ACCORDO SULLA PROTEZIONE DEI DATI PERSONALI

1. OGGETTO

Il presente Accordo sulla protezione dei dati definisce le condizioni alle quali Doctolib si impegna a effettuare le operazioni di Trattamento dei Dati personali forniti dall'Abbonato /Utente per la prestazione dei Servizi.

Nell'ambito del rapporto contrattuale esistente, le Parti si impegnano a rispettare le disposizioni di cui alla legislazione vigente in materia di protezione dei dati personali ("Normativa sulla Protezione dei Dati Personali") tra cui il D.Lgs. 196/2003, come vigente, i provvedimenti vincolanti emessi dal Garante per la Protezione dei Dati e il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, applicabile dal 25 maggio 2018 (di seguito il «GDPR»).

2. DEFINIZIONI

Le definizioni allegate al presente Accordo sulla protezione dei dati sono disponibili qui.

3. ENTRATA IN VIGORE E DURATA

Il presente Accordo entra in vigore dalla firma del Contratto cui è allegato e rimarrà efficace per tutta la durata del rapporto contrattuale tra Doctolib e l'Abbonato/Utente.

4. QUALITÀ DELLE PARTI

Le Parti convengono che l'Utente/Abbonato è il Titolare del trattamento e Doctolib è il Responsabile dei Trattamenti dei Dati Personali e dei Dati Sanitari riportati nell'Allegato 1, indipendentemente dal fatto che essi siano forniti direttamente o indirettamente a Doctolib dall'Utente/Abbonato o da un Amministratore al quale l'Utente/Abbonato ha concesso l'accesso ai Servizi.

Doctolib è autorizzata dall'Utente/Abbonato a trattare, per conto del Titolare del trattamento, i Dati Personali e i Dati Sanitari necessari alla prestazione dei Servizi per le finalità, e nel rigoroso rispetto delle condizioni, di seguito menzionate.

Si precisa che l'incarico di Doctolib è limitato all'installazione, alla prestazione dei Servizi e all'hosting della Piattaforma Doctolib, delle Schede Pazienti e del Portale Pazienti. Su espressa richiesta dell'Utente/Abbonato e sotto il suo controllo e responsabilità, Doctolib potrà tuttavia assisterlo nell'importare il Database Paziente sulla Piattaforma Doctolib.

Quando il Titolare del trattamento inserisce Dati Personali o Dati Sanitari di terzi nella Piattaforma Doctolib o nel Portale Pazienti, come i dati dei colleghi, deve osservare i requisiti normativi in relazione al rilascio dell'informativa e/o all'ottenimento del consenso da parte di detti terzi.

4.1. Obblighi dell'Utente/Abbonato

L'Utente e/o l'Abbonato, in qualità di Titolare del trattamento, è l'unico responsabile della tenuta del registro dei trattamenti e, se del caso, dell'esecuzione delle formalità preliminari al trattamento dei Dati Personali e dei Dati Sanitari. Il Titolare del trattamento ha anche il compito di informare i Pazienti in merito all'inserimento dei loro Dati Personali e dei Dati Sanitari sulla Piattaforma Doctolib e delle modalità di esercizio dei loro diritti, fornendo loro un foglio informativo.

In qualità di Titolare del trattamento, l'Utente e/o l'Abbonato è l'unico responsabile dell'esattezza, affidabilità e pertinenza dei Dati Personali e dei Dati Sanitari. In particolare, è responsabile dell'uso della Piattaforma Doctolib e dei Documenti che carica, conserva, consulta e rimuove dallo spazio di archiviazione. È tenuto a effettuare tutti gli adempimenti necessari. L'Utente e/o l'Abbonato si obbliga a risarcire e tenere indenne Doctolib, i suoi rappresentanti, dipendenti e responsabili del trattamento rispetto a qualsiasi reclamo, responsabilità, danno e costo (tra cui le spese e gli onorari legali) posti a carico o subiti da Doctolib, i suoi rappresentanti, dipendenti e responsabili del trattamento derivanti dalla mancata osservanza da parte dell'Utente e/o Abbonato del presente obbligo.

L'Utente e/o l'Abbonato si obbliga a:

- Rispettare e far rispettare la riservatezza del rapporto medico-paziente;

- Attuare una politica di responsabilizzazione, gestione dei diritti di accesso e dei ruoli , garantendo la riservatezza dei Dati Personali e dei Dati Sanitari, in linea con la volontà espressa dai Pazienti e dai loro Familiari;

- Fornire a Doctolib i dati necessari per svolgere la propria attività quale responsabile del trattamento, tra cui l'elenco dei Dati Personali e dei Dati Sanitari oggetto del trattamento, la base giuridica dello stesso, le finalità dei trattamenti, nonché il periodo di conservazione dei Dati Personali e dei Dati Sanitari;

- Documentare per iscritto eventuali istruzioni riguardanti il(i) Trattamento(i) di Dati Personali e Dati Sanitari effettuato(i) da Doctolib;

- Assicurarsi, prima e durante il periodo del Trattamento, che Doctolib rispetti gli obblighi stabiliti dal GDPR;

- Sovrintendere ai trattamenti posti in essere da Doctolib in qualità di Responsabile del trattamento;

- Nominare un interlocutore per rappresentare il Titolare del trattamento e, se necessario, un responsabile della protezione dei Dati personali secondo quanto previsto dal GDPR;

- Nella fase dei test, condividere con Doctolib solo dati fittizi, senza alcun Dato Personale o Dato Sanitario;

- Assicurarsi, prima e durante il periodo del Trattamento, il rispetto degli obblighi stabiliti nel GDPR.

