

**Meldingsskjema for sjølvdeklarasjon av ordning for elektronisk identifikasjon
– tryggleiksnivå «høgt»****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 sjølvdeklarasjonsordninga 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 deklart(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.

Offentleggjing 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 sjølvdeklart etter sjølvdeklarasjonsforskrifta, saman med motteken melding etter sjølvdeklarasjonsforskrifta § 7. Forretningsmessige opplysningar av sensitiv art eller teiepliktige opplysningar må difor oppgjevast i vedlegg der det blir spesifisert kva krav dei er relaterte til.

Utfylt skjema sendast til: firmapost@nkom.no

Opplysningar om tilbydar

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

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 «høyt»

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 «høyt» og er strukturert i tråd med identifikasjonsnivåforskriftens oppbygning. Norske tilpasninger for sikkerhetsnivå «høyt» er lagt inn på de relevante punktene i identifikasjonsnivåforskriften, pkt. 2.1.2 og 2.3.1.

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. Dette gjelder punktene 2.1.2, 2.2.1, 2.2.4, 2.3.1, 2.4.3, 2.4.6. Skjemaet skal ta høyde for denne leserutfordringen, inkludert de norske tilpasninger for kravene for sikkerhetsnivå «høyt» i pkt. 2.1.2 og 2.3.1, jf. selvdeklarasjonsforskriften § 19. Når kumulative krav er gjengitt fremgår det av nummereringen i skjemaet. (L.1 = krav nr. 1 for sikkerhetsnivå «lavt», B.1 = krav nr. 1 for sikkerhetsnivå «betydelig»).

Beskrivelse av krav

Det skal beskrives hvordan kravene for følgende elementer er oppfylt med sikte på å nå sikkerhetsnivå «høyt» for elektroniske identifikasjonsmiddelet innenfor rammen av eID-ordningen som er selvdeklart. Det skal angis hvilket alternativ av kravet som er oppfylt dersom kravet har flere alternativer.

2.1. Registrering		
2.1.1. Søknad og registrering		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til 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. Bekreftelse og kontroll av identitet (fysisk person)		
Kravbeskrivelse	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
Krava i nr. 1 eller 2 skal vere oppfylte. Oppgjev tydeleg kva krav som er oppfylt: 1. Krava til tryggleiksnivå «betydeleg» (krava L.1-L.3 og eitt av krava B.1-B.4), samt eitt av alternativane i bokstav (a) til (b) skal vere oppfylte. L.1. Personen kan antakast 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 antakast å vere ekte eller eksistere i samsvar med ein autoritativ kjelde, og framstår som gyldig. L.3. Den påberopte identiteten eksisterer i samsvar med ein autoritativ kjelde, og det kan antakast at vedkomande er den personen som påberoper seg identiteten. Eitt av alternativa i bokstav B.1 til B.4 skal vere oppfylt. Oppgjev tydeleg kva alternativ som er oppfylt: B.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 ein 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. B.1), jf. sjølvdeklarasjonsforskrifta § 20 første ledd: <i>- 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 eID-en i bruk, typisk varsling til ei anna eller same adresse.</i> eller B.2. det blir lagt fram eit identitetsdokument i løpet av ein registreringsprosess i medlemsstaten der dokumentet er utferda, og dokumentet framstår som om det høyrer til 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 B.3. når framgangsmåtar som tidlegare er nytta av ein offentlig 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		
---	--	--

B.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.

Og eitt av alternativa i nr. 1 bokstav (a) til (c) skal vere oppfylt. Oppgjev tydeleg kva alternativ som er oppfylt:

(a) når det er stadfesta at personen er i besittelse av eit fotografisk eller biometrisk identifikasjonsbevis som er godkjent av medlemsstaten der det blir søkt om det elektroniske identitetsmiddelet, og beviset er knytt til den påberopte identiteten, blir beviset kontrollert med sikte på å fastslå at det er gyldig i samsvar med ein autoritativ kjelde.

Følgjande tilpassing gjeld for kravet i dette punktet (2.1.2 nr. 1 bokstav a), jf. sjølvdeklarasjonsforskrifta § 19 første ledd:

- Som gyldig identitetsbevis blir pass eller nasjonalt identitetskort rekna. For utanlandsk identitetsbevis må eintydig knyting til norsk identitetsnummer godtgjers.
- Kravet er òg oppfylt for eID på nivå 4 i samsvar med rammeverket frå 2008 for autentisering og uavvising.

og

søkjaren blir identifisert som den påberopte identiteten ved å samanlikne eitt eller fleire av personen sine fysiske kjenneteikn med ein autoritativ kjelde.

