Nasjonal kommunikasjons-myndighet

Postboks 93
4791 Lillesand
www.nkom.no

Telefon: 22 82 46 00
Telefaks: 22 82 46 40
E-post: firmapost@nkom.no

# Meldingsskjema for selvdeklarasjon av ordning for elektronisk identifikasjon – sikkerhetsnivå «betydelig»

## Melding om selvdeklarasjon

***Melding om selvdeklarasjon av ordning for elektronisk identifikasjon, jf. forskrift av 21. november 2019 nr. 1578 om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften) § 7***
*Tilbydere av eID-ordninger kan etter selvdeklarasjonsforskriften sende inn skjema for melding om selvdeklarasjon av sine ordninger for elektronisk identifikasjon til Nasjonal kommunikasjonsmyndighet (Nkom). Selvdeklarerte eID-ordninger underlegges da det norske tilsynsregimet i henhold til selvdeklarasjonsforskriften. Tilbydere erklærer ved meldingen at forskriftens krav er oppfylt for deklarert(e) sikkerhetsnivå(er). Selvdeklarasjon er en nødvendig forutsetning for eventuell senere norsk innmelding av ordningene til EU-kommisjonen.*

***Meldeplikt om endringer i opplysninger angitt i melding om selvdeklarasjon av ordning for elektronisk identifikasjon, jf. selvdeklarasjonsforskriften § 8***
*Endrede forhold som påvirker opplysninger gitt ved melding om selvdeklarasjon etter selvdeklarasjonsforskriften § 7 skal uten ugrunnet opphold meldes til Nkom.*

***Offentliggjøring av informasjon om tilbydere av ordning for elektronisk identifikasjon, jf. selvdeklarasjonsforskriften § 13***
*Nkom skal på sin hjemmeside publisere en liste over selvdeklarerte ordninger for elektronisk identifikasjon med opplysninger om hvilke eID-nivåer som tilbydere av eID-ordninger har selvdeklarert etter selvdeklarasjonsforskriften, sammen med mottatt melding etter selvdeklarasjonsforskriften § 7.*
*Forretningsmessige opplysninger av sensitiv art eller taushetsbelagte opplysninger må derfor oppgis i vedlegg der det spesifiseres hvilket krav det er relatert til.*

*Utfylt skjema sendes til: firmapost@nkom.no*

## Opplysninger om tilbyder

| | |
|---|---|
| Organisasjonsnavn | |
| Organisasjonsnummer | |
| Postadresse | |
| Besøksadresse | |
| Telefon | |
| Nettside med informasjon om eID-ordningen | |

| Gjeldende erstatningsansvar | |
|---|---|
| Beskriv erstatningsansvaret for tilbyder | |

| Gjeldende forvaltningsordning | |
|---|---|
| Beskriv hvordan avvik og sikkerhetsbrudd vil kunne påvirke løsningen – eksempelvis om hele eller deler av ordningen tas ned | |

**Generell informasjon**

***Krav for sikkerhetsnivå «betydelig»***
*Den meldte ordningen for selvdeklarasjon skal oppfylle alle kravene for det relevante sikkerhetsnivå i selvdeklarasjonsforskriften del III, som definerer norske sikkerhetsnivåer for elektroniske identifikasjonsordninger. Kravene bygger på de europeiske sikkerhetsnivåene, slik de er definert i identifikasjonsnivåforskriften (Kommisjonens gjennomføringsforordning 2015/1502). Alle kravene for sikkerhetsnivåer i identifikasjonsnivåforskriften gjelder med de norske tilpasninger og presiseringer som fremgår av selvdeklarasjonsforskriften §§ 18-21.*

*Kravene nedenfor gjelder sikkerhetsnivå «betydelig» og er strukturert i tråd med identifikasjonsnivåforskriftens oppbygning. Norske tilpasninger for sikkerhetsnivå «betydelig» er lagt inn på de relevante punktene i identifikasjonsnivåforskriften, pkt. 2.1.2 og 2.4.6.*

