Privacy Policy

KeepYourHabits

Effective Date: 1 February 2026

Last Updated: 1 February 2026

---

1. Who We Are

Data Controller:

- **Name: Grohmann Patrik Tamás**
- **Address:** ***Address available on request***
- **Email:** patrikgrohmann@gmail.com
- **Website:** keepyourhabits.com

Data Protection Officer or Privacy Lead:
We have not appointed a Data Protection Officer. For all privacy-related queries, please contact us at patrikgrohmann@gmail.com

This privacy policy applies to the KeepYourHabits app and website (collectively, "the Service"). We are committed to protecting your privacy in accordance with the UK General Data Protection Regulation (UK GDPR) and the EU General Data Protection Regulation (EU GDPR), as we process personal data of users worldwide, including those in the EU and UK.

---

2. What Data We Collect

We collect personal data directly from you when you use our Service. Below we describe each category:

2.1 Account Data

When you create an account, we collect:

- **Email address** (required for account creation and login)
- **Name** (you may provide any name, including pseudonyms or aliases)
- **Authentication credentials** (password hash or authentication tokens from Google/Apple sign-in providers)

2.2 Habit Activity Data

Once you begin using the app, we collect:

- **Habit entries:** Data about habits you create and track (e.g., habit name, description)
- **Completion records:** Dates, times, status of your habit completions and notes
- **Progress metrics:** Streaks, completion rates, and other habit-related statistics
- **Timestamps:** When you access the app and interact with features

These are the core features that we need to store for the service to work.

2.3 Device and Technical Data

Our Service automatically collects:

- **IP address**
- **Device type and model** (e.g., iPhone 15, Samsung Galaxy S24)
- **Operating system and version** (e.g., iOS 17, Android 14)
- **App version and build number**
- **Online identifiers:** Unique identifiers assigned by our service providers (e.g., Firebase Installation ID) and platform providers (Google/Apple)

2.4 App Store and Platform Data

We receive aggregated analytics from:

- **Google Play Store:** Install counts, geographic regions, crash reports, review data
- **Apple App Store:** Install counts, geographic regions, crash reports, review data
- **Web server logs:** IP addresses, browser type, pages visited, timestamps

These platforms act as independent data controllers for their own analytics. Refer to Google Play Privacy Notice and Apple Privacy Policy for their data practices.

2.5 Authentication Provider Data

When you sign in via Google or Apple:

- We receive your **email address** and **profile name** from the provider
- We do not request or access contacts, calendar, or other sensitive data
- **Google Sign-In:** See Google Account Privacy Notice
- **Apple Sign-In:** See Apple Privacy Policy

Google and Apple act as independent controllers for their sign-in data.

2.6 Newsletter Signup Data (Optional)

If you manually opt in to our newsletter:

- **Email address**

- **Signup timestamp**
- **Consent flag** (recording that you explicitly consented)

Note: Newsletter signup is a separate, manual process and is **not** part of account creation or onboarding.

---

3. Why We Collect This Data

3.1 Core Service Delivery

We process your email, name, and habit data to:

- Create and maintain your account
- Sync your habit data across devices (mobile and web)
- Display your progress and habit history
- Send functional notifications (e.g., habit reminders, account security alerts)
- Enable you to access, update, and delete your data

Your email and habit data are required to provide the Service. If you do not provide them, we cannot offer the Service.

3.2 Security, Stability, and Legitimate Interests

We process device/technical data to:

- Prevent fraud and abuse
- Debug and improve app stability
- Monitor server performance and security
- Comply with legal obligations

Legal Basis: Legitimate interests in providing a secure, stable Service.

3.3 Analytics and Service Improvement

We may use aggregated, anonymized habit data and technical metrics to:

- Understand feature usage patterns
- Identify bugs and performance bottlenecks
- Improve user experience

No individual user habits are sold or shared for marketing. We may disclose anonymized usage statistics to investors or partners to demonstrate product value.

Legal Basis: Legitimate interests in improving the Service.

3.4 Email Communications

We send newsletters and promotional emails **only to users who have explicitly opted in** via our separate newsletter signup form.

