

Meldingsskjema for sjølvdeklarasjon av ordning for elektronisk identifikasjon – tryggleiksnivå «betydeleg»

Melding om sjølvdeklarasjon

Melding om sjølvdeklarasjon av ordning for elektronisk identifikasjon, jf. forskrift av 21. november 2019 nr. 1578 om sjølvdeklarasjon av ordninger for elektronisk identifikasjon (sjølvdeklarasjonsforskrifta) § 7

Tilbydarar av eID-ordningar kan etter sjølvdeklarasjonsforskrifta sende inn skjema for melding om sjølvdeklarasjon av sine ordningar for elektronisk identifikasjon til Nasjonal kommunikasjonsmyndighet (Nkom). Sjølvdeklarerte eID-ordningar blir då underlagde det norske tilsynsregimet i samsvar med sjølvdeklarasjonsforskrifta. Tilbydarar erklærer ved meldinga at forskrifta sine krav er oppfylte for deklarerert(e) tryggleiksnivå(er). Sjølvdeklarasjon er ein nødvendig føresetnad for eventuell seinare norsk innmelding av ordningane til EU-kommisjonen.

Meldeplikt om endringar i opplysningar angitt i melding om sjølvdeklarasjon av ordning for elektronisk identifikasjon, jf. sjølvdeklarasjonsforskrifta § 8
Endra forhold som påverkar opplysningar gitt ved melding om sjølvdeklarasjon etter sjølvdeklarasjonsforskrifta § 7 skal utan ugrunna opphald meldast til Nkom.

Offentleggjering av informasjon om tilbydarar av ordning for elektronisk identifikasjon, jf. sjølvdeklarasjonsforskrifta § 13

Nkom skal på si heimeside publisere ei liste over sjølvdeklarerte ordningar for elektronisk identifikasjon med opplysningar om kva eID-nivå tilbydarar av eID-ordningar har sjølvdeklarert etter sjølvdeklarasjonsforskrifta, saman med motteken melding etter sjølvdeklarasjonsforskrifta § 7. Forretningsmessige opplysningar av sensitiv art eller teiepliktige opplysningar må difor oppgivast i vedlegg der det blir spesifisert kva krav dei er relaterte til.

Utfyllt skjema sendast til: firmapost@nkom.no

Opplysningar om tilbydar

Organisasjonsnamn	
Organisasjonsnummer	
Postadresse	
Besøksadresse	
Telefon	
Nettside med informasjon om eID-ordninga	

Gjeldande erstatningsansvar

Beskriv erstatningsansvaret for tilbydaren

Gjeldande forvaltningsordning

Beskriv korleis avvik og tryggleiksbrot kan påverke løysinga
– til dømes om heile eller delar av ordninga blir tatt ned

Generell informasjon

Krav for tryggleiksnivå «betydeleg»

Den meldte ordninga for sjølvdeklarasjon skal oppfylle alle krava for det relevante tryggleiksnivået i sjølvdeklarasjonsforskrifta del III, som definerer norske tryggleiksnivå for elektroniske identifikasjonsordningar. Krava byggjer på dei europeiske tryggleiksnivåa, slik dei er definerte i [identifikasjonsnivåforskrifta](#) (Kommisjonen si gjennomføringsforordning 2015/1502). Alle krava for tryggleiksnivå i identifikasjonsnivåforskrifta gjeld med dei norske tilpassingar og presiseringer som fremgår av [sjølvdeklarasjonsforskrifta](#) §§ 18-21.

Krava nedanfor gjeld tryggleiksnivå «betydeleg» og er strukturerte i tråd med oppbygginga i identifikasjonsnivåforskrifta. Norske tilpassingar for tryggleiksnivå «betydeleg» er lagt inn på dei relevante punkta i identifikasjonsnivåforskrifta, pkt. 2.1.2 og 2.4.6.

For nokre av elementa er krava like på alle tryggleiksnivå, og for nokre er krava kumulative, dvs. at for høgare tryggleiksnivå må alle eller nokre av krava på lågare tryggleiksnivå òg vere oppfylte. Kumulative krav finst i punkta 2.1.2, 2.3.1, 2.4.3, 2.4.6. Skjemaet skal ta høgd for denne lesarutfordringa, inkludert dei norske tilpassingar for krava for tryggleiksnivå «betydeleg» i pkt. 2.1.2 og 2.4.6, jf. sjølvdeklarasjonsforskrifta § 20. Når krav frå lågare tryggleiksnivå er gjengitt, går det fram av nummereringa (L.1 = krav nr. 1 for tryggleiksnivå «lågt»).

