OCTOBER HEALTH DATA BRIEF | SECURING WHAT MATTERS

At October, protecting the privacy and security of our users personal information is our top priority. This document outlines our data practices:

1. **What is the lawful basis for processing personal information?**

   We process the personal data of individuals who use our platform. This processing is based on the consent of those individuals, who voluntarily sign up to use the October Health app and agree to our Terms & Conditions and Privacy Policy when creating an account. Through agreeing to these terms, users provide their informed and explicit consent for October Health to process their personal data in order to provide our service.

2. **Data collected**

   One of the platform's main requirements is to provide as much anonymity to a user as possible. We collect only the minimum amount of personal information necessary for account creation, including email, nickname, gender (optional), age range and selected interests.

   No additional personally identifiable information is requested. Any user-generated content is voluntarily provided, for example where a user submits information in chats, through coaching or in their journals.

   Our data categories include the following:

   - Account Information: Email address, username, password (hashed), gender, age range
   - User Content: Any text or audio uploaded by users
   - Usage Data: App usage data such as screens viewed, buttons clicked
   - Device Information: IP address, browser type, operating system

3. **Data transfers**

   Data is transferred to the UK, the EU and the US where our servers are hosted. This is noted in our Privacy Policy, which users consent to.

4. **User rights**

   Users can access, modify or delete their personal information. We fully support the right to be forgotten - users can request account deactivation and their data will be anonymized. October Health keeps personal information for as long as a contractual relationship exists and in accordance with applicable legal obligations and applicable statute of limitation periods, unless a user opts out or withdraws their consent. Generally information is kept for 5 years to maintain customer records and provide ongoing services. This includes names, contact details, and inquiry information. However, users can request deletion of their personal data at any time. October Health will promptly comply with deletion requests unless there is a legitimate reason permitted by law to retain the data, such as to complete a transaction.

When a user deletes their October account, all their personal information is then anonymized. This means that their personal information is randomized (cannot be forward or backward solved), and profiles are deactivated on our side once they delete their October account.

We do not fully delete their profile to ensure that reporting and analytics are not impacted. By anonymizing the user information, we can ensure that user's data remains inaccessible whilst still being able to aggregate data where required. This is compliant with GDPR and POPIA regulations.

5. Data protection and compliance

October has a full-time head of Legal and Data Protection Officer and CISO ensuring our compliance with standards such as GDPR, HIPAA, POPIA and other data protection needs. We are also SOC2 certified, demonstrating our compliance with stringent security, availability and confidentiality standards.

6. Audits and monitoring

We utilize automated hourly and weekly security scans to detect vulnerabilities or issues. Our API backend undergoes weekly third-party penetration testing, and our source code is scanned hourly for any vulnerable components. We also conduct comprehensive penetration testing of our entire platform once a year through 3rd party providers, and our reports (both SOC2 and pentesting) are available for enterprise clients on request.

7. Infrastructure

All data and systems are hosted in Europe, the UK and US. Our provider is AWS. This environment is SOC2 and PCI compliant. Access to personal information is restricted to only staff who need it for their job functions. All data that is used by the platform is encrypted in transit and at rest (where it is stored). The app makes use of a PostgreSQL database and a Redis in memory datastore, which are encrypted and access controlled. Passwords are also hashed and individually salted.

8. Data sharing

Any statistical data shared with partners is fully anonymized and aggregated. Partners do not have access to identifiable personal information.

October Health does not sell or share personal information with any third parties for their own commercial purposes.

Personal data may be shared only with our partners and service providers for limited purposes such as:

- Delivering our services and support
- Ensuring security and performance of our platform
- Managing payments and billing
- Conducting regulated health operations
- Complying with law enforcement requests as required by law

All October Health partners and vendors are required to comply with our strict confidentiality and security standards when handling any personal data. Partners only receive the minimum data required to perform contracted services.

While we may utilize third-party partners to assist in operations, October Health maintains control over personal information at all times. We do not allow partners to use data for their own purposes or share it further.

9. Recipients of Data

Refer to the 3rd Party Service Provider list from October.

10. Password policies and device security

October uses several password policies to enforce secure passwords for your users:

- Password to email similarity is prevented
- Minimum length and complexity is required
- Common passwords are disallowed
- Purely numeric passwords are disallowed

Passwords are protected using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST. This also includes a unique salt per user password preventing precomputation attacks.

Devices use local authentication as a second factor where supported (e.g. FaceID) to protect phone access.

Corporate clients can choose additional login security such as a second factor email OTP, etc.

We are committed to minimizing collection of user data, restricting access only to authorized staff, and prioritizing privacy across our systems and operations. Please let us know if you have any additional questions! You can contact us on security@october.health