PRIMARY SYSTEM RESEARCH SPA

Sede legale in Fabio Filzi, n. 2 – 20124 Milano - Capitale sociale €. 123.000,00.
Codice Fiscale, Partita IVA, Iscrizione al Registro Imprese di Padova n. 02398860227

POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

Revisione:	DOCUMENTO INIZIALE
Data di revisione:	23 MAGGIO 2018
Redatto da:	DIEGO OCCARI
Approvato da:	CONSIGLIO DI AMMINISTRAZIONE

Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica
23.05.2018	0.1	DIEGO OCCARI	DOCUMENTO ORIGINARIO

Sommario

1. Campo d'applicazione, scopo e destinatari

PRIMARY SYSTEM RESEARCH SPA, in seguito denominata "Azienda", si impegna a rispettare le leggi e i regolamenti applicabili relativi alla protezione dei dati personali nei paesi in cui l'Azienda opera. Questa Politica stabilisce i principi di base con cui l'Azienda 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 all'Azienda e alle aziende che controlla direttamente o indirettamente che svolgono attività allinterno 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 dell'Azienda.

2. Documenti di Riferimento

- 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);
- Legislazione nazionale in materia di privacy e provvedimenti del Garante per la protezione dei dati personali;
- Politica di Conservazione dei Dati;
- Descrizione dei Responsabile Dati Personali;
- Procedura per la Richiesta di Accesso ai Dati da parte dell'Interessato;
- Metodologia di Valutazione d'Impatto sulla Protezione dei Dati;
- Procedura di Trasferimento Transfrontaliero di Dati Personali;
- Politiche di Sicurezza IT;
- Procedura di Comunicazione di una Violazione di Dati.

3. 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.

Dati personali sensibili: meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, 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.

Titolare del Trattamento dei Dati: 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 dei Dati: una 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: 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 del Trattamento 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.

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 dei dati nell'Unione ove il Titolare del Trattamento o il Responsabile del Trattamento siano stabiliti in più di uno Stato membro; oppure il 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 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 del Trattamento o un Responsabile del Trattamento 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 del Trattamento e del Responsabile del Trattamento dei dati, compresi eventuali strumenti e mezzi per il trattamento.

"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" 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 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 del Trattamento è competente per il rispetto dei principi, e in grado di comprovarlo*."

4.1. Liceità, Correttezza e Trasparenza

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

4.2. 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.

4.3. Minimizzazione dei Dati

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

4.4. 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.

4.5. 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.

4.6. 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, l'Azienda 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.

4.7. Responsabilizzazione

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

5. 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 commerciali.

5.1. Raccolta

L'Azienda deve sforzarsi di raccogliere il minor numero di dati personali possibili. Se i dati personali sono raccolti da terzi, il Responsabile Dati Personali deve garantire che i dati personali siano raccolti legalmente.

5.2. 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. L'azienda 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 Dati Personali (di seguito anche "DPO") si cura di verificare che tempo per tempo venga rispettata la conformità con i requisiti elencati in questa sezione.

5.3. Divulgazione a terzi

Ogni volta che la Società utilizza un fornitore o un partner commerciale terzo per il trattamento dei dati personali per suo conto, il Responsabile Dati Personali verifica, mediante apposito questionario approvato dal CDA, che tale Responsabile del Trattamento fornisca misure di sicurezza per salvaguardare i dati personali adeguate ai rischi associati.

La Società 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 dell'Azienda o dietro istruzioni dell'Azienda e non per altri scopi. Quando l'Azienda tratta i dati personali congiuntamente con un terzo indipendente, l'Azienda deve specificare esplicitamente le responsabilità proprie e quelle del terzo nel relativo contratto o qualsiasi in altro documento legale vincolante, come l'Accordo con il Fornitore del Trattamento dei Dati.

5.4. Trasferimento Transfrontaliero dei Dati Personali

Prima di trasferire i dati personali dallo Spazio Economico Europeo (SEE) devono essere utilizzate misure di protezione adeguate, 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.

