

# Avancerad elektronisk signatur (AES): efterlevnadsblad

Signaturnivå, lagring av bevis och hosting

Uppdaterad den 12 oktober 2026

## Signaturnivå

Avancerad elektronisk signatur enligt artikel 26 i förordning (EU) nr 910/2014 (eIDAS). Den bygger på de fyra kraven nedan.

- 1 Unikt kopplad till undertecknaren: ett personligt nyckelpar skapas i undertecknarens webbläsare och ett certifikat som är specifikt för denna signatur utfärdas.
- 2 Identifiering av undertecknaren: personlig signeringslänk via e-post, därefter en engångskod via SMS till undertecknarens mobil. Två skilda kanaler.
- 3 Under undertecknarens exklusiva kontroll: den privata nyckeln kan inte exporteras och lämnar aldrig webbläsaren.
- 4 Varje senare ändring kan upptäckas: dokumentets innehåll är förseglat med ett signerat SHA-256-avtryck och en RFC 3161-tidsstämpel.

## Bevis som lämnas

Varje signerat dokument åtföljs av ett bevisintyg: tidsstämplade händelser (öppnande, mottagen kod, signatur), IP-adress, certifikatnummer och dokumentets avtryck.

## Lagring

**Signerade dokument och revisionsspår sparas i 10 år, oavsett vilket abonnemang som tecknats.**

Endast data som skapats med en testnyckel (sandlåda) raderas efter 30 dagar.

## Hosting och dataskydd

Applikationen, databasen och dokumentlagringen körs på vår egen infrastruktur inom Europeiska unionen (hostingleverantör IONOS). TLS 1.3 vid överföring och AES-256 vid lagring. Ett personuppgiftsbiträdesavtal (DPA) enligt GDPR kan signeras online från kundkontot.

## Bra att veta

Kvalificerad signatur (QES) erbjuds per signatur via en kvalificerad leverantör av förtroendetjänster som partner; detta blad beskriver endast den avancerade nivån.

ISO 27001-certifiering: certifieringsrevision pågår, certifikatet har ännu inte erhållits.