Datatilsynets tilleggskrav til akkreditering av sertifiseringsorganer

Februar 2024

Datatilsynet

Innhold

Introduksjon

Dette dokumentet inneholder Datatilsynets tilleggskrav til akkreditering av sertifiseringsorganer i henhold til ISO/IEC 17065:2012 ("**ISO 17065**") og personvernforordningen artikkel 43 nr. 1 bokstav b og 43 nr. 3. Kapitlene nedenfor (bortsett fra kapittel 9) referer til kapitteloverskriftene i ISO 17065 og fastsetter tilleggskravene for tilsvarende punktnummer i ISO 17065.

Forord

Etter personvernforordningen artikkel 43 nr.1 bokstav a og b, har både Datatilsynet og Norges nasjonale akkrediteringsmyndighet, Norsk akkreditering, kompetanse til å akkreditere sertifiseringsorganer.

Likevel vil Norsk akkreditering i praksis være ansvarlig for å akkreditere sertifiseringsorganer, fordi de har omfattende erfaring med akkreditering på andre områder. Selskaper eller offentlige myndigheter må derfor kontakte Norsk akkreditering hvis de ønsker å bli akkreditert som sertifiseringsorgan.

Måten Datatilsynet og Norsk akkreditering skal samarbeide på er fastsatt i en samarbeidsavtale utarbeidet av Datatilsynet og Norsk akkreditering. Samarbeidsavtalen fastslår roller, ansvarsområder, og operasjonelle prosedyrer for akkreditering av sertifiseringsordninger knyttet til personvernforordningen. Samarbeidsavtalen er tilgjengelig på Datatilsynets nettside.

Hvis Datatilsynet på noe tidspunkt velger å benytte sin kompetanse til å akkreditere sertifiseringsorganer i henhold til personvernforordningen artikkel 43 nr.1 bokstav a, vil Datatilsynet akkreditere sertifiseringsorganer i henhold til ISO 17065 og disse tilleggskravene med nødvendige justeringer. Slike nødvendige justeringer vil primært innebære å referere til Datatilsynet hvor tilleggskravene nå referer til Norsk akkreditering.

1 Omfang

Dette dokumentet inneholder tilleggskrav til ISO 17065 for å vurdere sertifiseringsorganers dybdekunnskap, konsekvent drift og uavhengighet under personvernforordningen.

ISO 17065 skal brukes i samsvar med personvernforordningen. Det europeiske Personvernrådet ("Personvernrådet") sine retningslinjer om akkreditering[1] og sertifisering[2] gir mer utfyllende informasjon.

Det brede omfanget av ISO 17065, som dekker produkter, prosesser og tjenester, hverken senker eller tilsidesetter kravene i personvernforordningen. Derfor må sertifisering gjelde behandling av personopplysninger, det vil si behandlingsaktiviteter. Et styringssystem, for eksempel et informasjonsstyringssystem for personvern, kan være en del av en sertifiseringsmekanisme, men det kan ikke være det eneste elementet i mekanismen, fordi sertifiseringen må gjelde behandling av personopplysninger.

Omfanget av en sertifiseringsmekanisme (for eksempel sertifisering av behandlingsaktiviteter knyttet til en skytjenestetilbyder) må tas i betraktning av akkrediteringsmyndigheten i løpet av akkrediteringsprosessen, særlig med hensyn til kriterier, dybdekunnskap og evalueringsmetoder.

I tillegg skal sertifisering under personvernforordningen kun utstedes for behandlingsaktivitetene til behandlingsansvarlige og databehandlerne, jf. personvernforordningen artikkel 42 nr. 1.

[1] Retningslinjer 4/2018 om akkreditering av sertifiseringsorganer i henhold til artikkel 43 i personvernforordningen (2016/679). Også tilgjengelig på dansk.

[2] Retningslinjer 1/2018 om sertifisering og identifisering av sertifiseringskriterier i overenstemmelse med artikkel 42 og 43 i personvernforordningen. Også tilgjengelig på dansk.

2 Normative referanser

Personvernforordningen har forrang over ISO 17065. Hvis det henvises til andre ISO-standarder i tilleggsvilkårene eller i sertifiseringsmekanismen, skal disse tolkes i tråd med bestemmelsene i personvernforordningen.