*For noen av elementene er kravene like på alle sikkerhetsnivåer, og for noen er kravene kumulative, dvs. at for høyere sikkerhetsnivåer må alle eller noen av kravene på lavere sikkerhetsnivåer også være oppfylt. Kumulative krav finnes i punktene 2.1.2, 2.3.1, 2.4.3, 2.4.6. Skjemaet skal ta høyde for denne leserutfordringen, inkludert de norske tilpasninger for kravene for sikkerhetsnivå «betydelig» i pkt. 2.1.2 og 2.4.6, jf. selvdeklarasjonsforskriften § 20. Når krav fra lavere sikkerhetsnivå er gjengitt, fremgår det av nummereringen (L.1 = krav nr. 1 for sikkerhetsnivå «lavt»).*

*Skjemaet tar imidlertid ikke høyde for at oppfyllelse av sikkerhetskrav på ett nivå alternativt kan oppfylles ved å oppfylle kravet på et høyere sikkerhetsnivå (inkl. norske tilpasninger), jf. identifikasjonsnivåforskriften artikkel 1 nr. 3. Dersom tilbyderen påberoper seg dette alternativet, ber vi om at det tydelig angis i beskrivelseskolonnen.*

***Beskrivelse av krav***
*Det skal beskrives hvordan kravene for følgende elementer er oppfylt med sikte på å nå sikkerhetsnivå "betydelig" for elektroniske identifikasjonsmiddelet innenfor rammen av eID-ordningen som er selvdeklarert. Det skal angis hvilket alternativ av kravet som er oppfylt dersom kravet har flere alternativer.*

| **2.1. Registrering** | | |
|---|---|---|
| 2.1.1. Søknad og registrering | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Det sikres at søkeren er kjent med vilkårene for bruk av elektroniske identifikasjonsmidler. | | |
| 2. Det sikres at søkeren er kjent med anbefalte sikkerhetstiltak knyttet til elektroniske identifikasjonsmidler. | | |
| 3. Relevante identitetsdata som kreves ved bekreftelse og kontroll av identitet, samles inn. | | |
| 2.1.2. Bekreftelse og kontroll av identitet (fysisk person) | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| L.1. Personen kan antas å være i besittelse av et bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, og som representerer den påberopte identiteten. | | |
| L.2. Beviset kan antas å være ekte eller eksistere i henhold til en autoritativ kilde, og framstår som gyldig. | | |
| L.3. Den påberopte identiteten eksisterer i henhold til en autoritativ kilde, og det kan antas at vedkommende er den personen som påberoper seg identiteten. | | |
| **Ett av alternativene i nr. 1 til 4 skal være oppfylt.**<br>**Angi tydelig hvilket alternativ som er oppfylt:**<br><br>1. Det er kontrollert at personen er i besittelse av et bevis som er godkjent av medlemsstaten der det søkes om det elektroniske identitetsmiddelet, og som representerer den påberopte identiteten,<br><br>og | | |

| | | |
|---|---|---|
| beviset kontrolleres for å fastslå at det er ekte, eller at det i henhold til en autoritativ kilde eksisterer og gjelder en virkelig person,<br><br>og<br><br>det er truffet tiltak for å minimere risikoen for at personens identitet ikke er den påberopte identiteten, for eksempel ved å ta hensyn til risikoen for at beviset er tapt, stjålet, midlertidig opphevet, tilbakekalt eller utløpt,<br><br>***Følgende tilpasning gjelder for kravet i dette punkt (2.1.2 nr. 1), jf. selvdeklarasjonsforskriften § 20 første ledd:***<br><br>- *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.*<br><br>**eller**<br><br>2. det legges fram et identitetsdokument i løpet av en registreringsprosess i medlemsstaten der dokumentet er utstedt, og dokumentet framstår som det tilhører personen som legger det fram,<br><br>og<br><br>det er truffet tiltak for å minimere risikoen for at personens identitet ikke er den påberopte identiteten, for eksempel ved å ta hensyn til risikoen for at dokumentene er tapt, stjålet, midlertidig opphevet, tilbakekalt eller utløpt,<br><br>**eller**<br><br>3. når framgangsmåter som tidligere er benyttet av en offentlig eller privat enhet i samme medlemsstat, men for et annet formål enn utstedelse av elektroniske identifikasjonsmidler, gir en sikkerhet tilsvarende det som er angitt for fysisk person for sikkerhetsnivået «betydelig», behøver den registreringsansvarlige enheten ikke gjenta de tidligere framgangsmåtene, forutsatt at den likeverdige sikkerheten bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i europaparlaments- og rådsforordning (EF) nr. 765/2008 eller av et tilsvarende organ,<br><br>**eller** | | |