4.2. Obblighi di Doctolib

4.2.1. Doctolib si obbliga a:

- Trattare i Dati Personali e i Dati Sanitari secondo le finalità e il quadro definito nel presente Accordo, e a rispettare le norme tecniche e le good practice applicabili ai Dati Personali e ai Dati Sanitari;

- Agire solo su preventiva istruzione del Titolare del trattamento. In caso di impossibilità o difficoltà nel dare esecuzione a determinate istruzioni, Doctolib informerà tempestivamente il Titolare del trattamento. Doctolib può presentare una richiesta scritta per derogare alle istruzioni e, per poter procedere sulla base di tale deroga, deve ottenere la previa e specifica autorizzazione scritta del Titolare del trattamento.

- Non estrarre copie dei Dati Personali e dei Dati Sanitari in mancanza di autorizzazione o istruzioni del Titolare del trattamento in tal senso, non comunicarli a terzi e non utilizzarli per scopi diversi da quelli specificati nel Contratto;

- Non sfruttare o trattare i Dati Personali e i Dati Sanitari, affidatigli dal Titolare dei trattamenti, per conto proprio e/o per conto di terzi, per qualsiasi finalità e con qualsiasi modalità;

- Avvalersi di tutti i mezzi in suo possesso, nel rispetto delle previsioni contrattuali e secondo lo stato dell'arte, per garantire la sicurezza e la riservatezza dei Dati Personali e dei Dati Sanitari che gli sono affidati e, in particolare, per evitare che siano modificati, danneggiati o comunicati a terzi non autorizzati; più in generale, attuare le misure tecniche e organizzative appropriate per proteggere i Dati Personali e i Dati Sanitari dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla diffusione o dall'accesso non autorizzato, in particolare laddove il Trattamento comporti la trasmissione di dati in rete, nonché da qualsiasi forma di trattamento illecito;

- Comunicare tempestivamente al Titolare del trattamento ogni violazione della sicurezza che riguardi direttamente o indirettamente i Dati Personali, i Dati Sanitari o i Trattamenti che lo riguardano;

- Effettuare backup regolari dei Dati Personali e dei Dati Sanitari;

- Condurre regolarmente test di penetrazione (o Pentest);

- Manutenere quanto necessario per il corretto funzionamento dei Servizi;

- Garantire la riservatezza dei Dati Personali e dei Dati Sanitari oggetto di Trattamento;

- Dare seguito a qualsiasi aggiornamento, rettifica, cancellazione o altre modifiche comunicate dal Titolare del trattamento relativamente ai Dati Personali e ai Dati Sanitari;

- Osservare il periodo di conservazione dei Dati Personali e dei Dati Sanitari applicabile alle finalità per le quali sono stati raccolti o forniti, come da indicazioni del Titolare del trattamento e cancellarli/renderli anonimi non appena tali scopi vengono meno, fermi restando gli obblighi di legge;

- Nominare un Responsabile della Protezione dei Dati Personali.

4.2.2. Doctolib si impegna inoltre a garantire che le persone autorizzate a trattare Dati Personali e Dati Sanitari ai sensi del presente Accordo:

- Si impegnino a rispettare la riservatezza o siano vincolati da un adeguato impegno di riservatezza;

- Ricevano la formazione necessaria in materia di protezione dei Dati Personali e dei Dati Sanitari;

- con riguardo a strumentazione, prodotti, applicazioni o servizi, tenere in considerazione i principi di privacy by design e by default.

4.2.3. Cooperazione sulla conformità:

Doctolib pone in essere tutti i mezzi necessari per assistere il Titolare del trattamento nella realizzazione delle valutazioni d'impatto relative alla protezione dei Dati Personali e dei Dati Sanitari e nella consultazione preventiva dell'autorità di controllo.

Doctolib mette a disposizione del Titolare del trattamento tutte le informazioni necessarie in relazione al Trattamento dei Dati Personali e dei Dati Sanitari al fine di assisterlo nell'adempimento dei suoi obblighi legali e regolamentari come Titolare del trattamento in conformità alle disposizioni del GDPR (Allegato 3.1).

In assenza di diverse e ulteriori istruzioni specifiche del Titolare del trattamento in relazione alla natura dei Dati Personali e dei Dati Sanitari da trattare, alle finalità, alla base giuridica e al periodo di conservazione, il Titolare del trattamento riconosce dichiara ed accetta che i Dati Personali e i Dati Sanitari saranno trattati secondo le modalità di cui agli Allegati 1 e 2. In qualità di Titolare del trattamento, l'Utente/Abbonato può chiedere a Doctolib di modificare tali modalità nell'adempiere il Contratto.

5. VIOLAZIONE DEI DATI PERSONALI

Qualora Doctolib venga a conoscenza di una Violazione dei Dati Personali e/o dei Dati Sanitari, Doctolib comunica tempestivamente al Titolare del trattamento detta violazione, tramite e-mail o qualsiasi altro mezzo di comunicazione messo a sua disposizione dal Titolare del trattamento.

Su richiesta del Titolare del trattamento, tale notifica è accompagnata da ogni documento utile finalizzato a consentirgli, ove necessario, di comunicare tale violazione alla competente autorità di controllo e, se del caso, agli interessati.

6. TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Doctolib dichiara di tenere un registro scritto di tutti i trattamenti effettuati per conto del Titolare del trattamento in conformità con le disposizioni del GDPR.

7. INFORMAZIONE E DIRITTI DEGLI INTERESSATI

Il Titolare del trattamento è tenuto a informare l'Interessato o gli Interessati circa (i) i Trattamenti effettuati nell'ambito dei Servizi e ottenere il loro consenso o i loro consensi ogni volta che ciò sia necessario in conformità alla normativa applicabile; (ii) le basi giuridiche dei Trattamenti effettuati, le finalità dei Trattamenti e l'elenco dei responsabili che possono trattare i loro dati personali.