eller

(b) 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 «høgt», 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 forordning (EF) nr. 765/2008, eller av eit tilsvarande organ,

og

det blir sett i verk tiltak for å dokumentere at resultata frå tidlegare framgangsmåtar framleis er gyldige, eller (c) når det elektroniske identifikasjonsmiddelet er utferda på grunnlag av eit gyldig, meldt elektronisk identifikasjonsmiddel med tryggleiksnivået «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 «høgt» stadfestast av eit samsvarsvurderingsorgan som nemnt i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, eller av eit tilsvarande organ, <i>Tilvisingar i pkt. 2.1.2 til stadfestingar frå eit samsvarsvurderingsorgan blir òg oppfylte av sjølvdeklarerte ordningar, jf. sjølvdeklarasjonsforskrifta § 17 andre ledd.</i> og det blir sett i verk tiltak for å dokumentere at resultata av denne tidlegare framgangsmåten for utferding av eit meldt elektronisk identifikasjonsmiddel framleis er gyldige. ELLER 2. Når søkjaren ikkje legg fram eit godkjent fotografisk eller biometrisk identifikasjonsbevis, blir same framgangsmåte nytta for å framskaffe eit slikt godkjent fotografisk eller biometrisk identifikasjonsbevis som den som blir nytta på nasjonalt plan i den aktuelle medlemsstaten av den registreringsansvarlege eininga.		
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 koplinga ikkje kan baserast på personen sitt 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. De elektroniske identifikasjonsmidlenes egenskaper og utforming

Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
B.1. Det elektroniske identifikasjonsmiddelet nyttar minst to autentiseringsfaktorar frå ulike kategoriar som er definerte i pkt. 1 nr. 2 i vedlegget til identifikasjonsnivåforskrifta.		
B.2. Det elektroniske identifikasjonsmiddelet er utforma slik at det kan leggjast til grunn at det berre vert brukt dersom eigaren har kontroll over eller er i besittelse av det.		
1. Det elektroniske identifikasjonsmiddelet er verna mot kopiering og manipulering, og mot angripingar med høg angrepskapasitet.		
2. Det elektroniske identifikasjonsmiddelet er utforma slik at eigaren på ein trygg måte kan hindre at det vert brukt av andre.		

2.2.2. Utferding, levering og aktivering

Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
1. Aktiveringsprosessen kontrollerer at det elektroniske identifikasjonsmiddelet ikkje er levert til andre enn eigaren.		

2.2.3. Mellombels oppheving, tilbakekalling og reaktivering

Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
1. Det er 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 opphevinga eller tilbakekallinga, framleis er oppfylte.		
2.2.4. Fornyng og erstatning		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
L.1. Samtidig som det vert teke omsyn til risikoen for endring i personidentifikasjonsopplysningane, skal fornyng eller erstatning oppfylle dei same tryggleikskrava som ved opphavleg stadfesting og kontroll av identitet, eller vere basert på eit gyldig elektronisk identifikasjonsmiddel på same eller høgare tryggleiksnivå.		
1. Når fornyng eller erstatning er basert på eit gyldig elektronisk identifikasjonsmiddel, skal identitetsdata kontrollerast mot ei autoritativ kjelde.		

2.3. Autentisering		
2.3.1. Autentiseringsordning		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
L.1. Personidentifikasjonsopplysningar vert utleverte etter behørig kontroll av det elektroniske identifikasjonsmiddelet og gyldigheita til dette.		
L.2. Når personidentifikasjonsopplysningar vert 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 lite sannsynleg at ein angripar med auka grunnleggjande angrepskapasitet kan gjette seg fram til, avlytte, avspela eller manipulere kommunikasjonen og på den måten omgå autentiseringsordninga.		
B.1. Personidentifikasjonsopplysningar vert utleverte etter behørig kontroll av det elektroniske identifikasjonsmiddelet og gyldigheita til dette ved dynamisk autentisering.		

B.2. Autentiseringsordninga gjennomfører tryggleikskontrollar av det elektroniske identifikasjonsmiddelet, slik at det er svært lite sannsynleg at ein angripar med moderat angrepskapasitet kan gjette seg fram til, avlytte, avspela eller manipulere kommunikasjonen og på den måten omgå autentiseringsordninga.		
1. Autentiseringsordninga gjennomfører tryggleikskontrollar av det elektroniske identifikasjonsmiddelet, slik at det er svært lite sannsynleg at ein angripar med moderat angrepskapasitet kan gjette seg fram til, avlytte, avspela eller manipulere kommunikasjonen og på den måten omgå autentiseringsordninga.		
Følgjande presisering gjeld for kravet i dette punktet (2.3.1 nr. 1), jf. selvdeklarasjonsforskrifta § 19 andre ledd: <i>- Kravet er ikkje til hinder for at identitetsinformasjon, til dømes fødselsnummer, vert gjort tilgjengeleg på annan måte, til dømes i oppslagsteneste eller ved at det vert lagra i sertifikatet for PKI-baserte eID-ar. Kravet i 2.3.1 nr. 2 høgt gjeld utlevering av identitetsinformasjon ved autentisering.</i>		

2.4. Forvaltning og organisering		
2.4.1. Generelle føresegner		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
1. Tilbydarar av operative tenester som er omfatta av denne forordninga, skal vere ei offentlig myndigheit eller ei eining som er anerkjend som ein juridisk person i ein medlemsstats 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 ved erstatningsansvar, og at dei har tilstrekkelege økonomiske midlar til vidare drift og levering av tenester.		