3 Termer og definisjoner

Termer og definisjoner i Personvernrådets retningslinjer for akkreditering og sertifisering skal anvendes og har forrang over ISO-definisjoner. For enkelhets skyld er de sentrale definisjonene brukt i dette dokumentet listet nedenfor.

Akkreditering: En attestering fra et nasjonalt akkrediteringsorgan og/eller av en tilsynsmyndighet, om at et sertifiseringsorgan er kvalifisert til å utføre sertifisering i henhold til personvernforordningen artikkel 42 og 43, idet det tas hensyn til ISO 17065 og tilleggskrav fastsatt av tilsynsmyndigheten og/eller av Personvernrådet. For mer informasjon om tolkningen av akkreditering i henhold til personvernforordningen artikkel 42 og 43, se kapittel 3 i Personvernrådets retningslinjer for akkreditering.

Akkrediteringsorgan: Organet som akkrediterer sertifiseringsorganer. I dette dokumentet menes Norsk akkreditering ved bruk av begrepet. Hvis Datatilsynet på noe tidspunkt velger å benytte sin kompetanse til å gi akkreditering, menes Datatilsynet ved bruk av begrepet.

Berørt tilsynsmyndighet: En berørt tilsynsmyndighet, som definert i personvernforordningen artikkel 4 nr. 22.

Evaluering: Sertifiseringsorganets aktiviteter som innebærer en vurdering av hvorvidt sertifiseringsobjektet (evalueringsmålet) oppfyller de godkjente sertifiseringskriteriene.

ISO 17065: ISO/IEC 17065:2012.

Klient[3]: Virksomheten som har blitt sertifisert (tidligere søkeren).

Kompetent tilsynsmyndighet: Når det refereres til i dette dokumentet, betyr det Datatilsynet.

Nasjonalt akkrediteringsorgan: Det eneste organet i en medlemsstat utpekt i samsvar med Europaparlaments- og rådsforordning (EF) nr. 765/2008 av 9. juli 2008 om fastsettelse av kravene til akkreditering og markedstilsyn for markedsføring av produkter, og om oppheving av forordning (EØF) nr. 339/93, som utfører akkreditering med myndighet avledet fra medlemsstaten. I Norge er det nasjonale akkrediteringsorganet Norsk akkreditering (NA).

Personopplysningsloven: Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Personvernforordning: Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, og om oppheving av direktiv 95/46/EF.

Personvernrådets retningslinjer for akkreditering: EDPB Retningslinjer 4/2018 om akkreditering av sertifiseringsorganer i henhold til personvernforordningen artikkel 43 (2016/679).

[3] Når begreper «klient» brukes i den internasjonale standarden ISO/IEC 17065/2012, gjelder det både for «søker» og «klient», med mindre annet er spesifisert.

Personvernrådets retningslinjer for sertifisering: EDPB Retningslinjer 1/2018 om sertifisering og identifisering av sertifiseringskriterier i henhold til personvernforordningen artikkel 42 og 43.

Sertifisering: Vurdering og bekreftelse fra en uavhengig tredjepart på at oppfyllelse av sertifiseringskriteriene er påvist med hensyn til en eller flere behandlingsaktiviteter til en behandlingsansvarlig eller databehandler.

Sertifiseringskriterier: Kriteriene i en gitt sertifiseringsordning som en sertifisering utføres etter for en virksomhets behandlingsaktiviteter.

Sertifiseringsmekanisme: En godkjent sertifiseringsordning, som er tilgjengelig for søkeren. Det er en tjeneste som tilbys av et akkreditert sertifiseringsorgan basert på godkjente kriterier og evalueringsmetoder. Det er systemet der en behandlingsansvarlig eller databehandler blir sertifisert.

Sertifiseringsobjektet eller evalueringsmålet: Objektet for sertifisering. Ved sertifisering etter personvernforordningen, vil dette være den eller de relevante behandlingsaktivitetene som den behandlingsansvarlige eller databehandleren søker om å få evaluert og sertifisert.

Sertifiseringsordning: Et sertifiseringssystem for bestemte produkter, prosesser og tjenester som er underlagt de samme spesifikke kravene, reglene og prosedyrene. Det inkluderer sertifiseringskriterier og evalueringsmetoder.

Sertifiseringsorgan: Et tredjeparts samsvarsvurderingsorgan som bruker en sertifiseringsordning.