| | | |
|---|---|---|
| 4. når det elektroniske identifikasjonsmiddelet er utstedt på grunnlag av et gyldig, meldt elektronisk identifikasjonsmiddel med sikkerhetsnivået «betydelig» eller «høyt», og det samtidig tas hensyn til risikoen for en endring i personidentifikasjonsopplysningene, er det ikke nødvendig å gjenta bekreftelsen og kontrollen av identitet. Når det elektroniske identifikasjonsmiddelet som ligger til grunn, ikke er meldt, skal sikkerhetsnivået «betydelig» eller «høyt» bekreftes av et samsvarsvurderingsorgan som nevnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av et tilsvarende organ.<br><br>***Henvisninger i pkt. 2.1.2 til bekreftelser fra et samsvarsvurderingsorgan tilfredsstilles også av selvdeklarerte ordninger, jf. selvdeklarasjonsforskriften § 17 annet ledd.*** | | |
| **Kobling til folkeregistrert person (selvdeklarasjonsforskriften § 18)** | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | |
| 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.<br><br>Beskriv hvordan koblingen til personens identifikator i folkeregisteret godtgjøres. | | |

| 2.2. Håndtering av elektroniske identifikasjonsmidler | | |
|---|---|---|
| 2.2.1. De elektroniske identifikasjonsmidlenes egenskaper og utforming | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Det elektroniske identifikasjonsmiddelet benytter minst to autentiseringsfaktorer fra ulike kategorier som er definert i pkt. 1 nr. 2 i vedlegget til identifikasjonsnivåforskriften. | | |
| 2. Det elektroniske identifikasjonsmiddelet er utformet slik at det kan antas det bare brukes dersom eieren har kontroll over eller er i besittelse av det. | | |
| 2.2.2. Utstedelse, levering og aktivering | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Etter utstedelse leveres det elektroniske identifikasjonsmiddelet via en mekanisme som gjør at det kan antas at det bare leveres til dets eier. | | |
| 2.2.3. Midlertidig oppheving, tilbakekalling og reaktivering | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Det er mulig å oppheve et elektronisk identifikasjonsmiddel midlertidig og/eller tilbakekalle det til rett tid og på en effektiv måte. | | |
| 2. Det finnes tiltak for å hindre uautorisert midlertidig oppheving, tilbakekalling og/eller reaktivering. | | |
| 3. Reaktivering skal finne sted bare dersom de samme sikkerhetskravene som gjaldt før den midlertidige opphevingen eller tilbakekallingen, fortsatt er oppfylt. | | |
| 2.2.4. Fornyelse og erstatning | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Samtidig som det tas hensyn til risikoen for en endring i personidentifikasjonsopplysningene, skal fornyelse eller erstatning oppfylle de samme sikkerhetskravene som ved opprinnelig bekreftelse og kontroll av identitet, eller være basert på et gyldig elektronisk identifikasjonsmiddel på samme eller høyere sikkerhetsnivå. | | |

| 2.3. Autentisering | | |
|---|---|---|
| 2.3.1. Autentiseringsordning | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| L.1. Personidentifikasjonsopplysninger utleveres etter behørig kontroll av det elektroniske identifikasjonsmiddelet og dets gyldighet. | | |
| L.2. Når personidentifikasjonsopplysninger lagres som en del av autentiseringsordningen, sikres disse opplysningene slik at de beskyttes mot tap og kompromittering, herunder mot analyse uten nettforbindelse. | | |
| L.3. Autentiseringsordningen gjennomfører sikkerhetskontroller av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynlig at det er mulig for en angriper med økt grunnleggende angrepskapasitet å gjette seg til, avlytte, avspille eller manipulere kommunikasjonen og på den måten omgå autentiseringsordningen. | | |
| 1. Personidentifikasjonsopplysninger utleveres etter behørig kontroll av det elektroniske identifikasjonsmiddelet og dets gyldighet ved dynamisk autentisering. | | |
| 2. Autentiseringsordningen gjennomfører sikkerhetskontroller av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynlig at det er mulig for en angriper med moderat angrepskapasitet å gjette seg til, avlytte, avspille eller manipulere kommunikasjonen og på den måten omgå autentiseringsordningen. | | |