Al fine di assistere il Titolare del trattamento rispetto a tali informazioni, Doctolib pubblica sul suo sito una Informativa sulla Privacy accessibile presso https://www.doctolib.itxxxx.

8. GESTIONE DEI DIRITTI

Il Titolare del trattamento è tenuto a dare seguito alle richieste degli Interessati in merito ai loro Dati Personali.

Per quanto possibile, Doctolib, in qualità di Responsabile del trattamento, e su richiesta del Titolare del trattamento potrà assisterlo nell'adempimento dell'obbligo di soddisfare le richieste di esercizio dei diritti degli Interessati: diritto di accesso, rettifica, cancellazione e opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere sottoposto a una decisione individuale automatizzata (compresa la profilazione), diritto di decidere dei propri Dati Personali, in particolare dopo il suo decesso, ecc.

Se un Interessato si rivolge direttamente a Doctolib per esercitare uno dei diritti che vanta sui suoi Dati personali trattati da Doctolib in qualità di Responsabile del trattamento, Doctolib si impegna a indirizzare l'Interessato verso il Titolare del trattamento, affinché questi possa dare seguito alla sua richiesta.
Su richiesta del Titolare del trattamento, Doctolib potrà assisterlo nel dare seguito alle richieste di esercizio di un diritto, ma non rispondere direttamente alle richieste di tali Interessati.

9. SICUREZZA E RISERVATEZZA

9.1 Per quanto riguarda i Servizi, Doctolib attua le misure tecniche e organizzative adeguate con riferimento alla sicurezza, in conformità alle disposizioni previste dalla Normativa sulla Protezione dei Dati Personali e dal GDPR, e dirette a garantire un livello di sicurezza adeguato rispetto ai rischi presentati dal Trattamento dei Dati personali dell'Utente/Abbonato, secondo quanto indicato *sub* Allegato 2 (Misure tecniche e organizzative). Per valutare il livello adeguato di sicurezza, Doctolib terrà conto dei rischi che possono derivare dalla distruzione accidentale o illecita, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso ai Dati Personali e Dati Sanitari che possono essere trasmessi, conservati o altrimenti trattati, conformemente alle disposizioni dell'articolo 32 del GDPR.

Gli obblighi di cui sopra non liberano in alcun modo l'Utente/Abbonato dall'obbligo di mettere in atto tutti i mezzi di sicurezza necessari a garantire la riservatezza dei Documenti e dei Dati Abbonati, del Database Paziente, dei Dati Utenti, dei Dati Personali e dei Dati Sanitari presenti sulla Piattaforma Doctolib.

Le parti convengono che, in caso di controllo, il Contratto di cui è parte il presente Accordo sulla protezione dei dati può essere messo a disposizione di qualsiasi autorità competente.

9.2 Segreto Professionale: Doctolib riconosce e accetta che i Dati Personali e i Dati Sanitari trattati dal Titolare del trattamento nel godimento dei Servizi sono rigorosamente coperti dal segreto professionale (articolo 622 del codice penale).

9.3 Tenuta dei dati: Salvo diverso espresso accordo sulla protezione dei dati, il Titolare del trattamento resta l'unico titolare dei Dati Abbonato/Utente pubblicati sul Portale Pazienti, così come sulla Scheda Profilo Utente e sulla Piattaforma Doctolib. Doctolib non potrà rivendicare alcun diritto sui dati pubblicati dal Titolare del trattamento. Le statistiche di utilizzo del Portale Pazienti, rese anonime, sono di proprietà di Doctolib.

10. PERSONALE DOCTOLIB

Doctolib individua team qualificati con le necessarie competenze tecniche e/o funzionali per la prestazione dei Servizi. Le persone autorizzate a trattare i Dati Personali e/o i Dati Sanitari per conto del Titolare del trattamento hanno ricevuto formazione in relazione alla normativa relativa alla protezione dei dati personali.

11. ULTERIORI RESPONSABILI DEL TRATTAMENTO

L'Utente/Abbonato concede in questa sede a Doctolib l'autorizzazione generale ad avvalersi di Responsabili ulteriori del trattamento qui elencati, laddove ciò sia ragionevolmente necessario per fornire i Servizi. Conformemente a tale autorizzazione generale, Doctolib si impegna a informare ciascun Utente/Abbonato, con un preavviso scritto di trenta (30) giorni, di ogni cambiamento previsto che comporti l'aggiunta o la sostituzione di Responsabili ulteriori del trattamento, offrendo così all'Utente/Abbonato la possibilità di sollevare eventuali obiezioni che lo stesso dovesse avere in merito a tali cambiamenti. Se l'Utente/Abbonato dovesse avere motivi legittimi e ragionevoli per opporsi alla nomina di un nuovo Responsabile ulteriore del trattamento, l'Utente dovrà tempestivamente motivare ciò a Doctolib inviandogli notifica scritta al seguente indirizzo: contact.dataprivacy@doctolib.com, entro trenta (30) giorni lavorativi successivi alla comunicazione di Doctolib, in difetto della quale si presumerà che l'Utente/Abbonato abbia approvato e accettato tale nomina.

Dopo eventuali discussioni, in mancanza di accordo tra Doctolib e l'Utente/Abbonato, quest'ultimo potrà, nei trenta (30) giorni successivi alla notifica, recedere dalla parte del Contratto interessata dall'aggiornamento in questione.

