

Avansert elektronisk signatur (AES): samsvarsark

Signaturnivå, lagring av bevis og hosting

Oppdatert 12. oktober 2026

Signaturnivå

Avansert elektronisk signatur i henhold til artikkel 26 i forordning (EU) nr. 910/2014 (eIDAS). Den bygger på de fire kravene nedenfor.

- 1 Entydig knyttet til undertegneren: det genereres et personlig nøkkelpar i undertegnerens nettleser, og det utstedes et sertifikat som er spesifikt for denne signaturen.
- 2 Identifisering av undertegneren: personlig signeringslenke sendt på e-post, deretter en engangskode sendt på SMS til undertegnerens mobil. To adskilte kanaler.
- 3 Under undertegnerens eneste kontroll: den private nøkkelen kan ikke eksporteres og forlater aldri undertegnerens nettleser.
- 4 Enhver senere endring kan oppdages: dokumentets innhold er forseglet med et signert SHA-256-fingeravtrykk og et RFC 3161-tidsstempel.

Bevis som leveres

Hvert signerte dokument følges av et bevissertifikat: tidsstemplede hendelser (åpning, mottatt kode, signatur), IP-adresse, sertifikatnummer og dokumentets fingeravtrykk.

Lagring

Signerte dokumenter og revisjonsspor lagres i 10 år, uavhengig av hvilket abonnement som er tegnet.

Bare data opprettet med en testnøkkel (sandkasse) slettes etter 30 dager.

Hosting og personvern

Applikasjonen, databasen og dokumentlagringen kjører på vår egen infrastruktur i Den europeiske union (hostingleverandør IONOS). TLS 1.3 under overføring og AES-256 i hvile. En databehandleravtale (DPA) etter GDPR kan signeres på nett fra kundekontoen.

Greit å vite

Kvalifisert signatur (QES) tilbys per signatur via en kvalifisert tillitstjenesteleverandør som partner; dette arket beskriver bare det avanserte nivået.

ISO 27001-sertifisering: sertifiseringsrevisjon pågår, sertifikat ikke oppnådd ennå.