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 dal Cliente/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 e ss. mod., i provvedimenti vincolanti emessi dal Garante per la Protezione dei Dati Personali 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 dei termini maiuscoli utilizzati nel 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 il Cliente/Utente.

4. QUALITÀ DELLE PARTI

Le Parti danno atto che: l'Utente/Cliente è il Titolare del trattamento Dati Personali e dei Dati Sanitari trattati attraverso i Servizi; Doctolib, ai sensi dell'art. 28 GDPR, è il Responsabile dei Trattamenti dei Dati Personali e dei Dati Sanitari riportati nell'Allegato 1.

Le Parti danno altresì atto che Doctolib e/o Siilo, in qualità di sub-responsabile, sono autorizzate dall'Utente/Cliente 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 alla prestazione dei Servizi e all'hosting dell'Admin Tool e dell'App, mentre l'incarico di Siilo è limitato alla fornitura dell'App.

4.1. Obblighi dell'Utente/Cliente

L'Utente e/o il Cliente, 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 sui Servizi e delle modalità di esercizio dei loro diritti, fornendo loro l'informativa privacy.

In qualità di Titolare del trattamento, l'Utente e/o il Cliente è l'unico responsabile dell'esattezza, affidabilità e pertinenza dei Dati Personali e dei Dati Sanitari. In particolare, è responsabile dell'uso dei Servizi e dei Contenuti Generati dall'Utente condivisi e scambiati attraverso l'App. L'Utente e/o il Cliente si obbliga a risarcire e tenere indenne Doctolib, Siilo e relativi 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, Siilo e i relativi rappresentanti, dipendenti e responsabili del trattamento derivanti dalla mancata osservanza da parte dell'Utente e/o Abbonato del presente obbligo.

L'Utente e/o il Cliente si obbliga a:

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

- Rispettare il principio di accountability, gestire i diritti degli interessati, garantendo la riservatezza dei Dati Personali e dei Dati Sanitari, in linea con la volontà espressa dai Pazienti;

- 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 le istruzioni riguardanti il Trattamento di Dati Personali e Dati Sanitari effettuato 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 referente privacye, se necessario, un responsabile della protezione dei Dati personali secondo quanto previsto dal GDPR;

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

4.2. Obblighi di Doctolib e Siilo

4.2.1. Doctolib e/o Siilo si obbligano a:

- Trattare i Dati Personali e i Dati Sanitari secondo le finalità e le modalità definite 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 utilizzare i Dati Personali e i Dati Sanitari per scopi diversi da quelli specificati nel Contratto e nel presente Accordo;

- Non sfruttare o trattare i Dati Personali e i Dati Sanitari, affidatigli dal Titolare dei trattamenti, per proprie finalità e/o per finalità di terzi, con qualsiasi modalità. In particolare, è proibito qualsiasi uso di questi Dati Sanitari per scopi pubblicitari, commerciali o statistici, di marketing;

- Avvalersi di tutti i mezzi in loro 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 sono loro 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 li 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 i periodi di conservazione dei Dati Personali e dei Dati Sanitari applicabili a ciascuna finalità e cancellarli/renderli anonimi non appena tali finalità vengano meno, secondo le indicazioni del Titolare del trattamento e fermi restando gli obblighi di legge;

- Nominare un Responsabile della Protezione dei Dati Personali.

4.2.2. Doctolib e/o Siilo si impegnano inoltre a garantire che le persone autorizzate a trattare i Dati Personali e i Dati Sanitari ai sensi del presente Accordo:

- Si impegnino a rispettare la riservatezza dei Dati Personali e dei Dati Sanitari o siano vincolati da un adeguato impegno di riservatezza;

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

Doctolib adottano le misure necessarie per assistere il Titolare del trattamento nella realizzazione delle valutazioni d'impatto relative alla protezione dei Dati Personali e dei Dati Sanitari trattati nell'ambito dei Servizi e nell'eventuale consultazione preventiva dell'autorità di controllo.