Søker: Virksomheten som har søkt om å få behandlingsaktivitetene sine sertifisert. Vanligvis en behandlingsansvarlig som utfører behandlingsaktiviteter eller en databehandler som tilbyr evaluerte produkter og tjenester for databehandling.

4 Generelle krav til akkreditering

4.1 Juridiske og kontraktsfestede anliggender

4.1.1 Juridisk ansvar

Et sertifiseringsorgan må (til enhver tid) kunne dokumentere overfor akkrediteringsorganet at de har oppdaterte prosedyrer som påviser etterlevelse av rettslige forpliktelser fastsatt i akkrediteringsvilkårene, herunder tilleggskravene med hensyn til anvendelsen av personvernforordningen.

Sertifiseringsorganet må kunne påvise at dets prosedyrer og tiltak som spesifikt angår kontroll og håndtering av søker- og klientvirksomheters personopplysninger, som en del av sertifiseringsprosessen, er i samsvar med personvernforordningen og personopplysningsloven. Sertifiseringsorganet må derfor fremlegge etterlevelsesdokumentasjon som kreves under akkrediteringsprosessen.

Dette inkluderer at sertifiseringsorganet skal bekrefte overfor akkrediteringsorganet at de ikke er gjenstand for tilsyn – og ikke tidligere har vært gjenstand for regulatoriske tiltak – fra Datatilsynet i medhold av personvernforordningen eller personopplysningsloven, som kan innebære at de ikke oppfyller ovennevnte krav, og som dermed kan hindre akkreditering. Før akkrediteringsprosessen fortsetter, kan akkrediteringsorganet kontakte Datatilsynet for å verifisere denne informasjonen. Datatilsynet vil verifisere informasjonen der det er hensiktsmessig.

Sertifiseringsorganet skal også bekrefte overfor akkrediteringsorganet at de ikke er gjenstand for undersøkelser – og at de ikke tidligere har vært gjenstand for regulatoriske tiltak fra tilsynsmyndigheter i andre områder, dersom disse undersøkelsene eller tiltakene gjelder behandling av personopplysninger og kan føre til at sertifiseringsorganet ikke oppfyller ovennevnte krav, og som dermed kan hindre akkreditering.

Sertifiseringsorganet skal umiddelbart underrette akkrediteringsorganet om relevante overtredelser av personvernforordningen eller personopplysningsloven konstatert av Datatilsynet, tilsynsmyndigheter i andre områder, eller kompetente rettsmyndigheter som kan påvirke akkrediteringen.

Før sertifiseringen utstedes eller fornyes, skal sertifiseringsorganet underrette Datatilsynet, jf. personvernforordningen artikkel 43 nr. 1.

Før akkrediteringen utføres kan Datatilsynet beslutte å legge til ytterligere krav og prosedyrer for å kontrollere sertifiseringsorganets etterlevelse av personvernforordningen.

4.1.2 Sertifiseringsavtale

Sertifiseringsorganet må, i tillegg til kravene i punkt 4.1.2.1 i ISO 17065, dokumentere at sertifiseringsavtalen:

1. krever at søkeren alltid overholder både de generelle sertifiseringskravene i punkt 4.1.2.2 bokstav a i ISO 17065, og kriteriene godkjent av Datatilsynet eller Personvernrådet, jf. personvernforordningen artikkel 43 nr. 2 bokstav b og artikkel 42 nr. 5
2. krever at søkeren har full åpenhet overfor Datatilsynet med hensyn til sertifiseringsprosessen, inkludert eventuelt konfidensielt materiale, enten det er kontraktsfestet eller lovfestet, knyttet til etterlevelse av

personvernregelverket i henhold til personvernforordningen artikkel 42 nr. 7 og artikkel 58 nr. 1 bokstav c

