NAs ref.: 23/0831	**Datatilsynets ref.**: 23/01175	**Dato**: 23. juni 2023

Bilag til samarbeidsavtalen mellom Datatilsynet og Norsk akkreditering

Det forventes at Ordningseieren skal ha uformelle diskusjoner med Norsk akkreditering og/eller Datatilsynet om deres Sertifiseringsordning før Fase 1 begynner.

Fase 1: Prosess for å gjennomgå en Sertifiseringsordning og for å godkjenne Sertifiseringskriterier

Steg 1: Ordningseieren sender søknad til Norsk akkreditering

Ordningseieren skal sende en søknad til Norsk akkreditering om:

- gjennomgåelse av den foreslåtte Sertifiseringsordningen (som skal gjøres av Norsk akkreditering), og
- godkjenning av Sertifiseringskriteriene (som skal gjøres av Datatilsynet).

Norsk akkreditering skal sjekke om søknaden inneholder alt den skal for at søknaden kan behandles før steg 2 kan begynnes.

Søknaden skal inneholde følgende:

- beskrivelse av hvordan den foreslåtte Sertifiseringsordningen medfører en klar og tydelig fordel for:
  - behandlingsansvarliges eller databehandleres påvisning av overholdelse av personvernforordningen, og
  - registrerte ved at behandlingen av deres personopplysninger påvises overholdt av personvernforordningen.
- Sertifiseringsordningens dokumenter, herunder:
  - en spesifikasjon av elementene beskrevet i NS-EN ISO/IEC 17067:2013 paragraf 6.5.1, og
  - Sertifiseringskriterier
- angivelse av hvilken type virksomhet, herunder størrelse på virksomheten som kan bruke Sertifiseringsordningen
- erklæring fra Ordningseieren om at de forstår at Sertifiseringskriterier skal offentliggjøres av Datatilsynet og/eller Personvernrådet etter godkjenning
- eksempler på hvordan Sertifiseringsordningen og Sertifiseringskriterier skal brukes (brukstilfeller)

Steg 2: Norsk akkreditering gjennomgår Sertifiseringsordningens dokumenter

Norsk akkreditering skal gjennomgå Sertifiseringsordningens dokumenter og skal blant annet:

- vurdere om Sertifiseringsordningen:
  - oppfyller kravene i EA 1/22 og IAF MD 25
  - egner seg for akkreditering i henhold til NS-EN ISO/IEC 17065:2012, det vil si om det er mulig å vurdere samsvar basert på Sertifiseringsordningen
- kontrollere at dokumentasjon er fremlagt som bekrefter:
  - Ordningseierens juridisk status
  - at Ordningseieren har myndighet til å endre og vedlikeholde Sertifiseringskriteriene og Sertifiseringsordningen for øvrig
  - om Ordningseieren også er et Sertifiseringsorgan som søker Akkreditering, eller en separat organisasjon fra eventuelle Sertifiseringsorganer
  - at eventuelle krav til Sertifiseringsorganer ikke motsier eller ekskluderer krav i NS-EN ISO/IEC 17065:2012 eller Datatilsynets tilleggskrav til akkreditering av sertifiseringsorgan.

Norsk akkreditering vil deretter utarbeider en rapport som viser eventuelle avvik (mangler). Rapporten sendes til Ordningseieren som gis mulighet til å lukke avvik. Hvis avvik ikke lukkes innen rimelig tid, terminerer Norsk akkreditering søknaden.

Etter alle avvik er lukket av Ordningseieren skal Norsk akkreditering informerer Datatilsynet om resultatet og sende dem relevante dokumenter for at Datatilsynet kan begynne steg 3.

Steg 3: Datatilsynet gjennomgår og vurderer Sertifiseringskriteriene

Datatilsynet vil gjøre en fullstendig vurdering av Sertifiseringskriterier i henhold til:

- retningslinjer 1/2018 utsedt av Personvernrådet om angivelse av sertifiseringskriterier i samsvar med personvernforordningen artikkel 42 og 43, og
- addendum til retningslinjer 1/2018

Vurderingen kan innebære møter mellom Ordningseieren og Datatilsynet for å diskutere Sertifiseringskriterier i mer detalj. Datatilsynet kan be Ordningseieren om å endre Sertifiseringskriteriene.

