

Geavanceerde elektronische handtekening (AES): compliance-fiche

Handtekeningniveau, bewaring van het bewijs en hosting

Bijgewerkt op 12 oktober 2026

Handtekeningniveau

Geavanceerde elektronische handtekening in de zin van artikel 26 van Verordening (EU) nr. 910/2014 (eIDAS). Zij berust op de vier onderstaande eisen.

- 1 Uitsluitend aan de ondertekenaar verbonden: in de browser van de ondertekenaar wordt een persoonlijk sleutelpaar gegenereerd en er wordt een certificaat uitgegeven dat specifiek is voor deze handtekening.
- 2 Identificatie van de ondertekenaar: persoonlijke ondertekeningsslink per e-mail, daarna een eenmalige code per sms op zijn mobiel. Twee afzonderlijke kanalen.
- 3 Onder exclusieve controle van de ondertekenaar: de privésleutel is niet exporteerbaar en verlaat zijn browser nooit.
- 4 Elke latere wijziging is detecteerbaar: de inhoud van het document is verzegeld met een ondertekende SHA-256-vingerafdruk en een RFC 3161-tijdstempel.

Geleverd bewijs

Elk ondertekend document gaat vergezeld van een bewijscertificaat: gebeurtenissen met tijdstempel (openen, ontvangen code, handtekening), IP-adres, certificaatnummer en vingerafdruk van het document.

Bewaring

Ondertekende documenten en auditsporen worden 10 jaar bewaard, ongeacht het gekozen abonnement.

Alleen gegevens die met een testsleutel (sandbox) zijn aangemaakt, worden na 30 dagen verwijderd.

Hosting en gegevensbescherming

De applicatie, de database en de documentopslag draaien op onze eigen infrastructuur binnen de Europese Unie (hoster IONOS). TLS 1.3 tijdens verzending en AES-256 in rust. Een verwerkersovereenkomst (AVG) kan online worden ondertekend vanuit de klantomgeving.

Goed om te weten

De gekwalificeerde handtekening (QES) wordt per handtekening aangeboden via een gekwalificeerde vertrouwensdienstverlener als partner; deze fiche beschrijft alleen het geavanceerde niveau.

ISO 27001-certificering: certificeringsaudit loopt, certificaat nog niet behaald.