Con riguardo agli eventuali Responsabili ulteriori del trattamento, Doctolib: (i) eserciterà la dovuta diligenza commerciale nel valutare, nominare e monitorare le attività di Trattamento dei Responsabili ulteriori del trattamento ; (ii) inserirà nel contratto tra Doctolib e ciascun Responsabile ulteriore del trattamento clausole che offrano, con riguardo ai Dati Personali e Dati Sanitari degli Abbonati/Utenti, un livello di protezione equivalente a quanto previsto nel presente Accordo.

Gli hosting di Servizi sono certificati HDS (Hosting Dati Sanitari) secondo quanto previsto dalla normativa francese (decreto dell'11 giugno 2018).

I nominativi dei relativi provider sono disponibili previa richiesta da inviare apro@doctolib.it.

La certificazione di cui beneficiano questi hosting è una certificazione HDS (Hosting Approvato dei Dati Sanitari) convalidata dal Ministero della Salute francese (e dalla sua agenzia incaricata dei sistemi informativi, l'Agence du Numérique en Santé – «Agenzia del Digitale per la Salute») e dalla Commission Nationale de l'Informatique et des Libertés («Commissione Nazionale dell'Informatica e delle Libertà») (CNIL).

12. AUDIT

12.1 Al fine di valutare la sicurezza dei Servizi, il Titolare del trattamento potrà far effettuare audit di sicurezza a proprie spese, nel rispetto delle condizioni previste dal presente articolo e nel limite di un (1) audit all'anno e per un massimo di cinque (5) giorni lavorativi; il tempo impiegato dal personale Doctolib sarà fatturato al Titolare del trattamento.

12.2 L'audit sarà limitato alla verifica dei processi, dell'organizzazione e degli strumenti direttamente ed esclusivamente legati all'attuazione delle disposizioni del GDPR per i Servizi interessati.

L'audit non avrà in nessun caso lo scopo di controllare o richiedere l'accesso a (i) qualsiasi Dato Personale o Dato Sanitario che non sia specifico, sia esso riservato o meno, o qualsiasi informazione la cui comunicazione potrebbe, a giudizio di Doctolib, danneggiare la sicurezza dei Servizi o di suo Utente; (ii) i dati finanziari di Doctolib; o (iii) i Dati Personali relativi ai dipendenti di Doctolib o dei suoi Responsabili.

Le Parti convengono che tutte le attività intraprese come parte di un audit non devono, né congiuntamente né in altro modo: (i) ostacolare, modificare o interessare in qualsiasi modo il funzionamento di Servizi, sistemi, reti, software e/o hardware diversi da quelli destinati all'uso esclusivo dell'Utente/Abbonato; (ii) danneggiare l'infrastruttura che ospita i Servizi (iii) danneggiare, cancellare, modificare qualsiasi tipo di dato; (iv) consentire l'accesso non autorizzato o il mantenimento dei dati summenzionati.

Non è consentito alcun test di intrusione o penetrazione della rete Doctolib per nessuna ragione, ed è esclusa tale attività nel corso degli audit.

Doctolib metterà a disposizione dei revisori tutti i documenti e le informazioni necessarie per lo svolgimento dell'audit esclusivamente nei suoi locali, senza alcuna possibilità di rimozione o copia per qualsiasi finalità. Tale divieto si applica anche ai documenti e alle informazioni messe a disposizione dai Responsabili di Doctolib.

12.3 Almeno trenta (30) giorni prima dell'audit, il Titolare del trattamento è tenuto a inviare a Doctolib un accordo di audit che specifichi l'esatta portata dei test, le date e gli orari dei test previsti e le loro condizioni. Il revisore deve anche specificare eventuali account e profili utilizzati per i test (indirizzo IP di origine, user agent, ecc.), la metodologia utilizzata e i soggetti da controllare.

Il Titolare del trattamento è tenuto a comunicare a Doctolib tutte le informazioni utili relative al test di penetrazione e in particolare (i) i dati di contatto del revisore e delle persone incaricate dell'audit; (ii) gli indirizzi IP utilizzati per condurre i test di penetrazione; e (iii) gli strumenti utilizzati per i test.

Doctolib deve preventivamente accettare il contenuto dell'accordo di audit prima che possa iniziare la relativa attività.

12.4 Le informazioni ottenute durante l'audit sono Informazioni Riservate e saranno trattate come tali dal Titolare del trattamento. Queste informazioni potranno essere comunicate solo a persone soggette a rigorosi obblighi di riservatezza e che hanno un interesse diretto e rilevante nel conoscerle e non devono essere divulgate in alcun modo al pubblico o internamente.

Se il Titolare del trattamento desidera avvalersi di un revisore esterno, questi deve ottenere il previo consenso scritto di Doctolib, fermo restando che Doctolib può rifiutare il suddetto revisore solo adducendo argomenti oggettivi e fondati.

Il revisore esterno non può in alcun modo essere un concorrente di Doctolib e deve impegnarsi per iscritto a rispettare le condizioni stabilite nel presente articolo.

Il Titolare del trattamento si impegna a comunicare il rapporto di audit gratuitamente a Doctolib, che potrà presentare le proprie osservazioni.

Doctolib avrà un periodo di tempo ragionevole dal ricevimento del rapporto per rimediare i vizi e/o le non conformità riscontrate.

13. RECUPERO DEI DATI

L'Abbonato e l'Utente potranno recuperare il Database paziente, così come la cronologia dei loro appuntamenti al termine del Contratto. Questi dati saranno messi a disposizione dell'Utente/Abbonato in un formato che garantisce la loro interoperabilità. La richiesta di portabilità deve essere fatta via e-mail al seguente indirizzo: pro@doctolib.com.

Doctolib si impegna, per tutta la durata del Contratto e per tutto il processo di recupero dei dati, a tenerne una copia a disposizione dell'Utente/Abbonato. Nel caso in cui l'accesso dell'Utente/Abbonato ai Servizi Doctolib venga sospeso per qualsiasi motivo, Doctolib consentirà all'Utente/Abbonato di recuperare, con qualsiasi mezzo e su qualsiasi supporto, l'ultima copia del proprio Database Paziente, nonché la sua cronologia degli appuntamenti.