3. ikke reduserer søkerens ansvar for overholdelse av personvernforordningen, og ikke berører oppgaver og myndighet til vedkommende tilsynsmyndighet, jf. personvernforordningen artikkel 42 nr. 5
4. krever at søkeren gir sertifiseringsorganet alle opplysninger og tilgang til alle behandlingsaktivitetene som er nødvendig for å gjennomføre sertifiseringsprosessen, jf. personvernforordningen artikkel 42 nr. 6
5. krever at søkeren overholder gjeldende frister og prosedyrer – sertifiseringsavtalen må fastsette at frister og prosedyrer, for eksempel fra sertifiseringsordningen, eller andre forskrifter, skal overholdes
6. med hensyn til punkt 4.1.2.2 bokstav c nr. 1 i ISO 17065, angir regler for gyldighet, fornyelse og tilbaketrekking i henhold til personvernforordningen artikkel 42 nr. 7 og artikkel 43 nr. 4, herunder regler som fastsetter passende intervaller for revurdering eller gjennomgang (regelmessighet), jf. personvernforordningen artikkel 42 nr. 7 og punkt 7.9 i dette dokumentet
7. tillater sertifiseringsorganet å opplyse Datatilsynet om begrunnelsen til innvilgelse eller tilbaketrekking av sertifiseringen, jf. personvernforordningen artikkel 43 nr. 5, og den informasjonen Datatilsynet trenger å gi Personvernrådet for at de skal kunne inkludere sertifiseringsmekanismen i et offentlig tilgjengelig register, jf. personvernforordningen artikkel 42 nr.8
8. inneholder nødvendige forholdsregler for å undersøke klager i henhold til punkt 4.1.2.2 bokstav c nr. 2 og bokstav j i ISO 17065, på en åpen og lett tilgjengelig måte, som også skal inneholde eksplisitte uttalelser om strukturen og prosedyren for klagebehandling i samsvar med personvernforordningen artikkel 43 nr. 2 bokstav d
9. inneholder, i tillegg til minstekravene nevnt i punkt 4.1.2.2 i ISO 17065, en beskrivelse av konsekvensene for sertifiseringsorganet ved tilbaketrekking eller suspensjon av akkrediteringen, og hvordan dette påvirker klienten. I så fall skal konsekvensene for klienten og eventuelle videre skritt som kan tas, også håndteres ved å inkludere hensiktsmessige prosedyrer i sertifiseringsorganets styringssystem
10. krever at søkeren underretter sertifiseringsorganet ved vesentlige endringer i dens faktiske eller juridiske situasjon og i dets produkter, prosesser og tjenester som berøres av sertifiseringen
11. inkluderer bindende evalueringsmetoder med hensyn til sertifiseringsobjektet
12. krever at søkeren underretter sertifiseringsorganet om eventuelle overtredelser av personvernforordningen konstatert av Datatilsynet og/eller annen rettsmyndighet som kan påvirke sertifiseringen

4.1.3 Bruk av personvernsertifikater, -segl og -merker

Sertifikater, segl og merker skal kun brukes i henhold til personvernforordningen artikkel 42 og 43, Personvernrådets retningslinjer for akkreditering og Personvernrådets retningslinjer for sertifisering.

4.2 Styring av upartiskhet

Akkrediteringsorganet må sikre, i tillegg til å oppfylle kravene i punkt 4.2 i ISO 17065:

1. at sertifiseringsorganet oppfyller tilleggskravene fastsatt av Datatilsynet (i henhold til personvernforordningen artikkel 43 nr. 1 bokstav b) ved
    a. å gi separat bevis på egen uavhengighet, jf. personvernforordningen artikkel 43 nr. 2 bokstav a – dette gjelder særlig bevis angående finansieringen av sertifiseringsorganet i den grad det gjelder sikring av uavhengighet

   b. å ha klare regler på plass for å identifisere og håndtere potensielle interessekonflikter, og sikre at oppgavene og pliktene sine ikke fører til interessekonflikter i henhold til personvernforordningen artikkel 43 nr. 2 bokstav e
2. at sertifiseringsorganet ikke har en relevant tilknytning til klienten de vurderer - for eksempel:
   a. Enhver form for økonomisk relasjon mellom sertifiseringsorganet og klienten, avhengig av dets egenskaper, som kan påvirke upartiskheten til sertifiseringsorganets sertifiseringsaktiviteter.
   b. Sertifiseringsorganet kan ikke tilhøre samme konsern/juridisk enhet som klienten det vurderer.
   c. Sertifiseringsorganet kan ikke på noen måte kontrolleres av klienten det vurderer.
   d. Sertifiseringsorganet kan ikke være i en relasjon som behandlingsansvarlig/databehandler overfor klienten det vurderer.

