



NORSK LOVTIDEND

Avd. I Lover og sentrale forskrifter mv.

Utgitt i henhold til lov 19. juni 1969 nr. 53.

Kunngjort 27. november 2019 kl. 15.30

PDF-versjon 4. desember 2019

21.11.2019 nr. 1578

Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften)

Hjemmel: Fastsatt av Kommunal- og moderniseringsdepartementet 21. november 2019 med hjemmel i lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester) § 2.

Del I – formål og definisjoner

§ 1. Formål og virkeområde

Formålet med forskriften er å definere sikkerhetsnivåer og tilsynsregime for elektroniske identifikasjonsordninger (eID-ordninger) og dermed øke tilliten til og bruken av elektroniske identifikasjonstjenester i Norge.

Forskriften skal også legge til rette for grenseoverskridende bruk av elektronisk identifikasjon, ved at selvdeklarte eID-ordninger kan meldes til EU-kommisjonen og deretter omfattes av anerkjennelsesplikten i eIDAS-forordningen artikkel 6.

Forskriften etablerer en selvdeklarasjonsordning hvor tilbydere av eID-ordninger ved selvdeklarasjon kan melde fra til et oppnevnt tilsynsorgan om at forskriftens krav er oppfylt.

Forskriften gjelder for tilbydere som er etablert i Norge.

§ 2. Definisjoner

- a. *eIDAS-forordningen*: forordning om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner i det indre markedet (forordning (EU) nr. 910/2014)
- b. *identifikasjonsnivåforskriften*: Kommisjonens gjennomføringsforordning (EU) 2015/1502 av 8. september 2015 til eIDAS-forordningen, jf. forskrift 21. november 2019 nr. 1577 om tillitstjenester for elektroniske transaksjoner § 6
- c. *eID*: elektronisk identitetsbevis, tilsvarer elektronisk identifikasjonsmiddel i eIDAS-forordningen
- d. *eID-ordninger*: ordninger for elektronisk identifikasjon.

Med mindre annet fremgår av sammenhengen gjelder eIDAS-forordningens definisjoner i artikkel 3.

Del II – selvdeklarasjon av eID-ordninger

Krav til selvdeklarererte eID-ordninger

§ 3. *Selvdeklarasjon – eID nivå høyt*

Tilbyder av eID-ordning skal oppfylle alle krav som er beskrevet for nivå høyt i denne forskriftens del III.

§ 4. *Selvdeklarasjon – eID nivå betydelig*

Tilbyder av eID-ordning skal oppfylle alle krav som er beskrevet for nivå betydelig i denne forskriftens del III.

§ 5. *Selvdeklarasjon – eID nivå lavt*

Tilbyder av eID-ordning skal oppfylle alle krav som er beskrevet for nivå lavt i denne forskriftens del III.

Melding om frivillig selvdeklarasjon mv.

§ 6. *Tilsyn*

Tilsynsorgan etter denne forskriften skal være Nasjonal kommunikasjonsmyndighet.

§ 7. *Krav til meldingens innhold*

Selvdeklarasjon etter denne forskriften skal sendes tilsynsorganet og inneholde beskrivelse av hvordan kravene etter § 3, § 4 eller § 5 er oppfylt.

Tilsynsorganet skal utarbeide standardskjema som skal benyttes ved melding etter første ledd.

§ 8. *Meldeplikt om endringer i opplysninger gitt etter § 7*

Endrede forhold som påvirker opplysninger gitt etter § 7 skal uten ugrunnet opphold meldes til tilsynsorganet.

Tilsynsorganets oppgaver mv.

§ 9. *Tilsynets kontrolloppgaver*

Tilsynsorganet skal kontrollere at mottatt melding etter § 7 er fullstendig og at kravene etter § 3, § 4 eller § 5 er oppfylt.

Når særlige grunner tilsier det kan tilsynsorganet gjøre unntak fra bestemmelsene i denne forskrift.

§ 10. *Krav om tilleggsinformasjon og revisjon*

Dersom tilsynsorganet finner at tilbyder av eID-ordning ikke oppfyller kravene etter § 3, § 4 eller § 5, eller at meldingen etter § 7 ikke er fullstendig, kan tilsynsorganet pålegge tilbyder av eID-ordning innen en angitt tidsfrist å dokumentere at kravene er oppfylt eller å komplettere meldingen. Dette kan skje ved fremleggelse av dokumentasjon eller på annen måte som tilsynsorganet finner hensiktsmessig.

Tilsynsorganet kan også kreve at tilbyder av eID-ordning foretar en revisjon for å vise at kravene i § 3, § 4 eller § 5 er oppfylt. Revisjonen skal foretas av en uavhengig tredjepart godtatt av tilsynsorganet og resultatet av revisjonen skal sendes tilsynsorganet.

Tilbyder av eID-ordning kan pålegges å betale for revisjonen.

§ 11. Tilsynsorganets kompetanse

Tilsynsorganet for selvdeklarasjonsordningen har kompetanse til å avgjøre om kravene i denne forskriftens del III er oppfylt. Tilsynsorganet skal vurdere alle relevante forhold, både eventuelle sikkerhetsbrudd og andre erfaringer med aktuelle løsninger.

§ 12. Tilsynsorganets dispensasjonsadgang

Tilsynet kan dispensere fra kravene i denne forskriftens del III, dersom en risikovurdering viser at avviket fra kravet etter tilsynets mening må anses kompensert av andre risikoreduserende tiltak, slik at løsningen samlet sett likevel tilfredsstiller det aktuelle sikkerhetsnivået.

§ 13. Offentliggjøring av informasjon om tilbyder av eID-ordning mv.