14. TRASFERIMENTO DI DATI PERSONALI

I Dati personali potranno essere oggetto di trasferimento, per le finalità elencate nell'Accordo sulla protezione dei dati personali, a società del Gruppo Doctolib, a loro subappaltatori o fornitori di servizi stabiliti in Paesi con un adeguato livello di protezione o che offrono adeguate garanzie in materia di protezione della privacy e dei diritti e delle libertà fondamentali delle persone, in conformità con la legislazione applicabile.

Doctolib informa l'Utente/Abbonato del fatto che i Dati Personali possono altresì essere trasferiti da Doctolib verso paesi terzi a Responsabili ulteriori del trattamento, esclusivamente nel caso in cui un tale trasferimento sia necessario per prestare i Servizi richiesti. L'elenco dei Responsabili ulteriori del trattamento è qui disponibile qui.

Se il trasferimento avviene verso un Paese terzo la cui legislazione non è stata riconosciuta come in grado di offrire un adeguato livello di protezione dei Dati Personali, Doctolib garantisce che siano messe in atto misure adeguate in conformità con la Normativa sulla Protezione dei Dati Personali e il GDPR, e in

particolare, se necessario, che le clausole contrattuali tipo o clausole equivalenti *ad hoc* siano incluse nel contratto concluso tra Doctolib e il Responsabile ulteriore del trattamento.

In qualità di Responsabile del trattamento, Doctolib si impegna ad conservare e far conservare i Dati Personali sul territorio dell'Unione Europea e, se del caso, a trasferire tutti gli obblighi previsti dal presente Accordo al fornitore di servizi che conserva i Dati Personali.

15. CONTATTI

In caso di domande relative al Trattamento dei Dati Personali e dei Dati Sanitari effettuato da Doctolib circa le clausole contrattuali, l'Utente/l'Abbonato può contattare il DPO di Doctolib all'indirizzo di seguito indicato.

Doctolib SAS è il rappresentante di Doctolib per la protezione dei Dati personali nello SEE. L'autorità di controllo capofila è il CNIL (https://www.cnil.fr). Il Responsabile della protezione dei dati di Doctolib SAS può essere contattato al seguente indirizzo: DOCTOLIB – DPO, sede legale in Milano, Corso Giacomo Matteotti n 1, C.F./P.IVA 11537360965, oppure all'indirizzo contact.dataprivacy@doctolib.com.

16. LEGGE APPLICABILE

L'Accordo è disciplinato e interpretato in conformità con la legge nazionale applicabile al Titolare del trattamento.

17. INTERO ACCORDO

Il presente Accordo costituisce l'intero accordo tra le Parti relativamente al suo oggetto e sostituisce tutti gli accordi precedenti o contemporanei conclusi tra le Parti aventi lo stesso oggetto, tra cui ogni versione precedente di un accordo sulla protezione dei dati personali che sia stato firmato tra Utente/Abbonato e Doctolib.

ALLEGATO 1: DETTAGLI RELATIVI AL TRATTAMENTO DEI DATI PERSONALI

Il presente Allegato 1 contiene alcuni dettagli relativi al Trattamento dei Dati Personali e dei Dati Sanitari, in conformità all'articolo 28(3) del GDPR.

TITOLARE DEL TRATTAMENTO: l'Abbonato sottoscrittore di un Abbonamento Doctolib e/o l'Utente avente un account Utente Doctolib.

Le attività del Titolare del trattamento comprendono Trattamenti che consentono l'esercizio di attività funzionale alla prenotazione delle prestazioni finalizzate alla prevenzione, diagnosi e cura così come alla gestione amministrativa del proprio istituto di cura, struttura sanitaria o studio privato.

I Trattamenti consentono in particolare, ai fini della cura dei pazienti (i) la gestione degli appuntamenti; (ii) la gestione delle cartelle cliniche necessarie al follow-up del paziente; (iii) le comunicazioni tra i professionisti identificati e le strutture di cura coinvolte nella cura dell'interessato e nel coordinamento della stessa; (iv) la redazione e la trasmissione telematica dei documenti intesi alla presa in carico delle spese sanitarie da parte dell'eventuale assicurazione medica (es. prescrizioni, documenti per la sospensione dal lavoro, ecc.); (v) la tenuta della contabilità.

I Trattamenti effettuati devono rispondere a un obiettivo preciso ed essere giustificati alla luce delle missioni e delle attività degli Operatori Sanitari Aderenti.

RESPONSABILE(I) DEL TRATTAMENTO: Doctolib S.r.l.

Le attività effettuate dal Responsabile del trattamento per conto dei Titolari del trattamento sono di seguito descritte.

TRATTAMENTO N°1: GESTIONE DEGLI ACCOUNT ABBONATI E UTENTI

TRATTAMENTI:

I Servizi Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, il recupero, la consultazione e l'utilizzo, la comunicazione per la trasmissione, l'anonimizzazione e la cancellazione dei Dati Personali di seguito elencati.

FINALITÀ DEL TRATTAMENTO:

- Gestione degli account: fornire Account Utenti agli Utenti (creazione e gestione di tali Account), gestire l'identificazione degli Utenti e rendere sicuro l'accesso agli Account Utenti, parametrare l'Account Utente e le credenziali degli Utenti;
- Supporto tecnico e assistenza: fornire supporto tecnico, manutenzione ed elaborazione delle richieste degli Utenti, consulenza, archiviazione, hosting e altri servizi forniti agli Utenti;
- Supporto Dati Personali: assistenza nella gestione delle Violazioni di Dati Personali e Dati Sanitari, assistenza nella conduzione della DPIA, supporto nella risposta alle richieste di esercizio dei diritti degli Interessati;
- Reporting, debug e statistiche;

BASE GIURIDICA DEL TRATTAMENTO:

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi trattamento.