4.3 Erstatningsansvar og finansiering

I tillegg til kravene i punkt 4.3.1 i ISO 17065, skal sertifiseringsorganet påvise regelmessig (dvs. én gang i året) overfor akkrediteringsorganet at de har egnede ordninger (f.eks. forsikring og/eller reserver) for å dekke sine forpliktelser i de geografiske områdene de opererer i.

Videre skal sertifiseringsorganet påvise økonomisk stabilitet og uavhengighet. Akkrediteringsorganet avgjør etter eget skjønn hvilke støttedokumenter som kreves.

4.4 Ikke-diskriminerende forhold

Kravene i punkt 4.4 i ISO 17065 gjelder.

4.5 Konfidensialitet

Kravene i punkt 4.5 i ISO 17065 gjelder.

4.6 Offentlig tilgjengelig informasjon

I tillegg til kravene i punkt 4.6 i ISO 17065, skal akkrediteringsorganet som et minimum kreve følgende fra sertifiseringsorganet:

1. At alle versjoner (nåværende og tidligere) av de godkjente sertifiseringskriteriene som brukes i henhold til personvernforordningen artikkel 42 nr. 5 publiseres og gjøres offentlig og lett tilgjengelige. Dette gjelder også alle sertifiseringsprosedyrer, som vanligvis angir den respektive gyldighetsperioden, herunder at sertifiseringskriteriene eventuelt er godkjent av EDPB.
2. At informasjon om prosedyrer for klagebehandling og anker offentliggjøres i henhold til personvernforordningen artikkel 43 nr. 2 bokstav d.

5 Strukturelle krav, personvernforordningen artikkel 43 nr. 4 [«egnet vurdering»]

5.1 Organisasjonsstruktur og øverste ledelse

Kravene i punkt 5.1 i ISO 17065 gjelder.

5.2 Mekanismer for å sikre upartiskhet

Kravene i punkt 5.2 i ISO 17065 gjelder.

6 Krav til ressurser

6.1 Personell hos sertifiseringsorganet

Det forventes, på grunn av bestemmelsene i personvernforordningen som spesifiserer elementene i personvernsertifiseringen, at både juridisk og teknisk personell vil måtte involveres i vurdering eller evaluering og beslutningstaking foretatt av sertifiseringsorganet. Dette skal gjøres i tråd med sertifiseringsordningen og er avhengig av sertifiseringsobjektet eller behandlingen som skal sertifiseres.

I tillegg til kravene i punkt 6 i ISO 17065, skal akkrediteringsorganet sikre for hvert sertifiseringsorgan at dets personell som utfører sertifiseringssamsvarsoppgaver:

1. har relevant og vedvarende ekspertise (kunnskap og erfaring) med hensyn til vern av personopplysninger i henhold til personvernforordningen artikkel 43 nr. 1, og knyttet til sertifiseringens innhold
2. har uavhengighet og vedvarende ekspertise med hensyn til sertifiseringens innhold i henhold til personvernforordningen artikkel 43 nr. 2 bokstav a, og har ikke en interessekonflikt i henhold til personvernforordningen artikkel 43 nr. 2 bokstav e
3. forplikter seg til å overholde sertifiseringskriteriene i personvernforordningen artikkel 42 nr. 5 i henhold til personvernforordningen artikkel 43 nr. 2 bokstav b
4. har relevant og passende kunnskap om og erfaring med anvendelse av personvernlovgivning
5. har påviselig, relevant og passende kunnskap om anvendelse av personvernlovgivning i forbindelse med sertifiseringens innhold
6. er i stand til å påvise erfaring fra de feltene som er nevnt i disse tilleggskravene, spesielt

   <u>For personell med teknisk ekspertise:</u>

   - Har enten oppnådd en kvalifikasjon i et relevant område med teknisk ekspertise til minst EQF[4] nivå 6, en anerkjent beskyttet tittel (f.eks. sivilingeniør) i det relevante regulerte yrket, eller har betydelig yrkeserfaring.
   - *Personell som er ansvarlig for sertifiseringsbeslutninger* må ha betydelig yrkeserfaring i personvernlovgivning, herunder identifisering og implementering av personverntiltak, eller tilgang til noen med den kompetansen, og en passende faglig/akademisk kvalifikasjon.
   - *Personell som er ansvarlig for evaluering* må ha relevant og nylig yrkeserfaring og kunnskap innen tekniske personvernspørsmål og erfaring med sammenlignbare prosedyrer (f.eks. sertifisering/revisjon), og passende faglige kvalifikasjoner der det er relevant.