4. Det er tilbydarane sitt ansvar at alle forpliktingar 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 vert informerte, samt nærare opplysningar om korleis register skal vernast, oppbevarast og destruerast i samsvar med retningslinjene for ordninga.		
2.4.2. Offentleggjorde meldingar og brukarinformasjon		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
1. Det finst ein offentleggjort 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 retningsliner og framgangsmåtar for å sikre at brukarane av tenesta vert informerte til rett tid og på behørig måte om eventuelle endringar i tenestedefinisjonen og i gjeldande vilkår og personvernprogram for den aktuelle tenesta.		
3. Det skal innførast føremålstenlege retningsliner og framgangsmåtar som sikrar fullstendige og riktige svar på førespurnader om informasjon.		
2.4.3. Forvaltning av informasjonssikkerheit		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
L.1. Det finst eit effektivt styringssystem for informasjonssikkerheit, til 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 eventuell tilvising til dokumentasjon

1. Relevante opplysningar vert registrerte og haldne ajour ved hjelp av eit effektivt registreringssystem, der det vert teke omsyn til relevant lovgiving og god praksis i samband med 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 oppbevaring, og vert deretter destruerte på ein trygg måte.		
2.4.5. Lokale og personale		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
1. Det finst framgangsmåtar for å sikre at personale og underleverandørar har tilstrekkeleg opplæring, kvalifikasjonar og erfaring til å kunne utføre oppgåvene sine.		
2. Det finst tilstrekkeleg personale og underleverandørar til å drifte og vedlikehalde tenesta i samsvar med dei retningslinene og framgangsmåtane som gjeld for henne.		
3. Lokala som vert nytta til å levere tenesta, vert kontinuerleg kontrollerte og verna mot skadar som kjem av miljøhendingar, uautorisert tilgang og andre faktorar som kan påverke tryggleiken til tenesta.		
4. Lokala som vert nytta til å levere tenesta, sikrar 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 eventuell tilvising til dokumentasjon
L.1. Det finst tekniske kontrollar som er eigna til å handtere risikoane knytte til tryggleiken i tenestene og sikre konfidensialitet, integritet og tilgjenge for dei opplysningane som vert handsama.		
L.2. Elektroniske kommunikasjonskanalar som vert nytta til å utveksle personopplysningar eller sensitive opplysningar, vert verna mot avlytting, manipulering og avspeling.		

L.3. Tilgang til sensitivt, kryptografisk materiale vert avgrensa til funksjonar og applikasjonar som absolutt krev tilgang, dersom det vert nytta til å utstede elektroniske identifikasjonsmiddel og til autentisering. Det skal sikrast at slikt materiale aldri vert lagra permanent i rein tekst.		
L.4. Det finst framgangsmåtar som garanterer at tryggleiken vert oppretthaldt 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, vert lagra, transporterte og bortskaffa på ein trygg og sikker måte.		
1. Sensitivt kryptografisk materiale vert verna mot ulovlege inngrep dersom det vert nytta til å utstede elektroniske identifikasjonsmiddel og til autentisering.		
2.4.7. Etterleving og revisjon		
Kravskildring	Oppfyller Ja/Nei	Skildring og eventuell tilvising til dokumentasjon
1. Det vert gjennomført jamlege, uavhengige eksterne revisjonar som omfattar alle delar som er relevante for levering av tenestene, for å sikre samsvar med relevante retningsliner.		
2. Når ei ordning vert forvalta direkte av eit statleg organ, skjer revisjon i samsvar med nasjonal rett.		

Underlagsdokumentasjon

Angje alle vedlagde underlagsdokument, og kva for element ovanfor dei er knytte til. Legg ved ein engelsk versjon eller ei engelsk omsetjing av dokumentasjonen dersom det finst.

Merknad

Dato og underskrift

Underteikna stadfestar kjennskap til føresegnene i forskrift om sjølvdeklarasjonsordninga som gjeld for tilbydarar av eID-ordningar, og at opplysningar gjevne på dette skjemaet er korrekte. Underteikna er merksam på at verksemda kan bli 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

Denne informasjonen er ikke en del av skjemaet og blir ikke publisert på Nkom si nettside.

E-post for administrative førespurnadar	
E-post for tekniske førespurnadar	
Kontaktperson(er): Namn, e-post, telefon	
Ansvarleg(e) person(ar) for rapportering av tryggleikshendingar	
Referanse/bestillingsnummer for elektronisk faktura	