INTERESSATI:

Abbonato e Utente, secondo la definizione contenuta nel Contratto.

TIPOLOGIE DI DATI PERSONALI:

Nell'intento di ridurre al minimo il numero di Dati Personali trattati, il Titolare del trattamento deve assicurarsi di raccogliere e utilizzare solo i dati pertinenti e necessari avuto riguardo alle proprie esigenze in termini di gestione amministrativa dei suoi pazienti.

In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate:

a) **L'identità e i dati di contatto dell'Operatore Sanitario Aderente**: sesso, nome, cognome, numero di telefono e indirizzo e-mail, indirizzo postale, fotografia, firma, documento d'identità, il titolo di laurea, il titolo di specializzazione e l'abilitazione professionale, il certificato di iscrizione all'Ordine di appartenenza (inclusa la data di iscrizione e il numero di iscrizione al relativo Albo).
b) **Dati professionali:** fotografia, specializzazione, dettagli della presa in carico, percorso professionale dell'Operatore Sanitario Aderente, tipi di prestazione/consulto disponibili, orari di apertura e chiusura, particolarità legate al luogo in cui avviene il consulto.
c) I **registri di utilizzo e di connessione** che riportano le «azioni commerciali» degli Utenti all'interno della Piattaforma Doctolib e i **registri tecnici** che riportano l'«attività» dei componenti software e hardware utilizzati dall'Utente/Abbonato, affinché Doctolib possa garantire il funzionamento e l'accesso alle funzionalità richieste.

Fatte salve istruzioni specifiche del Titolare del trattamento, Doctolib tratta tutti i suddetti Dati Personali al fine di fornire il Servizio, oggetto del Contratto.

DESTINATARI E RESPONSABILI ULTERIORI DEL TRATTAMENTO:

Si prega di fare riferimento all'elenco di cui all'articolo 14 del presente Accordo.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
In assenza di tale istruzione da parte del Titolare del trattamento, Doctolib applicherà i periodi di conservazione eventualmente raccomandati dal Garante per la protezione dei dati personali o previsti dalla Normativa in materia di Protezione dei Dati Personali.

TRATTAMENTO N°2: LA GESTIONE DEGLI APPUNTAMENTI & DELL'AGENDA

TRATTAMENTI:

I Servizi Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, il recupero, la consultazione e l'utilizzo, la comunicazione per la trasmissione, l'anonimizzazione e la cancellazione dei Dati Personali di seguito elencati.

FINALITÀ DEL TRATTAMENTO:

- Supporto nella gestione del caricamento e dell'estrazione del contenuto delle agende, degli appuntamenti e, quando necessario del Database Paziente degli Operatori Sanitari Aderenti sulla Piattaforma Doctolib;
- Osservare le norme relative alla sicurezza dell'identificazione;
- Consentire al Titolare del trattamento di gestire la sua agenda;
- Consentire al Titolare del trattamento di gestire il percorso di cura per i Pazienti e loro Familiari;
- Consentire al Titolare del trattamento di gestire la sua agenda, gestire la cura dei Pazienti all'interno del proprio istituto di cura o studio ;
- Consentire la prenotazione di appuntamenti online dei Pazienti, fatta per sé stessi e per i loro Familiari;
- Permettere la gestione degli appuntamenti;
- Consentire la comunicazione tra l'Operatore Sanitario Aderente e il Paziente e fornire ai Pazienti e ai loro Familiari le informazioni relative al Profilo Utente e al loro percorso di cura;
- Permettere al Titolare del trattamento di inviare e ricevere Documenti ai Pazienti e ai loro Familiari;
- Inviare SMS e e-mail (i) di conferma, annullamento o promemoria dell'appuntamento; (ii) informative sull'invio di Documenti; (iii) informative di promemoria (iv) informative legate alla cura del Paziente o all'organizzazione della sua attività;
- Consentire la gestione dei trasferimenti di contenuti delle agende e appuntamenti degli Operatori Sanitari Aderenti della Piattaforma Doctolib;
- Consentire di istituire un collegamento tra i Dati Personali e Sanitari dei Pazienti e il numero della Tessera sanitaria per la fruizione dei servizi prestati dal Sistema Sanitario Nazionale veicolata dal Titolare del trattamento o dal gestore del servizio scelto dal Titolare del trattamento e inviato a Doctolib.

BASE GIURIDICA DEL TRATTAMENTO:

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi Trattamento.

INTERESSATI:

I Pazienti e loro Familiari, colleghi degli Operatori Sanitari Aderenti.

TIPOLOGIE DI DATI PERSONALI:

Nell'intento di ridurre al minimo il numero di Dati Personali e Dati Sanitari trattati, il Titolare del trattamento deve assicurarsi di raccogliere e utilizzare solo i Dati personali e i Dati sanitari pertinenti e necessari avuto riguardo alle proprie esigenze in termini di gestione amministrativa dei suoi pazienti.

