquisti deve garantire che l’CRI si riservi il diritto di svolgere un audit presso i fornitori.

# **Risposta agli incidenti di Violazione dei Dati Personali**

Quando la CRI viene a conoscenza di una presunta o effettiva violazione dei dati personali, il Responsabile del trattamento dei Dati deve eseguire un'indagine interna e adottare misure correttive appropriate in modo tempestivo, in base alla Politica sulla violazione dei dati. Laddove sussistano rischi per i diritti e le libertà degli interessati, l’CRI deve informare l’autorità di controllo competente in materia di protezione dei dati senza indebiti ritardi e, ove possibile, entro 72 ore.

# **Audit e Responsabilizzazione**

L’Ufficio Legale o altro dipartimento competente è responsabile di verificare in che modo i reparti aziendali implementino questa politica.

Qualsiasi dipendente che violi questa Politica sarà soggetto ad azioni disciplinari e potrebbe anche essere soggetto a responsabilità civili o penali qualora la sua condotta violasse leggi o regolamenti.

# **Conflitti con la Legge**

Questa politica è intesa a rispettare le leggi e i regolamenti del luogo di stabilimento e dei paesi in cui la CRI opera. In caso di conflitto tra questa Politica e le leggi e i regolamenti applicabili, prevarranno questi ultimi.

# **Gestione delle registrazioni sulla base di questo documento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nome del documento | Luogo di archiviazione | Persona responsabile dell’archiviazione | Controlli per la protezione del documento | Tempo di archiviazione |
| **Modulo di Consenso dell’Interessato** | Clicca qui | Il Responsabile della Protezione dei Dati | Soltanto le persone autorizzate possono avere accesso ai moduli | 10 anni |
| **Modulo di Recesso dell’Interessato** | Clicca qui | Il Responsabile della Protezione dei Dati | Soltanto le persone autorizzate possono avere accesso ai moduli | 10 anni |
| **Modulo di Consenso dei Titolari della Responsabilità Genitoriale** | Clicca qui | Il Responsabile della Protezione dei Dati | Soltanto le persone autorizzate possono avere accesso ai moduli | 10 anni |
| **Modulo di Recesso dei Titolari della Responsabilità Genitoriale** | Clicca qui | Il Responsabile della Protezione dei Dati | Soltanto le persone autorizzate possono avere accesso ai moduli | 10 anni |
| **Accordi con il Fornitori del Trattamento dei Dati** | Clicca qui | Il Responsabile della Protezione dei Dati | Soltanto le persone autorizzate possono avere accesso alla cartella | 5 anni dopo la scadenza del contratto |
| **Registro delle Informative sulla Privacy** | Clicca qui | Il Responsabile della Protezione dei Dati | Soltanto le persone autorizzate possono avere accesso alla cartella | Permanente |

# **Validità e gestione del documento**

Questo documento ha effetto dal 25/05/2018.

Il responsabile per questo documento è il Responsabile della Protezione dei Dati il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.

Il Responsabile della Protezione dei Dati  
[nome]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[firma]