

Avanceret elektronisk signatur (AES): overensstemmelsesblad

Signaturniveau, opbevaring af beviser og hosting

Opdateret den 12. oktober 2026

Signaturniveau

Avanceret elektronisk signatur i henhold til artikel 26 i forordning (EU) nr. 910/2014 (eIDAS). Den bygger på de fire krav nedenfor.

- 1 Entydigt knyttet til underskriveren: der genereres et personligt nøglepar i underskriverens browser, og der udstedes et certifikat, som er specifikt for denne signatur.
- 2 Identifikation af underskriveren: personligt signeringslink sendt pr. e-mail, derefter en engangskode sendt pr. sms til underskriverens mobil. To adskilte kanaler.
- 3 Under underskriverens enekontrol: den private nøgle kan ikke eksporteres og forlader aldrig underskriverens browser.
- 4 Enhver senere ændring kan opdages: dokumentets indhold er forseglet med et signeret SHA-256-fingeraftryk og et RFC 3161-tidsstempel.

Leverede beviser

Hvert underskrevet dokument ledsages af et bevisbevis: tidsstemplede hændelser (åbning, modtaget kode, signatur), IP-adresse, certifikatnummer og dokumentets fingeraftryk.

Opbevaring

Underskrevne dokumenter og revisionsspor opbevares i 10 år, uanset hvilket abonnement der er tegnet.

Kun data oprettet med en testnøgle (sandkasse) slettes efter 30 dage.

Hosting og databeskyttelse

Applikationen, databasen og dokumentlageret kører på vores egen infrastruktur i Den Europæiske Union (hostingudbyder IONOS). TLS 1.3 under transmission og AES-256 i hvile. En databehandleraftale (DPA) efter GDPR kan underskrives online fra kundekontoen.

Godt at vide

Kvalificeret signatur (QES) tilbydes pr. signatur via en kvalificeret tillidstjenesteudbyder som partner; dette blad beskriver kun det avancerede niveau.

ISO 27001-certificering: certificeringsaudit i gang, certifikat endnu ikke opnået.