Doctolib e Siilo mettono 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 in conformità alle disposizioni del GDPR (Allegato 3.1).

In mancanza 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/Cliente può chiedere a Doctolib di modificare tali modalità nell'adempiere il Contratto.

5. VIOLAZIONE DEI DATI PERSONALI

Qualora Doctolib o Siilo vengano 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 a consentirgli, ove necessario, di comunicare tale violazione alla competente autorità di controllo e, se del caso, agli interessati.

La persona di contatto per la gestione degli incidenti che hanno un impatto sui Dati Personali e/o Dati Sanitari è privacy.italy@doctolib.com

6. TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Doctolib e Siilo dichiarano 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, ove previsto dalla legge, il loro consenso o i loro consensi (ii) le basi giuridiche dei Trattamenti effettuati, le finalità dei Trattamenti e l'elenco dei responsabili del trattamento che possono trattare i loro dati personali.

8. GESTIONE DEI DIRITTI

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

Per quanto possibile, Doctolib, in qualità di Responsabili del trattamento e su richiesta del Titolare del trattamento, potranno 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 sottoposti a una decisione individuale automatizzata (compresa la profilazione), diritto di decidere dei propri Dati Personali e Dati Sanitari, in particolare dopo il loro decesso, ecc.

9. SICUREZZA E RISERVATEZZA

Per quanto riguarda i Servizi, Doctolib e Siilo attuano 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 e dei Dati Sanitari di cui l'Utente/Cliente è Titolare, secondo quanto indicato *sub* Allegato 2 (Misure tecniche e organizzative). Per valutare il livello adeguato di sicurezza, conformemente alle disposizioni dell'articolo 32 del GDPR Doctolib e Siilo terranno 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 ai Dati Sanitari trattati.

Gli obblighi di cui sopra non liberano in alcun modo l'Utente/Cliente dall'obbligo di mettere in atto tutte le misure di sicurezza necessarie a garantire la riservatezza dei Documenti e dei Dati Abbonati, del Database Paziente, dei Dati Utenti, dei Dati Personali e dei Dati Sanitari presenti attraverso i Servizi.

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 e Siilo riconoscono e accettano che i Dati Personali e i Dati Sanitari trattati dal Titolare del trattamento attraverso i Servizi sono rigorosamente coperti dal segreto professionale cui è soggetto lo stesso Titolare (articolo 622 del codice penale).

9.3 Tenuta dei dati: Salvo diverso ed espresso accordo tra le Parti, , il Titolare del trattamento resta l'unico titolare dei Dati Cliente/Utente pubblicati attraverso i Servizi. Doctolib e Sillo non potranno rivendicare alcun diritto su tali Dati. Le statistiche di utilizzo dei Servizi, rese anonime, sono di proprietà di Doctolib.

10. PERSONALE DOCTOLIB

Doctolib e Siilo individuano 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 accetta che le attività di trattamento relative ai Servizi siano delegate da Doctolib a Siilo, società controllata al 100% da Doctolib, che agisce in qualità di sub-responsabile di Doctolib.

Inoltre, l'Utente/Cliente concede in questa sede a Doctolib l'autorizzazione generale ad avvalersi di ulteriori Responsabili 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/Cliente, con un preavviso scritto di trenta (30) giorni, di ogni cambiamento che comporti l'aggiunta o la sostituzione di ulteriori Responsabili del trattamento, offrendo così all'Utente/Cliente la possibilità di sollevare eventuali obiezioni che lo stesso dovesse avere in merito a tali cambiamenti. Se l'Utente/Cliente dovesse avere motivi legittimi e ragionevoli per opporsi alla nomina di un nuovo ulteriore Responsabile del trattamento, l'Utente dovrà tempestivamente motivare ciò a Doctolib inviandogli una comunicazione scritta al seguente indirizzo: privacy.italia@doctolib.com, entro trenta (30) giorni lavorativi successivi alla comunicazione di Doctolib, in difetto della quale si presumerà che l'Utente/Cliente abbia approvato e accettato tale nomina.