- **Functional emails** (account confirmations, password resets, security alerts) are sent without separate consent as they are necessary for the Service.
- **Marketing and newsletter emails** are sent only with your affirmative, separate consent, and you can unsubscribe at any time (see Section 7).

Legal Basis: Consent for Marketing

---

4. How We Store and Protect Your Data

4.1 Data Storage Location

- **Primary storage:** AWS (Amazon Web Services) EU region: **Europe (Stockholm, Sweden)**
- **Backups:** Retained within EU/UK regions; no transfers outside the UK/EU except where required by law
- **No cross-border transfers:** Your data is processed and stored exclusively within the EU/UK

4.2 Security Measures

We implement technical and organizational measures to protect your data:

- **Encryption:** Data in transit uses TLS/SSL encryption; data at rest is encrypted via AWS Key Management Service (KMS)
- **Access controls:** Only authorized employees and service providers can access your data
- **Database security:** AWS security groups, VPC isolation, and least-privilege access
- **Authentication:** Secure password hashing; optional multi-factor authentication where applicable
- **Monitoring:** Automated security monitoring and threat detection
- **Incident response:** We have procedures to detect, investigate, and remediate data breaches; we will notify affected users where required by law

Despite these measures, no system is 100% secure. We recommend using a strong, unique password.

---

5. Who We Share Your Data With (Recipients and Processors)

5.1 Service Providers (Data Processors)

AWS (Amazon Web Services)

- **Role:** Cloud infrastructure provider (data processor)
- **Data processed:** All account data, habit data, and backups
- **Location:** EU (Stockholm) region only
- **Contract:** AWS Data Processing Agreement complies with UK/EU GDPR
- **Details:** AWS Data Privacy Notice

Google (Firebase)

- **Role:** Backend analytics, crash reporting, and app development platform (data processor)
- **Data processed:** Device IDs, crash logs, analytics events, diagnostic data
- **Location:** Google may process data in EU and non-EU regions
- **Contract:** Google Signs data processing agreement for Firebase
- **Note:** Firebase may automatically collect diagnostic and crash data to improve app stability; you can disable non-essential analytics in app settings (where available)
- **Details:** Google Firebase Privacy Notice

Google Play Store

- **Role:** App distribution platform (independent controller for its own analytics)
- **Data processed:** Installs, reviews, crashes, region data
- **Details:** Google Play Privacy Notice

Apple App Store

- **Role:** App distribution platform (independent controller for its own analytics)
- **Data processed:** Installs, reviews, crashes, region data
- **Details:** Apple Privacy Policy

Sign-In Providers (Google/Apple)

- **Role:** Authentication service providers (independent controllers)
- **Data processed:** Email, profile name
- **Details:** Google Account Privacy, Apple Privacy

5.2 Newsletter/Email Service

- **Service Provider:** AWS SES
- **Role:** Email distribution and list management (data processor)

- **Data processed:** Email address, consent flag, engagement metrics (opens, clicks)
- **Location:** That data (email, name, basic technical info) is processed on their infrastructure in the EU (and possibly other regions when routing to recipients).
- **Contract:** AWS Data Processing Agreement complies with UK/EU GDPR
- **Details:** AWS Data Privacy Notice

5.3 No Sale or Sharing of Personal Data

We **do not sell** your personal data to third parties.
We **do not share** your personal data with advertisers or data brokers.
We **do not use** your data for targeted advertising on social media platforms.

We may share aggregated, anonymized data (e.g., "50% of users complete their habits in the morning") with investors or partners for business intelligence purposes. This data cannot identify you.

5.4 Legal Obligations

We may disclose your data if required by law (e.g., court order, government request) or to establish/exercise legal rights. We will notify you of such requests unless prohibited by law.

---

6. Data Retention and Deletion

6.1 How Long We Keep Your Data

Data Type	Retention Period
Email, name, authentication data	Duration of account + 30 days after account deletion (unless legally required longer)
Habit activity and progress data	Duration of account + 30 days after account deletion; you may delete individual habit entries anytime
Device/technical data (logs, crash reports)	30-90 days; older logs are automatically purged
Newsletter signup records	Until you unsubscribe

6.2 Account Deletion

You can delete your account anytime via app settings or by emailing patrikgrohmann@gmail.com

Upon deletion:

- Your email, name, and authentication data are marked for deletion within 30 days
- Your habit data is deleted or anonymized within 30 days

- We retain aggregated, anonymized statistics (which cannot identify you)

We do not retain backups beyond 30 days post-deletion.