5.5. Diritto d'Accesso da parte degli Interessati

Quando agisce come Responsabile del Trattamento dei dati, Il Responsabile Dati Personali è responsabile di fornire agli interessati un ragionevole meccanismo di accesso per consentire loro di accedere ai propri dati personali e deve consentire loro di aggiornare, rettificare, cancellare o trasmettere i propri dati personali, se del caso o richiesto dalla legge.

5.6. 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 del Trattamento, gratuitamente. Il

Responsabile Dati Personali 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.

5.7. Diritto all'oblio

Su richiesta, gli interessati hanno il diritto di ottenere dall'Azienda la cancellazione dei propri dati personali. Quando l'Azienda agisce come Titolare del Trattamento, il DPO deve intraprendere le azioni necessarie (comprese le misure tecniche) per informare i terzi che utilizzano o trattano tali dati per conformarsi alla richiesta.

6. Linee guida sul Corretto Trattamento

L'Azienda deve decidere se eseguire la Valutazione d'Impatto sulla Protezione dei Dati per ciascuna attività di trattamento dei dati in base alle Linee guida sulla Valutazione d'Impatto sulla Protezione dei Dati.

6.1. 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 personale di volta in volta preposto alla raccolta 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'Azienda per proteggere i dati personali. Queste informazioni sono fornite tramite un'Informativa sulla Privacy.

Laddove i dati personali siano condivisi con terzi, ciò deve essere previsto nelle informative sulla privacy, che devono sempre riportare esplicitamente lo scopo per il quale i dati vengono raccolti.

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.

6.2. Ottenere i Consensi

Ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, deve essere conservata la documentazione comprovante il consenso (informativa sulla privacy firmata in caso di clienti o dipendenti, consenso fornito tramite email o procedure web, in caso di dati raccolti telematicamente ad esempio per attività di Marketing).

E' compito del DPO verificare che, tempo per tempo, la documentazione dei consensi ottenuti da parte dello Studio sia completa e ben conservata. Anche mantenendo traccia di eventuali revoche del consenso.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 18 anni, il soggetto tempo per tempo preposto alla raccolta 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 DPO si occupa che tali richieste siano gestite entro un ragionevole lasso di tempo. IL DPO 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 l'Azienda desideri trattare i dati personali raccolti per un altro scopo, l'Azienda deve richiedere 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 DPO deve garantire che i metodi di raccolta siano conformi alla legge, alle buone pratiche e alle norme industriali pertinenti.

IL DPO è responsabile della creazione e della manutenzione di un registro delle Informative sulla Privacy.

7. Organizzazione e Responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori per o con l'Azienda e abbia accesso ai dati personali trattati dall' Azienda.

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. Ed è il responsabile ultimo del rispetto delle procedure sulla privacy.

Il **Responsabile della Protezione dei Dati (o DPO),** ha la responsabilità di verificare tempo per tempo il corretto rispetto delle politiche e delle procedure adottate dal consiglio di amministrazione in materia di privacy, di aggiornare quando necessario le politiche, di relazionarsi con il responsabile IT per ottenere gli interventi di supporto informatico e di riferire in merito al trattamento dei dati personali sia al Consiglio di amministrazione che al Collegio sindacale;

L'Addetto privacy, è la figura base dell'organigramma della società che, sotto la direzione e la responsabilità del DPO si assicura che (1) le informative sulla privacy vengano consegnate agli interessati; (2) i consensi sulla privacy correttamente raccolti ed archiviati; (3) se vi sono richieste di cancellazione, modifiche o aggiornamento dei dati da parte degli interessati, queste richieste trovino tempestiva esecuzione; (3) che sul sito internet della società siano sempre riportate la presente politica, le informative e la documentazione sulla privacy per l'esercizio dei diritti dell'interessato.

Il Comitato di Controllo sulla Gestione ha la responsabilità di integrare nel proprio piano dei controlli il rispetto da parte della società delle disposizioni in materia di privacy, delle politiche e delle

procedure tempo per tempo adottate, nonché di verificare il corretto assolvimento da parte del DPO della propria funzione.