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

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

Nel caso in cui gli ulteriori Responsabili del trattamento non adempiano ai loro obblighi in materia di protezione dei Dati Personali, Doctolib rimane responsabile nei confronti del Titolare per l'adempimento da parte degli ulteriori Responsabili dei loro obblighi in conformità ai termini del Contratto.

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 una durata massima 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 all'applicazione e/o alla piattaforma Doctolib per nessuna ragione,

ed è esclusa tale attività nel corso degli audit senza che sia prestato il previo consenso di Doctolib a tal fine.

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

12.3 Almeno trenta (30) giorni prima dell'audit, il Titolare del trattamento è tenuto a inviare a Doctolib un piano di audit che specifichi l'esatta portata dei test, le date e gli orari dei test previsti e le loro condizioni. L'auditor 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.

Doctolib deve preventivamente accettare il contenuto del piano 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 auditor esterno, questi deve ottenere il previo consenso scritto di Doctolib, fermo restando che Doctolib può rifiutare il suddetto auditor solo adducendo argomenti oggettivi e motivati.

L'auditor 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 ai vizi e/o alle non conformità riscontrate.

13. ESPORTAZIONE DEI DATI

Il Cliente e l'Utente, ove applicabile, potranno esportare i Contenuti Generati dall'Utente che siano ancora conservati attraverso i Servizi per l'intera durata del Contratto, esportando direttamente il post (condiviso sul Feed di Rete) o la conversazione attraverso la funzionalità di esportazione disponibile sull'App. Se l'Utente non ha attivato il Servizio di Backup/Ripristino, per impostazione predefinita i Contenuti Generati dall'Utente vengono archiviati solo sul dispositivo dell'Utente utilizzato per i Servizi, e solo per un periodo di trenta (30) giorni.

Per gli Utenti che hanno attivato il Servizio di Backup/Ripristino, Doctolib archivia i Contenuti Generati dall'Utente sui propri Server, e si impegna a conservare una copia dei dati, a disposizione dell'Utente/Cliente per tutta la durata del Contratto.

Decorso il termine di 7 giorni dalla cessazione del Contratto, Doctolib si impegna a distruggere i Dati Personali e i Dati Sanitari senza conservarne copia, fatti salvi gli obblighi di conservazione cui è soggetta Doctolib ai sensi di legge. L'avvenuta distruzione dei Dati Personali Sanitari può essere comunicata su richiesta del Titolare.

15. 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 dei dati personali e dei diritti e delle libertà fondamentali delle persone, in conformità con la normativa applicabile.

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

Se il trasferimento avviene verso un Paese terzo la cui normativa non è stata riconosciuta come in grado di offrire un adeguato livello di protezione dei Dati Personali, Doctolib garantisce che sono 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 l'ulteriore Responsabile del trattamento.

In qualità di Responsabile del trattamento, Doctolib e Siilo si impegnano a 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.

Inoltre, su eventuale richiesta, Doctolib potrà comunicare alle autorità amministrative e giudiziarie i Dati Personali che tratta in nome e per conto del Titolare per adempiere ai propri obblighi di legge. In tal caso, e salvo quanto diversamente previsto dalla legge, Doctolib si impegna a informare il Titolare del trattamento di tale comunicazione.

16. 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 da considerarsi lo stabilimento principale del gruppo Doctolib, ai sensi dell'art. 4 n.16 del GDPR. L'autorità di controllo capofila per i trattamenti transfrontalieri ai sensi dell'art. 56 GDPR del gruppo Doctolib è il CNIL (https://www.cnil.fr). Per i trattamenti che non rientrano nella competenza dell'autorità di controllo capofila, l'autorità competente è il Garante per la protezione dei dati personali (https://www.garanteprivacy.it/). Il Responsabile della protezione dei dati 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 privacy.italia@doctolib.com.