---

7. Push Notifications and In-App Messaging

7.1 Functional Notifications

We send **functional, non-promotional notifications** only:

- Habit reminders (based on habits you set)
- Account security alerts (login attempts, password changes)
- App updates or critical service notices

These are sent based on your preferences and account data alone; we do not profile or target based on external data.

7.2 Notification Preferences

You can manage notification settings in-app:

- Enable/disable reminders
- Adjust reminder times and frequency
- Disable all notifications (except critical security alerts)

---

8. Cookies and Tracking Technologies (Web Version)

8.1 Current Practice

Our web app currently uses **minimal tracking**:

- **Session cookies** (strictly necessary for login and security)
- **Local storage** for user preferences (stored only on your device, not transmitted to servers)
- **No third-party cookies**
- **No tracking pixels** or analytics scripts

---

9. International Data Transfers

9.1 UK-EU Adequacy

- Your data is stored exclusively in the EU (Stockholm)
- The UK and EU have mutual **data protection adequacy decisions** in place (as of December 2025), allowing unrestricted personal data flows between them
- **No Standard Contractual Clauses (SCCs) or additional safeguards are required** for UK-EU transfers

9.2 Google/Firebase

Google processes some Firebase data outside the EU (including in the US). Google relies on:

- **Data Processing Addendum (DPA)** with UK GDPR-compliant safeguards
- **Standard Contractual Clauses (SCCs)** for US data transfers

You can review Google's safeguards at Google Cloud Data Processing.

9.3 US Users

If you are a resident of the United States (including California):

- We process your data under UK GDPR and EU GDPR principles, which provide strong privacy protection.
- **CCPA/CPRA:** We currently fall below the thresholds for California Consumer Privacy Act (CPRA) applicability (revenue <$25M, <100K users, <50% revenue from data sales). However, we voluntarily comply with key CPRA principles:
    - You have the right to access, delete, and correct your personal data
    - We do not sell your data
    - We do not share your data for targeted advertising
- **State Privacy Laws:** Similar principles apply to users in other US states (Virginia, Colorado, Connecticut, Utah, etc.)
- **How to Exercise US Rights:** Email patrikgrohmann@gmail.com with "US Privacy Request" in the subject line

---

10. Your Data Protection Rights

Under UK GDPR and EU GDPR, you have the following rights (subject to legal limitations):

10.1 Right of Access (Data Subject Access Request)

You have the right to request a copy of all personal data we hold about you, in a structured, commonly used, and machine-readable format (e.g., CSV).

- **How to request:** Email patrikgrohmann@gmail.com with subject "Data Access Request"
- **Response time:** Within 30 calendar days (or up to 90 days for complex requests with advance notice)

10.2 Right of Rectification (Correction)

You can correct inaccurate personal data. For example:

- Update your name or email in app settings
- Request we correct information if you believe it's wrong
- **How to request:** Email patrikgrohmann@gmail.com with subject "Data Correction Request"

10.3 Right of Erasure (Right to be Forgotten)

You can request deletion of your personal data in certain circumstances:

- **Always available:** If you delete your account via app settings
- **May be limited:** If we have a legal obligation to retain data (e.g., tax records, audit trails) or ongoing legitimate interests

How to request: Email patrikgrohmann@gmail.com with subject "Erasure Request" or delete your account in-app.

We will delete your data within 30 days unless a lawful basis requires retention.

10.4 Right to Restriction of Processing

You can request that we limit how we use your data (e.g., store but don't process it) while you dispute its accuracy or we assess your objection.

- **How to request:** Email patrikgrohmann@gmail.com with subject "Restriction Request"

10.5 Right to Data Portability

You have the right to receive your personal data in a structured, commonly used, machine-readable format and to transmit it to another service.

