XELER

Privacy Policy

Last updated: October 13, 2026

IN SHORT

- Your data is encrypted at rest with AES-256-GCM. The database and files are stored in the EU (Frankfurt).
- We never sell your data or share it with third parties without your consent.
- You can access and export your data at any time, and ask for it to be deleted.
- Issued invoices and signed proposals are kept for 7 years only because Dutch tax law requires it.

1. Introduction

Xeler respects your privacy and is committed to protecting your personal data. This privacy policy explains how we collect, use, and protect your data when you use our tools and services.

2. Data We Collect

2.1 Automatically Collected Data

- Email address (for account access)
- Usage data (which tools you use and when)
- Device information
- IP address and location data

2.2 Data You Provide

- Business and personal expenses
- Lead information and contact details
- Income goals and financial data
- Subscription and service information

2.3 Proposal Signing Data

When you sign or decline a proposal, we collect the following data to execute the agreement and maintain a legally required audit trail (GDPR Art. 6(1)(b), contract performance):

- Full legal name and email address
- Signature image (drawn or typed)
- IP address and browser information
- Consent acknowledgment text
- Timestamp of signing

> All signing data is encrypted at rest using AES-256-GCM encryption. The data controller for proposal signing is the business that sent you the proposal.

3. How We Use Your Data

- To provide and improve our tools and services
- To process payments and manage your account
- To calculate rates and provide financial insights
- To track leads and manage your business data
- To comply with legal obligations

4. Data Storage and Security

All your data is encrypted and stored securely. We use industry-standard encryption methods to protect your information. Your financial data and business information are never shared with third parties without your explicit consent.

5. Data Retention

We keep your data for the following periods. After that it is deleted, or, for records the law makes us keep, the personal details on it are removed:

- Issued invoices, signed or accepted proposals and their signing record: 7 years from the invoice or signing date, unchanged (required by Dutch tax law, AWR Art. 52)
- Rejected and other unsigned proposals: kept while your account exists; their personal details are removed 30 days after you delete your account
- Proposal view records: kept as long as the proposal they belong to
- Draft proposals: deleted when you delete them; when you delete your account, their personal details are removed after 30 days
- Account data: deleted 30 days after you delete your account, except where retention is legally required
- Activity log (who changed what, for security and accountability): kept as an append-only record. New entries store a pseudonymous code instead of your email address; entries written before October 2026 still contain it.

6. Sub-processors and Data Transfers

We use the following third-party sub-processors to deliver our services:

- Neon, PostgreSQL database hosting (EU region). Processes and stores all application data.
- Resend, Transactional email delivery. Processes email addresses for verification codes and notifications.
- Vercel, Application hosting and edge network. Processes requests and serves the application.

We also use Stripe (payment processing) and Upstash (rate-limit and session caching), and, only when you connect it, Google Workspace APIs (Slides/Drive export for strategy presentations). The complete, always-current list with locations and DPA links is published on our Subprocessors page. All sub-processors are bound by GDPR-compliant Data Processing Agreements (DPAs). Where data is transferred outside the EU/EEA, Standard Contractual Clauses (SCCs) are in place to ensure adequate protection.

7. Your Rights

You have the right to:

- Access your personal data
- Correct inaccurate data

- Request deletion of your data (note: issued invoices, signed proposals and their audit trail are kept for 7 years as required by Dutch tax law, AWR Art. 52)
- Export your data: download it yourself at any time under Profile > Your data
- Object to processing of your data

8. Children

Xeler is a service for work and business and is not directed at children. An account is for people aged 18 or older; people invited by a Xeler customer, such as team members and client contacts, must be at least 16. We do not knowingly collect personal data of children under 16. We do not ask for your date of birth, so that we collect no more data than we need.

If you believe that personal data of a child under 16 has been entered into Xeler, please contact us at support@rawww.online

and we will delete it without undue delay.

9. Contact

If you have questions about this privacy policy or wish to exercise your rights, please contact us at support@rawww.online

10. Google API Data, TimeSync

> Xeler TimeSync is a desktop application that syncs Google Calendar events to Moneybird time entries. This section describes how TimeSync uses Google API data, in compliance with the Google API Services User Data Policy.

10.1 Data We Access

- Calendar events (titles, start/end times, descriptions), via the calendar.readonly scope
- Your email address, via the userinfo.email scope, used to identify your account

10.2 How We Use This Data

- Calendar events are matched against user-defined mapping rules to create time entries in Moneybird
- Your email address is used to link your Google account within the app
- Data is only used for the purpose of syncing time entries, never for advertising, analytics, or any other purpose

10.3 Data Storage

Calendar event data is stored locally on your device in an encrypted SQLite database (AES-256-GCM via SQLCipher). OAuth tokens are encrypted at rest and stored in your operating system's secure keychain where available. The email addresses linked to your Google accounts are sent to our license server only for seat-count verification of your subscription. No calendar event content ever leaves your device except when you choose to sync it to your own Moneybird account.

10.4 Revoking Access

You can disconnect your Google account at any time from the Connections tab in TimeSync. You can also revoke access from your Google Account settings at myaccount.google.com/permissions. Upon disconnection, all stored tokens and calendar data are deleted from your device.