Certyneo SASU · 14 rue Beffroy, 92200 Neuilly-sur-Seine
RCS Nanterre 105 648 703 · certyneo.com

Advanced electronic signature (AES): compliance sheet

Signature level, retention of evidence and hosting

Updated on October 12, 2026

Signature level

Advanced electronic signature within the meaning of Article 26 of Regulation (EU) No 910/2014 (eIDAS). It rests on the four requirements below.

1. Uniquely linked to the signatory: a personal key pair is generated in the signatory's browser and a certificate specific to that signature is issued.
2. Signatory identification: a personal signing link sent by e-mail, then a one-time code sent by SMS to the signatory's mobile. Two separate channels.
3. Under the signatory's sole control: the private key cannot be exported and never leaves the signatory's browser.
4. Any later change is detectable: the document content is sealed by a signed SHA-256 digest and an RFC 3161 timestamp.

Evidence provided

Each signed document comes with a certificate of evidence: time-stamped events (opening, code received, signature), IP address, certificate number and document fingerprint.

Retention

Signed documents and audit trails are kept for 10 years, whichever plan is subscribed.

Only data created with a test key (sandbox) is deleted after 30 days.

Hosting and data protection

The application, database and document storage run on our own infrastructure within the European Union (IONOS hosting). TLS 1.3 in transit and AES-256 at rest. A GDPR data processing agreement (DPA) can be signed online from the customer account.

Good to know

Qualified signature (QES) is offered per signature through a partner qualified trust service provider; this sheet covers the advanced level only.

ISO 27001 certification: certification audit under way, certificate not yet obtained.

Questions and supporting documents : security@certyneo.com · certyneo.com/security

Information document, not contractual. It does not constitute legal advice.