- **How to request:** Email patrikgrohmann@gmail.com with subject "Portability Request"
- **Response time:** Within 30 days, we'll provide a CSV file of your habit data and account information

10.6 Right to Object

You can object to processing for legitimate interests or marketing. For example:

- **Object to marketing emails:** Click "Unsubscribe" in any newsletter email or email patrikgrohmann@gmail.com
- **Object to other processing:** Email patrikgrohmann@gmail.com with specific reasons

10.7 Right to Withdraw Consent

For processing where we rely on your consent (e.g., newsletter signup), you can withdraw consent at any time without penalty.

- **How to withdraw:** Unsubscribe in app settings, click unsubscribe in email, or email patrikgrohmann@gmail.com
- **Effect:** We will stop processing for the withdrawn purpose; past processing is lawful

10.8 How to Exercise Your Rights

- **Email:** patrikgrohmann@gmail.com
- **In-App:** Use in-app "Privacy and Data" settings (for account deletion, notification preferences, etc.)
- **Response:** We will acknowledge your request within 5 business days and resolve within 30 days (or notify you if this is complex)

Verification: We may ask you to verify your identity (e.g., via email confirmation) to prevent unauthorized access to your data.

---

11. Automated Decision-Making and Profiling

We do **not** use automated decision-making or profiling that has legal or similarly significant effects on you.

For example, we do not:

- Automatically exclude users based on algorithms
- Use predictive models to deny service or assess credit
- Profile your behavior for automated eligibility decisions

However, we may use aggregated analytics to identify general trends (e.g., "morning reminders are most effective"), but this does not impact on your individual rights or access.

---

12. Links to Other Websites and Services

Our Service may contain links to third-party websites (e.g., Google Sign-In, Apple Sign-In, AWS documentation).

We are **not responsible** for the privacy practices of third-party websites. Please review their privacy policies before using their services. This privacy policy applies only to data processed by KeepYourHabits.

---

13. Data Breaches and Incident Response

In the unlikely event of a data breach:

1. **Detection:** We monitor systems for unauthorized access
2. **Investigation:** We investigate the scope and impact
3. **Notification:** If your data is compromised, we will notify you via email within 72 hours (or as required by law), along with details of the breach, affected data, and recommended actions
4. **Authority Reporting:** We will notify the UK ICO and relevant EU data protection authorities if required by law

You can report suspected breaches to patrikgrohmann@gmail.com

---

14. Data Protection Officers and Legal Representatives

Currently, we are a small startup and have not appointed a Data Protection Officer. However, you may direct privacy inquiries to patrikgrohmann@gmail.com.

---

15. Supervisory Authorities and Complaints

You have the right to lodge a complaint with a data protection authority (DPA) if you believe we have violated your rights.

UK

Information Commissioner's Office (ICO)

- **Website:** https://ico.org.uk
- **Address:** Water Lane, Wigan, WN3 5DF, UK

- **Email:** casework@ico.org.uk
- **Phone:** +44 (0)303 123 1113

EU Member States

If you are in an EU country you have the right to complain to your **local DPA**.

You can file complaints with either your local DPA or the ICO, and with multiple authorities if your data is processed in multiple jurisdictions.

---

16. Changes to This Privacy Policy

We may update this privacy policy to reflect:

- Changes in our data practices
- New laws or regulations
- Technical improvements
- User feedback

How we notify you:

- For material changes (e.g., new data sharing), we will notify you via email and/or in-app notification at least 30 days before the change takes effect
- For minor updates (e.g., contact info, links), we will update this page with a new "Last Updated" date

Your rights: If you disagree with changes, you can delete your account before the changes take effect.

---

17. Contact Us

For any questions, requests, or concerns about this privacy policy or your data:

KeepYourHabits Privacy Team

- **Email:** patrikgrohmann@gmail.com
- **Response Time:** We will respond to inquiries within 5 business days; requests for data access will be processed within 30 days

---

18. Summary of Key Points

✓ We collect minimal data: email, name (optional), and habit activity only
✓ We store all data in EU (Stockholm); no transfers outside EU/UK

✓ We use only necessary processors (AWS, Google Sign-In, Firebase)
✓ We do not sell your data
✓ We do not use profiling or automated decisions
✓ You have full rights to access, correct, delete, and port your data
✓ We are transparent about our practices and committed to compliance

---

Version: 1.0 (MVP Launch)
Effective Date: 1 February 2026
Review Date: 1 July 2026