17. LEGGE APPLICABILE

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

18. 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/Cliente 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: il Cliente sottoscrittore di un Abbonamento e/o l'Utente avente un account Utente.

Le attività del Titolare del trattamento comprendono Trattamenti che consentono l'esercizio di attività funzionale alla prenotazione ed erogazione 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 effettuati devono rispondere a un obiettivo preciso ed essere giustificati alla luce della mission e delle attività degli Operatori e Professionisti Sanitari.

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: FORNITURA DI UN SERVIZIO DI MESSAGGISTICA ISTANTANEA (Doctolib Siilo Messanger e Doctolib Siilo Webchat)

OPERAZIONI DI TRATTAMENTO:

I Servizi implicano la raccolta, la registrazione, l'organizzazione, la conservazione, l'estrazione, la consultazione e l'utilizzo, la comunicazione per la trasmissione, l'anonimizzazione e la cancellazione dei Dati personali di seguito elencati.

FINALITÀ:

Il Servizio di messaggistica istantanea è progettato per garantire un migliore coordinamento delle cure, consentendo agli Utenti di comunicare e inviare messaggi di testo, video, foto, note vocali e altri media. Consente discussioni individuali e discussioni di gruppo.

1/ Facilitare la comunicazione tra i Professionisti Sanitari offrendo un canale di scambio sicuro tramite la messaggistica istantanea;
2/ Consentire lo scambio di documenti o altri media e dati che possono includere Dati personali dei Pazienti;
3/ Consentire agli Utenti di bloccare o sbloccare un altro Utente;
4/ Reporting, debug e statistiche.

BASE GIURIDICA

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

A titolo indicativo, il legittimo interesse potrebbe costituire la base giuridica. Il Titolare del trattamento è libero di indicare a Doctolib un'altra base giuridica.

Nel caso in cui il Titolare del trattamento comunichi i Dati anagrafici del paziente a un Professionista Sanitario che non fa parte del team di cura del Paziente in questione, il Titolare del trattamento deve prima ottenere il consenso del Paziente.

INTERESSATI:

1/ Pazienti
2/ Professionisti Sanitari con o senza un Account

TIPOLOGIE DI DATI PERSONALI:

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

- Dati di identificazione dei Professionisti Sanitari;
- Dati di contatto dei Professionisti Sanitari;
- Anamnesi medica, familiare e allergie;
- Dati della visita;
- Dati relativi alla prescrizione;
- Dati biometrici e biologici;
- Dati relativi al team di assistenza sanitaria;
- Immagini diagnostiche;
- Foto, video;
- Note vocali;
- Per le videochiamate e le chiamate vocali: flusso video/vocale che consente la trasmissione tra Professionisti Sanitari;
- Informazioni di utilizzo e di connessione ai Servizi dell'Utente/Cliente.

DESTINATARI DEI DATI:

- Professionisti Sanitari in possesso di un Account.

PERIODO DI CONSERVAZIONE:

A meno che l'Utente non abbia attivato l'opzione "Conserva la conversazione" nell'impostazione specifica di ciascuna conversazione, tutti i messaggi verranno eliminati dopo un periodo di trenta (30) giorni.

TRATTAMENTO N°2: FORNITURA DI UNA RETE ORGANIZZATIVA PRIVATA (Doctolib Siilo per le Organizzazioni)

OPERAZIONI DI TRATTAMENTO:

Il Servizio comporta 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:

Attraverso Doctolib Siilo per le Organizzazioni, i dipendenti/membri dell'organizzazione possono facilmente trovarsi e contattarsi a vicenda e condividere informazioni tramite il Feed di Rete. Attraverso l'Admin Tool del Servizio Doctolib Siilo per le Organizzazioni, il personale del Cliente può configurare e personalizzare la propria Rete Organizzativa, trasmettere messaggi, invitare persone a unirsi alla rete, pre-impostare conversazioni per gli Utenti.