Skjemaet tek likevel ikkje høgd for at oppfylting av tryggleikskrav på eitt nivå alternativt kan oppfyllest ved å oppfylle kravet på eit høgare tryggleiksnivå (inkl norske tilpassingar), jf. identifikasjonsnivåforskrifta artikkel 1 nr. 3. Dersom tilbydaren påberopar seg dette alternativet, ber vi om at det tydeleg blir angitt i beskrivingskolonnen.

Skildring av krav

Det skal skildrast korleis krava for følgjande element er oppfylte med sikte på å nå tryggleiksnivå «betydeleg» for det elektroniske identifikasjonsmiddelet innanfor ramma av eID-ordninga som er sjølvdeklart. Det skal oppgivast kva alternativ av kravet som er oppfylt dersom kravet har fleire alternativ.

2.1. Registrering		
2.1.1. Søknad og registrering		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Det blir sikra at søkjaren er kjend med vilkåra for bruk av elektroniske identifikasjonsmiddel.		
2. Det blir sikra at søkjaren er kjend med tilrådde tryggingstiltak knytte til elektroniske identifikasjonsmiddel.		
3. Relevante identitetsdata som blir kravde ved stadfesting og kontroll av identitet, blir samla inn.		
2.1.2. Stadfesting og kontroll av identitet (fysisk person)		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
L.1. Personen kan reknast med å vere i besittelse av eit bevis som er godkjent av medlemsstaten der det blir søkt om det elektroniske identitetsmiddelet, og som representerer den påberopte identiteten.		
L.2. Beviset kan reknast med å vere ekte eller eksistere i samsvar med ei autoritativ kjelde, og framstår som gyldig.		
L.3. Den påberopte identiteten eksisterer i samsvar med ei autoritativ kjelde, og det kan reknast med at vedkomande er den personen som påberoper seg identiteten.		
Eitt av alternativa i nr. 1 til 4 skal vere oppfylt. Angi tydeleg kva alternativ som er oppfylt: 1. Det er kontrollert at personen er i besittelse av eit bevis som er godkjent av medlemsstaten der det blir søkt om det elektroniske identitetsmiddelet, og som representerer den påberopte identiteten, og		

beviset blir kontrollert for å fastslå at det er ekte, eller at det i samsvar med ei autoritativ kjelde eksisterer og gjeld ein verkeleg person,

og

det er sett i verk tiltak for å minimere risikoen for at identiteten til personen ikkje er den påberopte identiteten, til dømes ved å ta omsyn til risikoen for at beviset er tapt, stole, mellombels oppheva, tilbakekalla eller utløpt,

Følgjande tilpassing gjeld for kravet i dette punktet (2.1.2 nr. 1), jf. sjølvdeklarasjonsforskrifta § 20 første ledd:

- Kravet om å ha eit bevis kan oppfyllest ved at personen godtgjer at han eller ho har tilgang til ei adresse (postadresse eller elektronisk) som er registrert på personen i det norske Folkeregisteret eller eit anna register som gir tilstrekkeleg tryggleik, til dømes kontaktregisteret. I tillegg må det finnast tiltak for å sikre at rett person tek i bruk eID-en, typisk varsling til ei anna eller same adresse.

eller

2. det blir lagt fram eit identitetsdokument i løpet av ein registreringsprosess i medlemsstaten der dokumentet er utferda, og dokumentet framstår som om det tilhøyrer personen som legg det fram,

og

det er sett i verk tiltak for å minimere risikoen for at identiteten til personen ikkje er den påberopte identiteten, til dømes ved å ta omsyn til risikoen for at dokumenta er tapte, stole, mellombels oppheva, tilbakekalla eller utløpt,