In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate:
a) **L'identità e i Dati di Contatto del Paziente o del Familiare:** sesso, nome, cognome, data di nascita, luogo di nascita, indirizzo postale, indirizzo e-mail e numero di telefono.
b) **la professione del Paziente o del Familiare**: professione.
c) **Salute**: eventuale stato assicurativo, identità e i dati di contatto del medico curante, l'identità e i dati di contatto del medico di riferimento, la data/ora e il luogo dell'appuntamento, la specializzazione del medico e la natura della consulto, lo stato dell'appuntamento, i documenti medici del Paziente, le note compilate dall'Operatore Sanitario Aderente, il numero della Tessera Sanitaria del paziente e le ulteriori informazioni disponibili dalla stessa (sesso, codice fiscale, cognome, nome, data di nascita, luogo di nascita);
d) I **registri di utilizzo e di connessione** che riportano le «azioni commerciali» degli Utenti all'interno della Piattaforma Doctolib e i **registri tecnici** che riportano l'«attività» dei componenti software e hardware utilizzati dall'Utente, affinché Doctolib possa garantire il funzionamento e l'accesso alle funzionalità richieste.

Fatte salve istruzioni specifiche del Titolare del trattamento, Doctolib tratta tutti i suddetti Dati Personali e Dati Sanitari al fine di fornire il Servizio, oggetto del Contratto.

DESTINATARI E RESPONSABILI ULTERIORI DEL TRATTAMENTO:

- Gli Operatori Sanitari Aderenti;
- Le persone incaricate della segreteria, nel rispetto delle disposizioni sul segreto professionale;
- Le persone autorizzate all'interno di Doctolib
- I Responsabili ulteriori del trattamento: si prega di fare riferimento all'elenco di cui all'articolo 14 del presente Accordo.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
Doctolib applicherà i periodi di conservazione eventualmente raccomandati dal Garante per la protezione dei dati personali o previsti dalla Normativa in materia di Protezione dei Dati Personali

TRATTAMENTO N°3: CARICAMENTO DEL DATABASE PAZIENTE

FINALITÀ:

1/ Consentire l'estrazione del Database Paziente identificato dall'Abbonato/ Utente, Titolare del trattamento;

2/ Permettere di strutturare il Database Paziente e di caricarlo nel servizio del software medico dell'Abbonato/Utente sulla piattaforma Doctolib;

3/ Permettere l'hosting e il backup del Database Paziente sulla piattaforma;

4/ Supporto e assistenza tecnica: assicurare il supporto tecnico, la manutenzione e l'elaborazione delle richieste di Utenti e altri servizi forniti agli Abbonati/Utenti.

BASE GIURIDICA DEL TRATTAMENTO

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi trattamento.

INTERESSATI:
I Pazienti e loro Familiari, gli Abbonati/Utenti, loro colleghi.

Spetta al Titolare del trattamento determinare l'elenco esatto delle persone suscettibili di essere interessate dal Trattamento.

TIPOLOGIE DI DATI INTERESSATI:

Si ricorda che spetta ai Titolari del trattamento fornire nel Servizio Software Medico messo a disposizione da Doctolib solo i Dati Sanitari e i Dati Personali necessari al monitoraggio del Paziente e dei suoi Familiari.
Si deve escludere qualsiasi integrazione di informazioni che non siano legate allo scopo della consultazione del Paziente e dei suoi Familiari o che non siano essenziali per la diagnosi e la prestazione delle cure.
Prima di qualsiasi integrazione di Dati Sanitari o Dati Personali relativi al Paziente e/o ai suoi Familiari, spetta agli Abbonati/Utenti ottenere il consenso preventivo del Paziente e dei suoi Familiari.

In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate: i dati identificativi e di contatto: il cognome, il nome, la data di nascita, l'indirizzo, il numero di telefono.

DESTINATARI E RESPONSABILI SUCCESSIVI DEL TRATTAMENTO DEI DATI:

Nell'ambito di queste azioni e al solo scopo di aiutare l'Abbonato ad utilizzare i suoi Servizi, Doctolib può essere obbligato ad avere accesso ai Database pazienti su base temporanea.

PERIODI DI CONSERVAZIONE:

I Dati Personali raccolti saranno conservati per tutta la durata del rapporto contrattuale che vincola il Titolare del trattamento e Doctolib.

ALLEGATO 2: MISURE TECNICHE E ORGANIZZATIVE

SICUREZZA DEL PRODOTTO

- **Verifica in due tappe (2FA)**: ogni volta che l'Utente si connette a nuove apparecchiature, deve fornire la sua password e un codice ottenuto via e-mail, SMS o uno smartphone (*authenticator*) utilizzabile una sola volta.

- **Politica delle password:**
  composta da 8 caratteri tra numeri, simboli, lettere e lettere maiuscole,
  le password più comuni sono vietate (ad esempio, login, nome, semplici sequenze di numeri).

- **Protezione della sessione Utente:**
  Le sessioni aperte possono essere invalidate.
  La sessione sbloccata con password scade automaticamente dopo 7 giorni.
  Sblocco semplificato tramite codice PIN.
  I codici PIN troppo semplici non sono ammessi.
  La sessione sbloccata dal codice PIN scade automaticamente ogni notte.

- **Processo di recupero sicuro**: verifica delle informazioni dell'account prima di consentire il recupero.

- **Controllo granulare degli accessi**: gli Amministratori possono conferire ad ogni Utente diritti specifici all'interno della loro organizzazione.

- **Tracciabilità delle azioni**: Le azioni dei diversi Utenti di un'organizzazione sono registrate e messe a verbale. Le azioni "sensibili" (modifica dell'accesso alle agende, creazione di account di amministratore) sono soggette a notifiche di sicurezza.

- **Protezione contro il furto dell'account**: i tentativi di connettersi illegittimamente a un account vengono rilevati e bloccati.

SICUREZZA DELLA PIATTAFORMA

- **Aggiornamenti di sicurezza automatici**: le patch di sicurezza sono qualificate e applicate automaticamente ai nostri componenti.

- **Sistemi operativi aggiornati e migliorati**.