Datatilsynet vil starte samarbeidsprosedyren med Personvernrådet når Datatilsynet mener at Sertifiseringskriterier er tilstrekkelige.

Steg 4: Datatilsynets samarbeidsprosedyre med Personvernrådet

<u>For Sertifiseringsordninger som kun skal gjelde i Norge</u>
Personvernrådet må gi en uttalelse på Sertifiseringskriterier før Datatilsynet kan eventuelt godkjenne dem.

<u>For Sertifiseringsordninger som skal gjelde i hele EØS</u>
Personvernrådet må godkjenne Sertifiseringskriterier selv. I sånne tilfeller, er ikke Steg 5 og 6 relevant, og Personvernrådets egen prosedyre gjelder.

Samarbeidsprosedyren med Personvernrådet finnes på Personvernrådets nettsider: https://edpb.europa.eu/system/files/2023-02/edpb_document_procedure_for_the_adoption_edpb_opinions_regarding_national_criteria_for_certification_european_data_protection_seals_en.pdf.

Steg 5: Eventuelle endringer til Sertifiseringskriterier

Uttalelse fra Personvernrådet kan inneholde anbefalinger og oppmuntringer om Sertifiseringskriterier som Datatilsynet skal ta hensyn til. Datatilsynet forventer at Ordningseieren endrer Sertifiseringskriterier i den grad det er nødvendig for å tilfredstille anbefalinger og oppmuntringer i uttalelsen fra Personvernrådet.

Steg 6: Datatilsynet godkjenner Sertifiseringskriteriene

For Sertifiseringsordninger som kun skal gjelde i Norge
Datatilsynet kan godkjenne Sertifiseringskriterier og gi beskjed til Norsk akkreditering og Ordningseieren etter at Ordningseieren tilfredsstiller anbefalinger og oppmuntringer i uttalelsen fra Personvernrådet. De godkjente Sertifiseringskriteriene skal offentliggjøres av Datatilsynet og/eller Personvernrådet – og kan deretter brukes som standard i en Sertifiseringsordning.

For Sertifiseringsordninger som skal gjelde i hele EØS
Datatilsynet skal videreformidle aktuell godkjennelse fra Personvernrådet til Norsk akkreditering og Ordningseieren.

Fase 2: Akkreditering av Sertifiseringsorganer

Sertifiseringsorganer som ønsker Akkreditering med hensyn til et Sertifiseringsordning med Sertifiseringskriterier godkjent av Datatilsynet eller Personvernrådet skal følge Norsk akkrediterings vanlig prosedyre for å bli akkreditert, med følgende tillegg:

- Sertifiseringsorganet skal vise at de ikke er gjenstand for kontroll eller tilsyn av Datatilsynet som kan være til hinder for Akkrediteringen. Norsk akkreditering skal verifisere dette med Datatilsynet.

Fase 3: Oppfølging

Norsk akkreditering har ansvar for å følge opp Sertifiseringsorganers Akkreditering i henhold til deres vanlige regler og rutiner. Norsk akkreditering skal tilbakekalle Akkreditering dersom vilkår for å være akkreditert (herunder Akkrediteringskravene) ikke lenger oppfylles eller dersom tiltak truffet av Sertifiseringsorganet er i strid med personvernforordningen. Norsk akkreditering skal samtidig varsle Datatilsynet om dette.

Hvis Datatilsynet blir oppmerksom på forhold som tilsier at forutsetningene for innvilget Sertifisering ikke var oppfylt eller ikke lenger oppfylles, skal de be det aktuelle Sertifiseringsorganet om å redegjøre for seg. Datatilsynet kan pålegge Sertifiseringsorganet

om å tilbakekalle Sertifisering i henhold til personvernforordningen artikkel 58 nr. 2 bokstav h. Datatilsynet skal samtidig informere Norsk akkreditering om dette.