Doctolib può anche eseguire report, debugging e statistiche per conto del Titolare.

BASE GIURIDICA DEL TRATTAMENTO:

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

A titolo indicativo, il legittimo interesse potrebbe costituire la base giuridica. Il Titolare è libero di indicare a Doctolib ogni altra base giuridica che ritenga opportuna.

INTERESSATI:

- Pazienti
- Professionisti Sanitari o Assistenti con un Account

TIPOLOGIE DI DATI PERSONALI:

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

- Dati identificativi, professionali e di contatto dei Professionisti Sanitari e Assistenti facenti parte dell'organizzazione del Titolare;
- Anamnesi medica, familiare e allergie;
- Dati della visita;
- Dati relativi alla prescrizione;
- Dati biometrici e biologici;
- Dati relativi al team di assistenza sanitaria;
- Immagini diagnostiche;
- Foto;
- Log di utilizzo e connessione che riportano le "azioni" degli Utenti all'interno dei Servizi nonché log tecnici che riportano l'"attività" dei componenti software e hardware utilizzati dall'Utente/Cliente affinché Doctolib possa garantire il funzionamento e l'accesso alle funzionalità richieste.

DESTINATARI E RESPONSABILI ULTERIORI DEL TRATTAMENTO:

- Professionisti Sanitari in possesso di un Account.

PERIODO DI CONSERVAZIONE:

Salvo diversa specifica indicazione da parte del Titolare, Doctolib applicherà i periodi di conservazione raccomandati dalle autorità competenti in materia di protezione dei dati personali o dalla normativa applicabile.

ALLEGATO 2: MISURE TECNICHE E ORGANIZZATIVE

Le misure tecniche e organi*zzative implementate da Doctolib per la fornitura dei Servizi si basano sulle misure e sui processi di sicurezza di Siilo.*

Politiche organizzative e controlli amministrativi

Siilo ha implementato un sistema di gestione della sicurezza delle informazioni (ISMS) ed è certificata ISO27001 e NEN7510 (standard olandese per la gestione della sicurezza delle informazioni nel settore sanitario).

Come parte dell'ISMS, Siilo ha implementato diverse policy e controlli organizzativi e amministrativi come valutazioni del rischio periodiche, standard, audit interni, una policy di sicurezza delle informazioni, una policy di privilegio minimo, formazione del personale, una procedura di gestione degli incidenti (di sicurezza) e un procedura di gestione e notifica delle violazioni dei dati. L'obiettivo dell'ISMS di Siilo è consentire un ulteriore miglioramento dell'organizzazione, del personale e dei suoi prodotti.

Ogni soluzione implementata da Siilo passa attraverso una valutazione del rischio e, quando richiesto, attraverso una valutazione dell'impatto sulla protezione dei dati. Segue un processo rigoroso salvaguardato dalle politiche ISMS dimostrate dai nostri certificati ISO-27001 e NEN7510.

Processo di sviluppo

Il processo di sviluppo di Siilo si basa su diverse strategie per garantire sia la qualità che la sicurezza dei dati:

(1) Test unitari: per ogni funzionalità Siilo sviluppa una serie di test di base che esercitano quella funzionalità in modo isolato;

(2) Peer code review: le modifiche all'app vengono esaminate da almeno due sviluppatori prima dell'accettazione in una versione beta. Per le funzionalità che influiscono sulla sicurezza o sulle attività relative alla privacy, queste nuove righe di codice software vengono esaminate da uno sviluppatore senior esterno al team che interagisce con il responsabile della sicurezza e il team privacy prima di rilasciare le nuove funzionalità;

(3) Test manuale e beta pubblica limitata: prima del rilascio, le funzionalità vengono rilasciate internamente per il test manuale e spesso vengono rilasciate anche a un pool selezionato di "beta tester amichevoli". Questo approccio viene utilizzato per vagliare le funzionalità specifiche del dispositivo, nonché tutte le funzionalità che possono emergere solo dopo essere state esposte a una serie diversificata di flussi di lavoro.

