Doctolib

Il nostro impegno in materia di privacy e sicurezza nei confronti dei nostri utenti.

In Doctolib crediamo che i dati personali e sanitari necessitano di un'attenzione particolare. Come azienda europea che fornisce servizi online sia ai professionisti sanitari che ai pazienti, ci impegniamo a fondo nel proteggere le informazioni e la privacy dei nostri utenti. Per questo motivo, sin dalla nostra creazione nel 2013, implementiamo un'ampia gamma di misure di sicurezza e ci impegniamo nel valutare costantemente nuove tecnologie.

CI IMPEGNIAMO A PROTEGGERE I DATI DEI NOSTRI UTENTI

1° Applichiamo un'ampia gamma di misure di protezione e esploriamo costantemente nuove tecnologie in materia di sicurezza.

- Proteggiamo gli account dei nostri utenti con i) Autenticazione a 2 fattori come impostazione predefinita per gli account dei pazienti e dei medici ii) Requisiti di complessità delle password e archiviazione crittografica, iii) Controllo degli accessi basato sui ruoli.
- Sviluppiamo la nostra applicazione in linea con le migliori pratiche dell'Open Web Application Security Project (OWASP), una accreditata fondazione no-profit che lavora per migliorare la sicurezza del software.
- La nostra infrastruttura è protetta da: Cloud firewall moderni, Hardening dei sistemi, Sistemi di rilevamento e prevenzione delle intrusioni, Sistemi di filtraggio degli accessi, Centro operativo di sicurezza (SOC) 24/7, Protezione DDoS

2° I nostri utenti beneficiano di tecniche di crittografia avanzate. Tutti i dati di Doctolib sono criptati, a riposo e in transito.

- Per la crittografia dei dati a riposo, le chiavi di crittografia master sono conservate presso ATOS, fornendo un ulteriore livello di protezione che impedisce l'accesso anche al nostro provider di soluzioni di hosting.
- Per la crittografia dei dati in transito, applichiamo la crittografia TLS ("Transport Layer Security"), un protocollo crittografico progettato per garantire la sicurezza delle comunicazioni sulle reti informatiche. Il canale di crittografia viene sempre terminato in Europa e sanificato dai payload di attacco dal nostro Web Application Firewall (Cloudflare). I certificati TLS di Doctolib non vengono mai rivelati a Cloudflare grazie alla tecnica di keyless handshake.

.**3° I dati dei nostri utenti si trovano in un luogo sicuro.** Abbiamo scelto AWS (Amazon Web Services) come host dei dati in quanto offre una delle soluzioni più rigorose e sicure al momento.

- AWS è certificata dai principali standard internazionali, tra cui l'ISO/IEC 27001, e viene sottoposta a regolari controlli.
- In Francia, AWS è certificata dal marchio francese Hébergeur de Données de Santé (HDS) in conformità alla legge e agli standard stabiliti dall'Agence du Numérique en Santé, in consultazione con la Commission nationale de l'informatique et des libertés (CNIL).
- In Germania, AWS ha ottenuto l'attestazione C5, pubblicata dall'Ufficio federale tedesco per la sicurezza informatica (BSI).
- La sicurezza fisica dei data centers è garantita 24 ore su 24, 7 giorni su 7.

4° Ci sottoponiamo regolarmente a certificazioni, audit di terze parti e controlli normativi.
Doctolib ha ottenuto la certificazione ISO/IEC 27001 in Germania e Francia e HDS ("healthcare data storage") in Francia dal Gruppo BSI, un importante ente di certificazione internazionale: questo dimostra che abbiamo implementato i giusti processi (basati sulla gestione del rischio), le migliori pratiche e testimonia il nostro impegno a lungo termine per la protezione dei dati (queste certificazioni prevedono audit di controllo annuali e audit di rinnovo ogni 3 anni).

5° La priorità alla sicurezza si riflette nei nostri investimenti a lungo termine.

- Abbiamo investito molto nella privacy sin dal lancio di Doctolib nel 2013.
- Abbiamo un team numeroso di esperti tecnici e legali dedicati alla sicurezza e alla privacy a Parigi e a Berlino.

CI IMPEGNIAMO A PROTEGGERE LA PRIVACY DEI NOSTRI UTENTI

6° Non vendiamo i dati dei nostri utenti.
Il modello di business di Doctolib si basa principalmente su un abbonamento pagato da professionisti e istituzioni sanitarie per l'utilizzo delle nostre soluzioni software.

7° I dati sono conservati in Europa.
I dati sono archiviati in Francia e in Germania presso un provider di hosting autorizzato: AWS (Amazon Web Services).

8° La privacy è al centro dello sviluppo dei nostri servizi.
I nostri esperti di sicurezza e legali lavorano fianco a fianco con i team Tech & Product nello sviluppo di nuovi servizi, dalla loro ideazione fino al loro rilascio.

9° I nostri servizi sono progettati per essere conformi alle normative nazionali ed europee sulla privacy.
Fin dalla nostra creazione, il rispetto di tutte le normative sulla protezione dei dati sanitari personali è stato al centro delle nostre attività: il Regolamento Generale Europeo sulla Protezione dei Dati (GDPR), la direttiva ePrivacy e le leggi locali sulla privacy: *Loi Informatique et Libertés* (LIL) in Francia, *Bundesdatenschutzgesetz* (BDSG) e *Datenschutz-Grundverordnung* (DSGVO) in Germania e il Codice in materia di protezione dei dati personali in Italia.

10° I nostri utenti possono modificare le loro funzioni di sicurezza per una maggiore privacy.
I nostri utenti possono modificare in qualsiasi momento le loro impostazioni sulla privacy i) Autenticazione a 2 fattori quando si connettono al loro account da un nuovo dispositivo, ii) Aggiunta di un codice a 4 cifre per limitare l'accesso alla propria applicazione mobile, iii) Sblocco della propria applicazione mobile tramite Face ID / Touch ID (dispositivi iOS) o tramite impronta digitale (Android).