

Privacy Policy

Last updated: April 14, 2026

1. Data Controller

The controller of the data collected via the Certyneo platform is Certyneo, whose registered office is located in France (Certyneo, 14 rue Beffroy, 92200 Neuilly-sur-Seine, France — R.C.S. Nanterre 105 648 703). For any question concerning your personal data, you may contact us at privacy@certyneo.com.

2. Data Collected

We collect data you provide directly to us (name, surname, email, hashed password, job title, company, phone number), documents you upload for signature purposes, and technical metadata necessary for the Service to function (IP address, user-agent, timestamp, session identifiers).

3. Processing Purposes

Your data is processed to: (i) provide and operate the electronic signature Service, (ii) ensure the evidentiary value of issued signatures, (iii) bill your subscription, (iv) ensure platform security and prevent fraud, (v) send you Service-related communications, and (vi) comply with our legal and regulatory obligations.

4. Legal Basis

Processing is based on contract performance (Article 6.1.b GDPR), legal obligation (Article 6.1.c), and our legitimate interest in securing our Service (Article 6.1.f). No commercial prospecting is conducted without your prior explicit consent.

5. Recipients

Your data is accessible to our authorized technical and support teams and to our current processors: hosting provider (IONOS, European Union), transactional email service (Resend), and SMS OTP service (Twilio Verify). All processors are contractually bound and provide sufficient security guarantees. An up-to-date list is available upon request at privacy@certyneo.com.

The complete and up-to-date list of our subprocessors, with the purpose and data categories for each, is published on the Subprocessors page.

6. Hosting and Location

Your data is hosted exclusively on servers located within the European Union. No personal data is transferred outside the EU without appropriate safeguards (Standard Contractual Clauses from the European Commission).

7. Retention Period

Your account data is retained as long as you are a Service user. Signed documents and their audit proof are retained for 10 years after signature, in accordance with eIDAS regulation and Civil Code requirements. Technical data (logs) are retained for a maximum of 12 months.

8. Your Rights

In accordance with GDPR, you have the right to access, rectify, erase, restrict, port, and object to the processing of your data. You may exercise these rights from your dashboard or by writing to us at privacy@certyneo.com. You also have the right to lodge a complaint with the CNIL (www.cnil.fr).

To delete your account and your data, follow the steps described on the Account deletion page.

8.bis Data Protection Officer (DPO)

Certyneo relies on an outsourced shared DPO through DPO-Consulting. You may contact them at dpo@certyneo.com for any questions regarding your personal data, and lodge a complaint with the CNIL (3, place de Fontenoy — TSA 80715 — 75334 Paris Cedex 07) if your request remains unanswered. A declaration with the CNIL in the DPO register has been filed as part of our GDPR compliance framework.

9. Security

We implement the following technical and organizational measures to protect your data: TLS 1.3 encryption for all communications (Caddy 2 + Let's Encrypt), script hashing with salt and timing-safe comparison for user passwords, single-use Twilio Verify OTP for advanced signatures, single-use email verification and password reset tokens with short validity (1 hour), rate limiting by plan on sensitive endpoints, timestamped logging of each stage in an envelope's lifecycle (audit log), object storage with versioning enabled for signed documents, restricted data access by administrators. A detailed list of our security practices is available on the /security page.

10. Cookies and other

We use only cookies strictly necessary for the operation of the Service (session management, language preferences, CSRF protection). No third-party analytics or advertising cookies are set without your explicit consent.

10.bis Data received from Google APIs (Limited Use)

When you connect your Google account to Certyneo, Certyneo's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy (<https://developers.google.com/terms/api-services-user-data-policy>), including its Limited Use requirements. In practice: the Google Drive files you designate and the Gmail attachments you import are used solely for the signature feature you asked for. They are never sold, never transferred to third parties for advertising purposes, never used for targeted advertising, and never read by humans — except with your explicit consent, for security purposes, to comply with a legal obligation, or for internal operations strictly necessary on anonymised or aggregated data. Certyneo never requests access to your whole Drive or your Gmail mailbox: the scopes in use only reach the files you designate and the message you have open.

11. Changes

This policy may be updated to reflect changes to our Service or applicable regulations. Any material changes will be notified to you by email. The date of last update is shown at the top of this page.

For any questions regarding your personal data, please contact our Data Protection Officer at privacy@certyneo.com.