Privilegi minimi

I privilegi sono forniti al personale autorizzato in base al rigoroso rispetto del principio di necessità. Questo viene monitorato e verificato annualmente da un responsabile della sicurezza. Qualsiasi dipendente che ha bisogno di accedere a informazioni al di fuori del proprio ruolo assegnato, deve prima registrare la richiesta con un modello standard. Queste richieste vengono esaminate una volta al trimestre.

Politiche e controlli tecnici

Dati del messaggio - dati in transito

Per conoscere le soluzioni implementate per mitigare i rischi per i dati in transito, si prega di consultare il white paper sulla sicurezza di Siilo (https://www.siilo.com/resource s/security-white-paper) che descrive in dettaglio l'approccio security-by-design, il modello di minaccia e i protocolli crittografici.

In breve, Siilo utilizza la crittografia end-to-end implementata con LibSodium, un fork della libreria crittografica NaCl https://nacl.cr.yp.to/.

Ciò significa che ogni messaggio tra mittente e destinatario è protetto tramite una coppia di chiavi pubblica/privata. Solo il mittente e il destinatario sono in grado di decrittografare e leggere i messaggi che si scambiano e l'autenticità di qualsiasi messaggio può essere verificata empiricamente. Terze parti, inclusa Doctolib e Siilo, non sono mai in grado di leggerli.

Siilo utilizza il blocco dei certificati per prevenire i cosiddetti "attacchi man-in-the-middle", un processo in base al quale gli aggressori accedono al traffico tra i telefoni e tentano di entrare e toccare le linee di comunicazione per leggere i messaggi. Le comunicazioni standard TLS v1.2 richiedono un certificato SSL valido emesso da un'autorità di certificazione attendibile, riconosciuta dal dispositivo. Il blocco dei certificati va oltre e impone che tali certificati debbano essere emessi solo da una catena di fiducia radicata a un emittente specificato. Ciò chiude una serie di vulnerabilità derivanti dai problemi di distribuzione delle chiavi associati all'infrastruttura dell'autorità di certificazione di Internet.

Dati del messaggio - dati inattivi sul dispositivo dell'Utente

Per i dati inattivi sul dispositivo (iPhone, iPad, Android) sono previste le seguenti misure di sicurezza:

- Tutto il "materiale chiave", noto anche come i codici utilizzati dal sistema di crittografia, viene archiviato nel KeyChain iOS o nel KeyStore Android, a seconda dei casi;
- Tutto il "materiale della chiave" è crittografato da una "chiave principale" derivata dal Codice Pin scelto dall'Utente;
- L'intero database è crittografato utilizzando SQLiteCipher. Tutti i messaggi, i metadati dei messaggi e le informazioni di contatto vengono archiviati in questo modo;
- Tutti i supporti ricevuti vengono archiviati una volta crittografati dalla chiave di crittografia simmetrica monouso. A questa chiave si accede tramite il database di cui sopra;
- Un meccanismo di Codice Pin a livello di applicazione impedisce l'accesso da parte di persone che possono accedere fisicamente al dispositivo. Questo risolve la maggior parte delle forme di ingegneria sociale, come ad esempio la richiesta di prendere in prestito il telefono per una chiamata veloce, ecc.
- Tutte le informazioni scambiate nel servizio di messaggistica vengono automaticamente cancellate dopo 30 giorni. Gli Utenti possono decidere autonomamente di eliminare i singoli messaggi ad hoc se ritengono che 30 giorni siano troppo lunghi. Siilo consapevolmente non ha incluso i timer per il conto alla rovescia e la durata dei messaggi come secondi/ore, in quanto potrebbe creare un

senso di urgenza con conseguente screenshot e altri comportamenti indesiderati;
● Quando un Utente sa che il suo dispositivo è stato smarrito, rubato o altrimenti compromesso, può avvisare la propria organizzazione (questa è una funzionalità di Doctolib Siilo per le organizzazioni) e un Amministratore può cancellare da remoto i dati di Siilo dal dispositivo.