eller

3. når framgangsmåtar som tidlegare er nytta av ein offentleg eller privat eining i same medlemsstat, men for eit anna føremål enn utferding av elektroniske identifikasjonsmiddel, gir ein tryggleik tilsvarande det som er angitt for fysisk person for tryggleiksnivået «betydelig», treng den registreringsansvarlege eininga ikkje gjenta dei tidlegare framgangsmåtane, føreset at den likeverdige tryggleiken blir stadfesta av eit samsvarsvurderingsorgan som nemnt i artikkel 2 nr. 13 i europaparlaments- og rådsforordning (EF) nr. 765/2008 eller av eit tilsvarande organ,

eller

4. når det elektroniske identifikasjonsmiddelet er utferda på grunnlag av eit gyldig, meldt elektronisk identifikasjonsmiddel med tryggleiksnivået «betydelig» eller «høgt», og det samstundes blir teke omsyn til risikoen for endring i personidentifikasjonsopplysningane, er det ikkje nødvendig å gjenta stadfestinga og kontrollen av identitet. Når det elektroniske identifikasjonsmiddelet som ligg til grunn, ikkje er meldt, skal tryggleiksnivået «betydelig» eller «høgt» stadfestast av eit samsvarsvurderingsorgan som nemnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av eit tilsvarande organ. <i>Henvisingar i pkt. 2.1.2 til stadfestingar frå eit samsvarsvurderingsorgan blir òg tilfredsstilte av sjølvdeklarerte ordningar, jf. sjølvdeklarasjonsforskrifta § 17 andre ledd.</i>		
Kopling til folkeregistrert person (sjølvdeklarasjonsforskrifta § 18)		
Kravskildring	Oppfyller Ja/Nei	
Identitetspåstanden må gjelde ein person som finst i Folkeregisteret. eID-tilbydaren må kunne gi ei trygg og eintydig kopling til denne personen sin identifikator i Folkeregisteret (fødsels- eller d-nummer). Det at koplinga er trygg og eintydig inneber at ho ikkje kan baserast på personens namn eller andre kjenneteikn som kan vere i bruk av fleire personar. Skildr korleis koplinga til personen sin identifikator i Folkeregisteret blir godtgjort.		

2.2. Handtering av elektroniske identifikasjonsmiddel		
2.2.1. Dei elektroniske identifikasjonsmidla sine eigenskapar og utforming		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Det elektroniske identifikasjonsmiddelet nyttar minst to autentiseringsfaktorar frå ulike kategoriar som er definerte i pkt. 1 nr. 2 i vedlegget til identifikasjonsnivåforskrifta.		
2. Det elektroniske identifikasjonsmiddelet er utforma slik at det kan reknast med at det berre blir brukt dersom eigaren har kontroll over eller er tilstutt.		
2.2.2. Utferding, levering og aktivering		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Etter utferding blir det elektroniske identifikasjonsmiddelet levert via ein mekanisme som gjer at det kan reknast med at det berre blir levert til eigaren.		
2.2.3. Mellombels oppheving, tilbakekalling og reaktivering		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Det skal vere mogleg å oppheve eit elektronisk identifikasjonsmiddel mellombels og/eller tilbakekalle det til rett tid og på ein effektiv måte.		
2. Det finst tiltak for å hindre uautorisert mellombels oppheving, tilbakekalling og/eller reaktivering.		
3. Reaktivering skal berre finne stad dersom dei same tryggleikskrava som gjaldt før den mellombelse opphevingen eller tilbakekallinga, framleis er oppfylte.		
2.2.4. Fornying og erstatning		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Samstundes som det blir teke omsyn til risikoen for endring i personidentifikasjonsopplysningane, skal fornying eller erstatning oppfylle dei same tryggleikskrava som ved den opphavlege stadfestinga og kontrollen av identitet, eller vere basert på eit gyldig elektronisk identifikasjonsmiddel på same eller høgare tryggleiksnivå.		

2.3. Autentisering

2.3.1. Autentiseringsordning

Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
L.1. Personidentifikasjonsopplysningar blir utleverte etter behørig kontroll av det elektroniske identifikasjonsmiddelet og gyldigheita til dette.		
L.2. Når personidentifikasjonsopplysningar blir lagra som ein del av autentiseringsordninga, skal desse opplysningane sikrast slik at dei er verna mot tap og kompromittering, inkludert mot analyse utan nettforbinding.		
L.3. Autentiseringsordninga gjennomfører tryggleikskontrollar av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynleg at ein angripar med auka grunnleggjande angrepskapasitet kan gjette seg til, avlytte, avspela eller manipulere kommunikasjonen og på den måten omgå autentiseringsordninga.		
1. Personidentifikasjonsopplysningar blir utleverte etter behørig kontroll av det elektroniske identifikasjonsmiddelet og gyldigheita ved dynamisk autentisering.		
2. Autentiseringsordninga gjennomfører tryggleikskontrollar av det elektroniske identifikasjonsmiddelet, slik at det er svært usannsynleg at ein angripar med moderat angrepskapasitet kan gjette seg til, avlytte, avspela eller manipulere kommunikasjonen og på den måten omgå autentiseringsordninga.		