| 2.4. Forvaltning og organisering | | |
|---|---|---|
| 2.4.1. Generelle bestemmelser | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Tilbydere av operative tjenester som omfattes av denne forordning, er en offentlig myndighet eller en enhet anerkjent som en juridisk person i en medlemsstats nasjonale rett, som har en etablert organisasjon og er fullt operativ på alle områder som er relevante for leveringen av tjenestene. | | |

| | | |
|---|---|---|
| 2. Tilbyderne oppfyller alle lovfestede krav de er pålagt i forbindelse med drift og levering av tjenesten, blant annet hva slags opplysninger som kan innhentes, hvordan identitet bekreftes samt hvilke opplysninger som kan lagres og hvor lenge. | | |
| 3. Tilbyderne skal dokumentere sin evne til å påta seg risikoen ved erstatningsansvar, og at de har tilstrekkelige økonomiske midler til fortsatt drift og tjenestelevering. | | |
| 4. Det er tilbydernes ansvar at alle forpliktelser som er satt ut til en annen enhet, blir oppfylt, og at retningslinjene for ordningen blir fulgt, som om de selv hadde utført oppgavene. | | |
| 5. Ordninger for elektronisk identifikasjon som ikke er opprettet i henhold til nasjonal rett, skal inneholde en effektiv plan for virksomhetsopphør. En slik plan skal innbefatte en ryddig avvikling av tjenesten, eller videreføring av en annen tilbyder hvordan vedkommende myndigheter og sluttbrukere informeres, samt nærmere opplysninger om hvordan registre skal beskyttes, oppbevares og destrueres i samsvar med retningslinjene for ordningen. | | |
| 2.4.2. Offentliggjorte meldinger og brukerinformasjon | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Det finnes en offentliggjort definisjon av tjenesten, som omfatter alle gjeldende vilkår og gebyrer, herunder eventuelle begrensninger i bruken. Tjenestedefinisjonen skal inneholde et personvernprogram. | | |
| 2. Det skal innføres hensiktsmessige retningslinjer og framgangsmåter for å sikre at brukerne av tjenesten informeres til rett tid og på behørig måte om eventuelle endringer av tjenestedefinisjonen og av gjeldende vilkår og personvernprogram for den aktuelle tjenesten. | | |
| 3. Det skal innføres hensiktsmessige retningslinjer og framgangsmåter som sikrer fullstendige og riktige svar på henvendelser om informasjon. | | |
| 2.4.3. Forvaltning av informasjonssikkerhet | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| L.1. Det finnes et effektivt styringssystem for informasjonssikkerhet, til håndtering og kontroll av risiko knyttet til informasjonssikkerhet. | | |

| | | |
|---|---|---|
| 1. Styringssystemet for informasjonssikkerhet følger dokumenterte standarder eller prinsipper for håndtering og kontroll av sikkerhetsrisiko. | | |
| 2.4.4. Oppbevaring av opplysninger | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Relevante opplysninger registreres og ajourføres ved hjelp av et effektivt registreringssystem, der det tas hensyn til relevant lovgivning og god praksis i forbindelse med vern av personopplysninger og datalagring. | | |
| 2. Opplysninger oppbevares, i den grad det er tillatt i henhold til nasjonal rett eller andre nasjonale administrative ordninger, og beskyttes så lenge det er behov for dem med sikte på revisjon, undersøkelse av sikkerhetsbrudd og oppbevaring, og destrueres deretter på en sikker måte. | | |
| 2.4.5. Lokaler og personale | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Det finnes framgangsmåter for å sikre at personale og underleverandører har tilstrekkelig opplæring, kvalifikasjoner og erfaring til å kunne utføre sine oppgaver. | | |
| 2. Det finnes tilstrekkelig med personale og underleverandører til å drive og vedlikeholde tjenesten i samsvar med de retningslinjene og framgangsmåtene som gjelder for den. | | |
| 3. Lokalene som benyttes til å levere tjenesten, kontrolleres kontinuerlig og beskyttes mot skader forårsaket av miljøhendelser, uautorisert tilgang og andre faktorer som kan påvirke tjenestens sikkerhet. | | |
| 4. Lokalene som benyttes til å levere tjenesten, sikrer at adgangen til områder der personopplysninger og kryptografiske eller andre sensitive opplysninger oppbevares eller behandles, er begrenset til godkjent personale eller godkjente underleverandører. | | |
| 2.4.6. Tekniske kontroller | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |

| | | |
|---|---|---|
| L.1. Det finnes tekniske kontroller som er egnede til å håndtere risikoene knyttet til tjenestenes sikkerhet og sikre de behandlede opplysningenes fortrolighet, integritet og tilgjengelighet. | | |
| L.2. Elektroniske kommunikasjonskanaler som benyttes til å utveksle personopplysninger eller sensitive opplysninger, beskyttes mot avlytting, manipulering og avspilling. | | |
| L.3. Tilgang til sensitivt, kryptografisk materiale begrenses til funksjoner og applikasjoner som absolutt krever tilgang, dersom det benyttes til å utstede elektroniske identifikasjonsmidler og til autentisering. Det skal sikres at et slikt materiale aldri lagres permanent i ren tekst. | | |
| L.4. Det finnes framgangsmåter som garanterer at sikkerheten opprettholdes over tid, og at det kan reageres på endrede risikonivåer, hendelser og sikkerhetsbrudd. | | |
| L.5. Alle medier som inneholder personopplysninger og kryptografiske eller andre sensitive opplysninger, lagres, transporteres og bortskaffes på en trygg og sikker måte. | | |
| 1. Sensitivt kryptografisk materiale beskyttes mot ulovlige inngrep dersom det benyttes til å utstede elektroniske identifikasjonsmidler og til autentisering.<br><br>***Følgende tilpasning gjelder for kravet i dette punkt (2.4.6 nr. 1), jf. selvdeklarasjonsforskriften § 20 annet ledd:***<br><br>- *Kravet kan eksempelvis oppnås ved bruk av sikrede maskinvaremoduler (HSM) eller kombinasjoner av tilgangsstyring, logging, overvåking og tjenestedeling. Kravet tar sikte på å hindre at autoriserte personer alene og uoppdaget kan kompromittere prosessene.* | | |
| 2.4.7. Overholdelse og revisjon | | |
| Kravbeskrivelse | Oppfyller Ja/Nei | Beskrivelse og henvisning til eventuell dokumentasjon |
| 1. Det gjennomføres jevnlig uavhengige interne eller eksterne revisjoner som omfatter alle deler som er relevante for levering av tjenestene, for å sikre samsvar med relevante retningslinjer. | | |

| Underlagsdokumentasjon | |
|---|---|
| Angi alle vedlagte underlagsdokumenter, og hvilket av elementene ovenfor de er knyttet til. Vedlegg en engelsk versjon eller en engelsk oversettelse av dokumentasjon dersom det foreligger. | |

| Merknad |
|---|
| |

| Dato og underskrift | |
|---|---|
| *Undertegnede bekrefter kjennskap til bestemmelser i forskrift om selvdeklarasjonsordningen som gjelder for tilbydere av eID-ordninger, og at opplysninger gitt på dette skjemaet er korrekte. Undertegnede er oppmerksom på at virksomheten kan bli pålagt å betale sektoravgift i henhold til forskrift av 21. november 2019 nr. 1578 om selvdeklarasjon om ordninger for elektronisk identifikasjon § 15 jf. lov av 15. juni 2018 nr. 44 om elektroniske tillitstjenester § 7, og forskrift av 20. mars 2017 nr. 386 om sektoravgift og gebyr til Nasjonal kommunikasjonsmyndighet § 7.* | |
| Sted, Dato | Underskrift (må ha signaturfullmakt) |
| | *Gjenta underskriften her med blokkbokstaver* |

## Vedlegg til skjema

| **Administrativ informasjon til Nkom**<br><br>*Denne informasjon er ikke en del av skjemaet og publiseres ikke på Nkom sin nettside.* | |
|---|---|
| E-post for administrative henvendelser | |
| E-post for tekniske henvendelser | |
| Kontaktperson(er): Navn, e-post, telefon | |
| Ansvarlig(e) person(er) for rapportering av sikkerhetshendelser | |
| Referanse/bestillingsnummer for elektronisk faktura | |