Il **Responsabile IT (anche Amministratore di Rete)** tempo per tempo individuato, 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.
- Verificare che i sistemi informatici dello Studio rispettino tempo per tempo le politiche e le procedure adottate dal Consiglio di Amministrazione.

Il Presidente del Consiglio di Amministrazione, in qualità di legale rappresentante, 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;
- 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 aziendali del datore di lavoro;
- 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'azienda utilizzi. Il reparto Acquisti deve garantire che l'Azienda si riservi il diritto di svolgere un audit presso i fornitori.

8. Linee guida per Stabilire l'Autorità di Controllo Capofila

8.1. Necessità di Stabilire l'Autorità di Controllo Capofila

PRIMARY SYSTEM RESEARCH SPA esegue trattamento transfrontaliero di dati personali mediante le proprie controllate in Regno Unito a Albania. Compente per la vigilanza sull'Azienda è comunque il Garante per il Trattamento dei Dati Personali in Italia.

8.2. Lo Stabilimento Principale e l'Autorità di Controllo Capofila

8.2.1. Lo Stabilimento Principale per il Titolare del Trattamento dei Dati

Lo stabilimento principale di PRIMARY SYSTEM RESEARCH SPA è in italia e quindi all'interno dell'Unione Europea. L'Azienda detiene una controllata nel Regno Unito che agisce come Responsabile del Trattamento di alcuni dati della Azienda.

L'autorità di controllo capofila in ogni caso è PRIMARY SYSTEM RESEARCH SPA.

8.2.2. Lo Stabilimento Principale in qualità di Responsabile del Trattamento (Responsabile del Trattamento di Dati)

PRIMARY SYSTEM RESEARCH SPA tratta per conto della propria controllata estera di Londra e per conto di terzi, dati personali. I trattamenti dei dati avvengono presso la sede operativa di Via Pierobon, n. 107 Limena, in Italia.

8.2.3. Lo Stabilimento Principale per Aziende al di fuori dell'Unione per Titolari del Trattamento e Responsabili del Trattamento di Dati

PRIMARY SYSTEM RESEARCH SPA assume il ruolo anche di rappresentante nella UE per conto dei terzi che trattano i propri dati in Albania (in particolare Occari & Partners Shpk ed Export Management Platform Shpk).

9. Risposta agli incidenti di Violazione dei Dati Personaliì

Quando l'Azienda viene a conoscenza di una presunta o effettiva violazione dei dati personali, il DPO 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'Azienda deve informare l'autorità di controllo competente in materia di protezione dei dati senza indebiti ritardi e, ove possibile, entro 72 ore.

10. Audit e Responsabilizzazione

Il Comitato di Controllo sulla Gestione 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.

11. Conflitti con la Legge

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

12. 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
Informative sulla privacy	Area riservata sul server della Società.	Il Responsabile della Protezione dei Dati (DPO).	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Consenso dell'Interessato	Area riservata sul server della Società.	Il Responsabile della Protezione dei Dati (DPO).	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Politiche, procedure ed altra documentazione in materia di privacy	Area riservata sul server della Società.	Il Responsabile della Protezione dei Dati (DPO).	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Consenso dell'Interessato	Area riservata sul server della Società.	Il Responsabile della Protezione dei Dati (DPO).	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Recesso dell'Interessato	Area riservata sul server della Società.	Il Responsabile della Protezione dei Dati (DPO).	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Accordi con i Fornitori del Trattamento dei Dati	Area riservata sul server della Società.	Il Responsabile della Protezione dei Dati (DPO).	Soltanto le persone autorizzate possono avere accesso alla cartella	5 anni dopo la scadenza del contratto

Le informative ed i consensi acquisiti dai clienti sono collocati invece all'interno del server della Società, in apposita area riservata.

13. Validità e gestione del documento

Questo documento ha effetto dal 25 maggio 2018.

Il responsabile per questo documento è il DPO, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale, e sottoporlo all'approvazione del CDA che è il responsabile ultimo della conformità dell'Azienda alla normativa sul GDPR.