Dati dei messaggi - dati inattivi sui server

Per i dati inattivi sui server Siilo sono in atto le seguenti misure di sicurezza:
● Tutti i server Siilo si trovano all'interno dell'Unione Europea e rispettano le più stringenti norme di sicurezza e conformità;
● Le regole del firewall impediscono l'accesso di rete ai database (MySQL ed ElasticSearch) ed è limitato a una sottorete contenente i server di Siilo e una VPN, a cui può accedere un sottoinsieme limitato di dipendenti di Siilo;
● Il database MySQL è protetto da password e crittografato secondo lo standard del settore AES-256 e memorizza i dati di messaggistica, i metadati di messaggistica, i dati di configurazione di Siilo Connect e i dati del profilo utente;
● ElasticSearch crittografa campi specifici come e-mail e numeri di telefono per consentire la corrispondenza. Altri campi del profilo che vengono mostrati nell'app Doctolib Siilo Messenger come "pubblici" per gli utenti sono memorizzati in testo normale;
● Tutti i media (inviati tramite l'applicazione e quindi considerati sensibili) vengono archiviati e crittografati dalla chiave di crittografia simmetrica monouso. Quella chiave non è memorizzata su nessun server Siilo, se non come parte dei dati dei messaggi crittografati archiviati in MySQL. Le chiavi per decrittografare tali dati sono disponibili solo sui dispositivi del mittente e del destinatario. Conservazione dei dati personali sui server Siilo
● I dati dei messaggi vengono archiviati presso i server a Francoforte (Germania) e, a scopo di backup, vengono acquisite "istantanee" automatiche giornaliere che vengono archiviate per non più di 7 giorni. Questi snapshot vengono crittografati quando sono inattivi. L'infrastruttura server di Siilo è ospitata da Amazon, Inc. Siilo ha scelto di proposito Amazon Web Services (AWS) in quanto utilizza i più elevati standard di sicurezza e crittografia e garantisce la conformità (GDPR) con il loro livello SOC I-II-III, ISO9001, ISO27001, ISO27017 e le certificazioni ISO27018.

Dati Utente

I dati degli Utenti vengono archiviati nei server a Dublino (Irlanda) e viene eseguito il backup quotidianamente e archiviati per non più di 30 giorni in un bucket preconfigurato che viene crittografato a riposo.

Numero di telefono corrispondente sul servizio di messaggistica

Siilo facoltativamente consente all'Utente di scoprire altri contatti Siilo mediante riferimenti incrociati con la rubrica del telefono. Se l'Utente sceglie di farlo, le seguenti informazioni vengono caricate tramite una connessione TLS crittografata al server:

(1) Primi 64 bit dell'hash SHA1 della forma normalizzata E.164 di ciascun numero di telefono trovato nella rubrica del telefono

(2) Legenda: EEDAAC207FC6BA08727C

(3) Solo i numeri di telefono sono sottoposti ad hashing e riferimenti incrociati. Siilo non tocca i nomi associati, gli indirizzi e-mail e le altre informazioni contenute nella rubrica del telefono. Il server Siilo confronta quindi l'elenco di hash dell'utente con gli hash telefonici noti degli attuali utenti Siilo. Il server corrisponderà solo agli attuali utenti Siilo e, dopo aver restituito le corrispondenze al client mobile, il server scarterà immediatamente gli hash inviati.
Le misure di sicurezza sono descritte nel white paper sulla sicurezza di Siilo disponibile qui.