

# NSIS 2.0.1 opdatering

3. oktober 2019

---

Digitaliseringsstyrelsen har publiceret en opdateret version (2.0.1) af National Standard for Identiteters Sikringsniveauer (NSIS).

Baggrunden for opdateringen er, at analysefaserne for MitID- og NemLog-in3 projekterne har identificeret områder med behov for præcisering og udbygning af standard og tilhørende vejledning. Der er tale om mindre præciseringer af NSIS, hvilket også er afspejlet i skiftet af versionsnummer fra 2.0.0 til 2.0.1. Da omfanget og karakteren af opdateringen er af mindre karakter, gennemføres ikke fornyet høring i forbindelse med opdateringen.

Spørgsmål og kommentarer til opdateringen kan rettes til [nl3@digst.dk](mailto:nl3@digst.dk).

## Opdateringer til standarden

Herunder findes en kort gennemgang af de væsentligste opdateringer i standarden:

- Overalt i NSIS er begrebet ”juridisk person” erstattet med begrebet ”juridisk enhed”, som er defineret i CVR-lovens § 3. Denne opdatering er sket med henblik på at opnå en bredere dækning i NSIS, idet juridisk enhed for eksempel også omfatter fysiske personer i deres egenskab af arbejdsgiver eller enkeltmandsvirksomhed i tillæg til kredsen af juridiske personer. Bemærk, at denne opdatering er undtaget fra versionen med ændringsmærking for at lette overskueligheden.
- I afsnit 3.1.2 og 3.1.3 er det nu præciseret, at det også er tilladt at basere identitetssikring på en autentifikation med gyldigt eIDAS identifikationsmiddel på samme sikringsniveau.
- I afsnit 3.1.2 er der indført en række præciseringer vedr. identitetssikring af fysiske personer:
  - Sprogbrugen er ensrettet, så termen ’dokumentation’ konsekvent benyttes (termen ’bevis’ udgår).
  - Punkt 6 er sprogligt justeret fra ’autoritativt register’ til ’autoritativ kilde’, og samtidig er vejledningen blevet udbygget, så det er mere tydeligt, hvordan identitetssikring for personer med hhv. uden CPR-nummer kan gennemføres.

- I afsnit 4.1.2 er det præciseret, at visse af kravene til oplysningspligt kun er relevante for Elektroniske Identifikationsordninger (dvs. ikke for Identitetsbrokere).
- I afsnit 4.1.3 vedr. informationssikkerhedsledelse er det præciseret på niveau Høj, at det er ledelsessystemet og ikke organisationen, som skal være certificeret (eller på tilsvarende måde skal kunne dokumentere efterlevelse af krav til informationssikkerhedsledelse).
- I afsnit 4.1.7 er det tydeliggjort, at en løsning først efter anmeldelse og publicering på Digitaliseringsstyrelsens hjemmeside må påberåbe sig overholdelse af NSIS samt påstemple NSIS sikringsniveauer i en autentifikation, der formidles til tredjepart.
- I afsnit 4.1.7 er links til revisionsvejledning opdateret til den seneste version.
- Link til Datatilsynets seneste vejledning om samtykke fra september 2019 er indsat.

Der publiceres en version af NSIS-dokumenterne med ændringsmarkering på styrelsens hjemmeside med henblik på at lette sammenligning af version 2.0.0 og 2.0.1.

## Opdateringer til vejledning til NSIS

Udover selve standarden er vejledningen til NSIS også blevet opdateret. Opdateringer gennemgås herunder:

- Vejledningen til identitetssikring af fysiske personer (3.1.2) er som tidligere nævnt blevet udbygget, så det er mere tydeligt, hvordan identitetssikring for personer med hhv. uden CPR gennemføres. Der henvises nu også til Finanstilsynets vejledning til hvidvaskloven for eksempler på indhentning og kontrol af identitetsoplysninger.
- Eksempler på gyldig dokumentation (fx pas og kørekort) for fysiske personer (3.1.2) er flyttet fra standard til vejledning.
- Under informationssikkerhedsledelse (4.1.3) er det præciseret, at ISMS'et skal dække ID-tjenesten men ikke nødvendigvis hele organisationen.
- Under anmeldelse og revision (4.1.7) henvises til den nye anmeldelsesskabelon, og listen med krav til indhold i anmeldelsen er flyttet til denne. Det er samtidig præciseret, at det er obligatorisk at anvende de udarbejdede skabeloner.
- I kapitel 6 (Identitetsbrokere) er det tydeliggjort, at brokere skal indestå for det sikringsniveau, der påtrykkes i et udstedt token, også er korrekt og lever op til NSIS.

## Vejledning til tjenesteudbydere

Vejledningen til tjenesteudbydere har ligeledes undergået en mindre opdatering. Her er den vigtigste ændring, at henvisningen til Excel-regneark vedr. privatlivsvurdering udgår, idet regnearket var udarbejdet før GDPR og NSIS, og den underliggende regnemodel i arket vurderes ikke at tage højde for alle relevante forhold. Regnearket er erstattet med beskrivelse af, hvorledes tjenesteudbydere kan foretage en risikovurdering i overensstemmelse med Datatilsynets seneste vejledning på området.

## Opdateret skema til revision

Regnearket med skema, der er bilag til revisionsvejledningen, er konsekvensrettet i henhold til de opdateringer, der (som tidligere nævnt) er sket til kravene i NSIS.

## Ny anmeldelsesskabelon

Digitaliseringsstyrelsen har udarbejdet en skabelon til anmeldelser, som oplister og strukturerer de dokumenter og den øvrige information, som skal indsendes. Skabelonen er obligatorisk at anvende og letter overblikket over, om informationspakken er komplet.