- **Vigilanza e sicurezza:** monitoriamo continuamente le minacce note ed emergenti, le vulnerabilità e i vettori di attacco.
- Firewall e sistemi di filtraggio degli accessi dedicati (proxy, vpn...).
- Protezione contro gli attacchi DDoS (*distributed denial of service*).
- Protezione contro gli attacchi software (WAF).

- **Tracciabilità:** registriamo ogni azione, monitoriamo e allertiamo per qualsiasi evento di sicurezza.

- **Centri dati protetti**: HDS, ISO 27001, Tier 3, forte sicurezza fisica, personale sul posto 24/7.

DISPONIBILITÀ

- Tutti i dati sono replicati in più centri dati.
- Ogni centro dati ha diversi collegamenti di rete con l'esterno.
- Tutti i servizi e i componenti sono coperti da procedure di *disaster recovery*, per lo più automatiche.
- Qualsiasi guasto viene automaticamente rilevato e allertato da un sistema di monitoraggio completo per ogni componente tecnico e servizio aziendale.
- Attuazione di una politica di backup e recupero dei dati.

CIFRATURA DEI DATI

Cifratura delle comunicazioni:

- Tutti i dati scambiati con e tra i sistemi sono cifrati utilizzando i protocolli TLS. Questo protocollo è configurato per offrire il miglior compromesso tra compatibilità e sicurezza.
- Gli accessi tecnici si realizzano attraverso una connessione fortemente cifrata e autenticata, con una convalida sistematica tra pari.

Memorizzazione dei dati:

- Tutti i nostri database sono cifrati a riposo.
- Le chiavi di cifratura sono cifrate con una chiave principale creata da un leader francese nella protezione dei segreti crittografici.
- I Dati Particolari sono soggetti a un ulteriore livello di cifratura da parte del server Doctolib. Anche le chiavi di cifratura sono cifrate dalla chiave principale protetta.
- I Dati Particolari sono cifrati end-to-end dall'applicazione Doctolib con chiavi memorizzate solo su hardware Utenti. Questi dati possono essere visibili solo all'Utente. Doctolib è ancora responsabile dell'archiviazione e della disponibilità dei dati, ma non può leggere le informazioni sanitarie. Nessun operatore e intermediario del sistema informatico può leggere questi dati.

CONTROLLO DELL'ACCESSO DEI DIPENDENTI

Si applica la politica del "minimo accesso" per cui a ciascun lavoratore sono concessi solo gli accessi necessari corrispondenti alla mansione lavorativa prestata.

L'Utente stesso può concedere a un membro del team di supporto, se necessario e in caso di indagine investigativa, solo l'accesso temporaneo ai dati.

Solo alcuni membri accreditati e sensibilizzati del team dell'infrastruttura Doctolib possono accedere ai dati in caso di guasti legati alla memorizzazione dei dati.

LE MIGLIORI PRATICHE DI SICUREZZA DELLE APPLICAZIONI

Memorizzazione delle password: hashed (*tritata*) grazie alla robusta funzione di *hashing* (*bcrypt*).

Limite di velocità: i Servizi e gli Utenti sono protetti contro gli attacchi di depauperamento delle risorse (*Denial of Service*), gli attacchi di "forza bruta" e il recupero automatico dei nostri dati, attraverso un algoritmo intelligente che controlla la condivisione e l'accesso ai Servizi e blocca le richieste automatiche.

CICLO DI VITA DELLO SVILUPPO DEL SOFTWARE SICURO (S-SDLC)

Sensibilizzazione, formazione in materia di sicurezza: gli sviluppatori sono formati e resi edotti in merito alle migliori pratiche in termini di sviluppo sicuro delle applicazioni.
Sicurezza a partire dalla progettazione: Ogni nuova caratteristica del prodotto Doctolib è progettata in collaborazione con esperti di sicurezza.
Revisione del codice sorgente:
La sicurezza del codice sorgente di Doctolib viene analizzata automaticamente a ogni modifica.
Le revisioni manuali del codice sorgente vengono eseguite quando viene modificato un componente sensibile.

Esame delle vulnerabilità:
Test di penetrazione:
Doctolib incarica regolarmente note aziende di eseguire test di penetrazione sulle nostre applicazioni e piattaforme.

Programma di ricompense per la segnalazione di vulnerabilità (*bug bounty*):
Dipendenti e ricercatori esterni vengono premiati quando identificano una falla di sicurezza nel prodotto Doctolib.

ACCESSO FISICO DA PARTE DEI DIPENDENTI DI DOCTOLIB

Gli uffici di Doctolib sono protetti da un allarme e dotati dei più moderni sistemi di sicurezza e di controllo degli accessi.
Tutti gli accessi autorizzati ai locali sono registrati.
I visitatori possono accedere ai locali solo a seguito della registrazione e sono accompagnati da un dipendente di Doctolib. Durante le visite, il terzo non sarà mai lasciato da solo o non sorvegliato.
Tutti i sistemi sono gestiti presso centri dati approvati. Questi sono dotati di sistemi di videosorveglianza e di sicurezza e di un servizio di sicurezza. Solo un piccolo gruppo di specialisti di Doctolib, debitamente formati, è autorizzato all'accesso. Ognuno di questi accessi è registrato.

Accesso da parte dei dipendenti dell'Istituto:
Specificare le eventuali misure organizzative nel caso di accesso a Doctolib da parte del personale.

Collegamento con il Sistema Informatico dell'ente:
Il collegamento con il Sistema Informatico dell'ente può essere fatto in diversi modi: (Spuntare la casella appropriata)
connettore API tra l'agenda Doctolib e quella del SI
connettore locale, l'agenda Doctolib consente di risalire alla Scheda Paziente del SI.
VPN IPSec tra il server e Doctolib (al fine di confermare la disponibilità).