2.4. Forvaltning og organisering

2.4.1. Generelle føresegner

Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Tilbydarar av operative tenester som er omfatta av denne forordninga, skal vere ei offentleg myndigheit eller ei eining som er anerkjend som ein juridisk person i ein medlemsstat sin nasjonale rett, som har ein etablert organisasjon og er fullt operativ på alle område som er relevante for levering av tenestene.		

2. Tilbydarane oppfyller alle lovfesta krav dei er pålagde i samband med drift og levering av tenesta, mellom anna kva slags opplysningar som kan hentast inn, korleis identitet vert stadfesta, samt kva opplysningar som kan lagrast og kor lenge.		
3. Tilbydarane skal dokumentere evna si til å ta på seg risikoen knytt til erstatningsansvar, og at dei har tilstrekkelege økonomiske middel til vidare drift og tenestelevering.		
4. Det er tilbydarane sitt ansvar at alle plikter som er sette ut til ei anna eining, vert oppfylte, og at retningslinjene for ordninga vert følgde, som om dei sjølve hadde utført oppgåvene.		
5. Ordningar for elektronisk identifikasjon som ikkje er oppretta i samsvar med nasjonal rett, skal innehalde ein effektiv plan for verksemdsavvikling. Ein slik plan skal omfatte ei ryddig avvikling av tenesta, eller vidareføring hos ein annan tilbydar, korleis vedkomande styresmakter og sluttbrukarar skal informerast, samt nærare opplysningar om korleis register skal sikrast, oppbevarast og destruerast i samsvar med retningslinjene for ordninga.		
2.4.2. Offentleggjorde meldingar og brukarinformasjon		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Det finst ein offentliggjord definisjon av tenesta som omfattar alle gjeldande vilkår og gebyr, inkludert eventuelle avgrensingar i bruken. Tenestedefinisjonen skal innehalde eit personvernprogram.		
2. Det skal innførast føremålstenlege retningslinjer og framgangsmåtar for å sikre at brukarane av tenesta vert informerte i rett tid og på ein forsvarleg måte om eventuelle endringar i tenestedefinisjonen og i gjeldande vilkår og personvernprogram for den aktuelle tenesta.		
3. Det skal innførast føremålstenlege retningslinjer og framgangsmåtar som sikrar fullstendige og korrekte svar på førespurnader om informasjon.		
2.4.3. Forvaltning av informasjonssikkerheit		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
L.1. Det finst eit effektivt styringssystem for informasjonssikkerheit, for handtering og kontroll av risiko knytt til informasjonssikkerheit.		

1. Styringssystemet for informasjonssikkerheit følgjer dokumenterte standardar eller prinsipp for handtering og kontroll av tryggleiksrisiko.		
2.4.4. Oppbevaring av opplysningar		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Relevante opplysningar vert registrerte og haldne oppdaterte ved hjelp av eit effektivt registreringssystem, der det vert teke omsyn til relevant lovgiving og god praksis knytt til vern av personopplysningar og datalagring.		
2. Opplysningar vert oppbevarte, i den grad det er tillate i samsvar med nasjonal rett eller andre nasjonale administrative ordningar, og vert verna så lenge det er behov for dei med sikte på revisjon, undersøking av tryggleiksbrot og dokumentasjon. Deretter vert opplysningane destruerte på ein trygg måte.		
2.4.5. Lokale og personale		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Det finst framgangsmåtar for å sikre at personale og underleverandørar har tilstrekkeleg opplæring, kompetanse og erfaring til å kunne utføre oppgåvene sine.		
2. Det finst tilstrekkeleg med personale og underleverandørar til å drifte og vedlikehalde tenesta i samsvar med dei gjeldande retningslinjene og framgangsmåtane.		
3. Lokala som vert nytta til å levere tenesta, vert kontinuerleg kontrollerte og verna mot skadar som følgje av miljøhendingar, uautorisert tilgang og andre faktorar som kan påverke tryggleiken til tenesta.		
4. Lokala som vert nytta til å levere tenesta, skal sikre at tilgangen til område der personopplysningar og kryptografiske eller andre sensitive opplysningar vert oppbevarte eller handsama, er avgrensa til godkjent personale eller godkjende underleverandørar.		
2.4.6. Tekniske kontrollar		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon

L.1. Det finst tekniske kontrollar som er eigna til å handtere risikoane knytte til tryggleiken i tenestene og til å sikre konfidensialitet, integritet og tilgjenge for dei handsama opplysningane.		
L.2. Elektroniske kommunikasjonskanalar som vert nytta til å utveksle personopplysningar eller sensitive opplysningar, vert verna mot avlytting, manipulering og gjenavspeling.		
L.3. Tilgang til sensitivt kryptografisk materiale skal avgrensast til funksjonar og applikasjonar som har eit absolutt behov for slik tilgang, når materialet vert nytta til å utferde elektroniske identifikasjonsmiddel og til autentisering. Det skal sikrast at slikt materiale aldri vert lagra permanent i klartekst.		
L.4. Det finst framgangsmåtar som sikrar at tryggleiken vert oppretthalden over tid, og at det kan reagerast på endra risikonivå, hendingar og tryggleiksbrot.		
L.5. Alle medium som inneheld personopplysningar og kryptografiske eller andre sensitive opplysningar, skal lagrast, transporterast og avhendast på ein trygg og sikker måte.		
1. Sensitivt kryptografisk materiale skal vernast mot ulovlege inngrep når det vert nytta til å utferde elektroniske identifikasjonsmiddel og til autentisering. Følgjande tilpassing gjeld for kravet i dette punktet (2.4.6 nr. 1), jf. sjølvdeklarasjonsforskrifta § 20 andre ledd: – Kravet kan til dømes oppfyllest ved bruk av sikra maskinvaremodular (HSM) eller kombinasjonar av tilgangsstyring, logging, overvaking og tenestedeling. Kravet tek sikte på å hindre at autoriserte personar åleine og utan å bli oppdaga kan compromittere prosessane.		
2.4.7. Etterleving og revisjon		
Kravskildring	Oppfyller Ja/Nei	Skildring og tilvising til eventuell dokumentasjon
1. Det vert jamleg gjennomført uavhengige interne eller eksterne revisjonar som omfattar alle delar som er relevante for levering av tenestene, for å sikre samsvar med relevante retningslinjer.		

Underlagsdokumentasjon

Gje opp alle vedlagde underlagsdokument og opplys kva for element ovanfor dei er knytte til. Legg ved ein engelsk versjon eller ei engelsk omsetjing av dokumentasjonen dersom ho ligg føre.

Merknad

Dato og underskrift

Underteikna stadfestar kjennskap til føresegnene i forskrift om sjølvdeklarasjonsordninga som gjeld for tilbydarar av eID-ordningar, og at opplysningane som er gjevne i dette skjemaet, er korrekte. Underteikna er merksam på at verksemda kan verte pålagd å betale sektoravgift i samsvar med [forskrift av 21. november 2019 nr. 1578 om sjølvdeklarasjon om ordningar for elektronisk identifikasjon § 15](#) jf. [lov av 15. juni 2018 nr. 44 om elektroniske tillitstenester § 7](#), og [forskrift av 20. mars 2017 nr. 386 om sektoravgift og gebyr til Nasjonal kommunikasjonsmyndigheit § 7](#).

Sted, Dato

Underskrift (må ha signaturfullmakt)

Gjenta underskriften her med blokkbokstaver

Vedlegg til skjema

Administrativ informasjon til Nkom	
<i>Denne informasjonen er ikke en del av skjemaet og vert ikke publisert på nettsida til Nkom.</i>	
E-post for administrative førespurnader	
E-post for tekniske førespurnader	
Kontaktperson(ar): Namn, e-post, telefon	
Ansvarleg(e) person(ar) for rapportering av tryggleikshendingar	
Referanse/bestillingsnummer for elektronisk faktura	