Tilsynsorganet skal publisere en liste over selvdeklarte eID-ordninger med opplysninger om hvilke eID-nivåer som tilbydere av eID-ordninger har selvdeklart etter denne forskriften, sammen med mottatt melding etter § 7.

Tilsynsorganet kan nekte publisering etter første ledd dersom mottatt melding ikke oppfyller kravene i § 7, eller at det er åpenbart for tilsynsorganet at kravene etter § 3, § 4 eller § 5 ikke er oppfylt.

Tilsynsorganet skal fjerne aktuelt eID-nivå fra publisert liste etter første ledd dersom tilbyder av eID-ordning ikke etterkommer kravene i § 8 eller tilsynsorganets pålegg etter § 10.

Øvrige bestemmelser

§ 14. Tvangsmulkt

Tilsynsorganet kan ilegge tilbyder av eID-ordning tvangsmulkt etter lov om elektroniske tillitstjenester § 4. Tvangsmulkt kan også ilegges næringsdrivende som i salgs- og markedsføringsøyemed uriktig angir at de tilbyr en ordning som er oppført på liste publisert etter § 13 første ledd.

§ 15. Sektoravgift

Tilbyder av eID-ordning som sender inn melding etter § 7 kan pålegges å betale årlig sektoravgift til tilsynsorganet etter lov om elektroniske tillitstjenester § 7 og forskrift 20. mars 2017 nr. 386 om sektoravgift og gebyr til Nasjonal kommunikasjonsmyndighet § 7.

Tilsynsorganet kan nekte oppføring på liste publisert etter § 13 første ledd før sektoravgiften er betalt.

§ 16. Klageinstans

Kommunal- og moderniseringsdepartementet er klageinstans for tilsynsorganets enkeltvedtak fastsatt i henhold til § 9 til § 14.

Klage på fastsatt sektoravgift avgjøres av Kommunal- og moderniseringsdepartementet etter forskrift 20. mars 2017 nr. 386 om sektoravgift og gebyr til Nasjonal kommunikasjonsmyndighet.

Del III – Sikkerhetsnivåer for ordninger for elektronisk identifikasjon for fysiske personer

§ 17. Gjenbruk av kravsettet i identifikasjonsnivåforskriften (Kommisjonens gjennomføringsforordning (EU) 2015/1502)

Alle kravene i identifikasjonsnivåforskriften gjelder med de tilpasninger som fremgår nedenfor.

Henvisninger i identifikasjonsnivåforskriften pkt. 2.1.2 til bekreftelser fra et samsvarsvurderingsorgan tilfredsstilles også av selvdeklarte løsninger etter denne forskrift.

§ 18. Identifikasjonen skal gi entydig kobling til Folkeregistrert person

Identitetspåstanden må gjelde en person som finnes i Folkeregisteret. eID-tilbyderen må kunne gi en sikker og entydig kobling til denne personens identifikator i Folkeregisteret (fødsels- eller d-nummer). Det at koblingen er sikker og entydig innebærer at koblingen ikke kan baseres på personens navn eller andre kjennetegn som kan være i bruk av flere personer.

§ 19. Tilpasninger for nivå høyt

For identifikasjonsnivåforskriften pkt. 2.1.2 høyt nr. 1 bokstav a gjelder følgende tilpasning:

- Som gyldig identitetsbevis regnes pass eller nasjonalt identitetskort. For utenlandsk identitetsbevis må entydig knytning til norsk identitetsnummer godtgjøres.
- Kravet er også oppfylt for eID på nivå 4 iht. rammeverket fra 2008 for autentisering og uavviselighet.

For identifikasjonsnivåforskriften 2.3.1 høyt nr. 2 gjelder følgende presisering:

- Kravet er ikke til hinder for at identitetsinformasjon, f.eks. fødselsnummer, gjøres tilgjengelig på annen måte, eksempelvis i oppslagstjeneste eller at det lagres i sertifikatet for PKI-baserte eID-er. Kravet i 2.3.1 nr. 2 høyt gjelder utlevering av identitetsinformasjon ved autentisering.

§ 20. Tilpasninger for nivå betydelig

For identifikasjonsnivåforskriften pkt. 2.1.2 nivå betydelig nr. 1 gjelder følgende tilpasning:

- Kravet til å besitte et bevis kan oppfylles ved at personen godtgjør at han/hun har tilgang til en adresse (postal eller elektronisk) som er registrert på personen i det norske Folkeregisteret eller annet register som gir tilstrekkelig sikkerhet, eksempelvis kontaktregisteret. I tillegg må det finnes tiltak for å sikre at riktig person tar eID-en i bruk, typisk varsling til annen eller samme adresse.

For identifikasjonsnivåforskriften pkt. 2.4.6. nivå betydelig gjelder følgende tilpasning:

- Kravet kan eksempelvis oppnås ved bruk av sikrede maskinvaremoduler (HSM) eller kombinasjoner av tilgangsstyring, logging, overvåking og tjenstedeling. Kravet tar sikte på å hindre at autoriserte personer alene og uoppdaget kan kompromittere prosessene.

§ 21. Tilpasninger for nivå lavt

For identifikasjonsnivåforskriften pkt. 2.1.2 skal også kravene for nivå betydelig tilfredsstilles, jf. § 20 første ledd.

For identifikasjonsnivåforskriften 2.4.7 gjelder følgende presisering:

- Kravet kan eksempelvis oppfylles ved revisjon iht. ISO 17065, som bl.a. dekker tillitstjenester, med relevante tilleggskrav i ETSI 319403.

Del IV – ikraftttredelse

§ 22. *Ikraftttredelse og overgangsordning*

Forskriften trer i kraft straks.

Seks måneder etter denne forskriftens ikraftttredelse oppheves forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere.