Doctolib

Our commitments to our users on privacy and security.

At Doctolib, we believe that personal and health information deserve extra care. As a European company providing online services to both care teams and patients, we're deeply committed to protecting our users' information and privacy. This is why, since our creation in 2013, we have been enforcing a wide array of protection measures as well as constantly exploring new technologies.

WE'RE COMMITTED TO PROTECTING OUR USERS' DATA.

1° We enforce a wide array of protective measures and constantly explore new security technologies.

- We protect our users' accounts by Two-Factor authentication by default for both patients and practitioners' accounts, Password complexity requirements and cryptographic storage and Role-based Access Control.
- We develop our application in line with the best practices of the Open Web Application Security Project (OWASP), a recognized nonprofit foundation that works to improve the security of software.
- Our infrastructure is protected by modern cloud firewalls, systems hardening, intrusion detection and prevention systems, access filtering systems, 24/7 Security Operations Center (SOC) and DDoS protection.

2° Our users benefit from advanced encryption techniques.

- All Doctolib data is encrypted, at rest and in transit.
- On top of that, we have set extra security measures:
    - For encryption of data at rest, master encryption keys are stored at ATOS, providing an additional protection layer preventing access even from our own hosting solution provider.
    - For encryption of data in transit, we enforce TLS encryption ("Transport Layer Security"), a cryptographic protocol designed to provide communications security over a computer network. The encryption tunnel is always terminated in Europe and sanitized from attack payloads by our Web Application Firewall (Cloudflare). Doctolib's TLS certificates are never disclosed to Cloudflare thanks to keyless handshake technique.
- We also resort to advanced encryption techniques such as end-to-end encryption or server-side encryption and will continue to explore technology breakthroughs.

3° Our users' data are in a safe place.

- We have chosen AWS (Amazon Web Services) to host data as it offers one of the most demanding and secure solutions as of today.
- AWS is certified by the main international standards, including ISO/IEC 27001 and is audited regularly.
- In France, AWS is certified by the French label *Hébergeur de Données de Santé* (HDS) in accordance with the law and the standards established by the *Agence du Numérique en Santé*, in consultation with the *Commission nationale de l'informatique et des libertés* (CNIL).
- In Germany, AWS received the C5 attestation based on the criteria of the BSI.

- Their data centers benefit from 24/7 physical security.

4° We regularly undergo certifications, third party audits and regulatory controls.

- Doctolib has been certified ISO/IEC 27001 in Germany and France and HDS ("healthcare data storage") in France by BSI Group, a leading international certification body: this proves that we have implemented the right processes (based on risk management), the best practices and it is a testimony to our long-term commitment to data protection (these certifications involve yearly control audits and renewal audits every 3 years).
- As one of the first E-Health providers, Doctolib receives the C5 attestation based on the demanding criteria of the Federal Office for Information Security (BSI).

5° Our priority towards security is reflected in our long-term investments.

- We have been investing heavily in Privacy since the launch of Doctolib in 2013.
- We have a large team of technical and legal experts dedicated to security and privacy in Paris and Berlin.

WE CARE ABOUT OUR USERS' PRIVACY.

6° We do not sell our users' data.

- Doctolib's business model is mainly based on a subscription paid for by health professionals and health institutions for the use of our software solutions.

7° Data is stored in Europe.

- Data is stored in France and in Germany at an approved hosting provider: AWS (Amazon Web Services).

8° Privacy is at the core of the development of our services.

- Our security and legal experts work hand in hand with the Tech & Product teams to accompany the development of new services from their conception until their release.

9° Our services are designed to comply with national and European privacy regulations.

- Since our creation, respecting all the regulations on the protection of personal health data has been at the forefront of what we do: the European General Data Protection Regulation (GDPR), the ePrivacy directive and local privacy laws: *Loi Informatique et Libertés* (LIL) in France, *Bundesdatenschutzgesetz* (BDSG) and *Datenschutz-Grundverordnung* (DSGVO) in Germany and the *Codice in materia di protezione dei dati personali* in Italy.

10° Our users can control their security parameters for enhanced privacy.

- Two-Factor authentication when connecting to their account on a new device.
- Addition of a 4-digit code to limit access to their mobile application.
- Unlocking of their mobile app via Face ID / Touch ID (iOS devices) or via fingerprint (Android).