   Personalet skal påvise at de opprettholder domenespesifikk kunnskap innen tekniske og revisjonsferdigheter gjennom kontinuerlig faglig utvikling.

   <u>For personell med juridisk ekspertise:</u>

   - Juridisk utdannelse ved et EU/EØS- eller statsanerkjent universitet i minst åtte semestre, inkludert den akademiske graden master i rettsvitenskap, eller tilsvarende.

4 Se sammenligningsverktøyet for kvalifikasjonsrammeverk på https://europa.eu/europass/en/compare-qualifications

- *Personell som er ansvarlig for sertifiseringsbeslutninger* må påvise betydelig yrkeserfaring innen personvernlovgivning, herunder identifisering og implementering av personverntiltak, eller tilgang til noen med den kompetansen, og en passende faglig/akademisk kvalifikasjon.
- *Personell som er ansvarlig for evaluering* må påvise minst to års yrkeserfaring innen personvernlovgivning, og kunnskap og erfaring innen tekniske personvernspørsmål og sammenlignbare prosedyrer (f.eks. sertifisering/revisjon), og passende faglige kvalifikasjoner der det er relevant.

Personalet skal påvise at de opprettholder domenespesifikk kunnskap innen revisjon og tekniske ferdigheter gjennom kontinuerlig faglig utvikling.

Sertifiseringsorganet må kunne definere og forklare til akkrediteringsorganet hvilke krav til yrkeserfaring som passer til omfanget av sertifiseringsordningen og det aktuelle sertifiseringsobjektet.

Når det gjelder kravene til personell med ansvar for sertifiseringsbeslutninger, vil sertifiseringsorganet beholde ansvar for beslutningstaking, selv om eksterne eksperter benyttes. Eksterne aktører skal ikke involveres i beslutningsprosessen.

Dersom evalueringsaktiviteter settes ut til eksterne organer, skal disse være underlagt samme vilkår som sertifiseringsorganet. Spesielt må de personvernrettslige kravene overholdes av underleverandør.

6.2 Evalueringsressurser

Kravene i punkt 6.2 i ISO 17065 gjelder.

7 Prosesskrav

7.1 Generelt

I tillegg til kravene i punkt 7.1 i ISO 17065 skal akkrediteringsorganet sikre følgende:

1. Sertifiseringsorganet oppfyller tilleggskravene fastsatt av Datatilsynet, jf. personvernforordningen artikkel 43 nr. 1 bokstav b, ved innsending av søknaden, slik at oppgaver og plikter ikke fører til en interessekonflikt, jf. personvernforordningen artikkel 43 nr. 2 bokstav e.
2. Datatilsynet og andre berørte tilsynsmyndigheter blir underrettet før et sertifiseringsorgan begynner å bruke et godkjent europeisk personvernsegl fra en etablering eller et kontor i en ny EØS-medlemsstat.[5]
3. Sertifiseringsorganet har prosedyrer på plass for å underrette Datatilsynet umiddelbart før utstedelse, fornyelse, tilbaketrekking eller avvisning av en sertifisering, og for å begrunne slike handlinger. Dette inkluderer å gi Datatilsynet en kopi av sammendraget av evalueringsrapporten, referert til i punkt 7.8 i dette dokumentet.
4. I tilfeller hvor klienten eller Datatilsynet underretter sertifiseringsorganene om vesentlige og relevante undersøkelser, etterforskninger, eller regulatoriske handlinger fra Datatilsynet eller annen tilsynsmyndighet i andre områder som setter spørsmålstegn ved klientens overholdelse av personvernregelverket, skal sertifiseringsorganet foreta en vurdering av hvorvidt klienten fortsatt oppfyller sertifiseringskriteriene. Sertifiseringsorganet skal gi Datatilsynet en rapport om utfallet av denne vurderingen. Vurderingen skal knyttes til omfanget av sertifisering og sertifiseringsobjektet.

7.2 Søknad

I tillegg til kravene i punkt 7.2 i ISO 17065, skal sertifiseringsorganet kreve at søknaden

1. inneholder en detaljert beskrivelse av sertifiseringsobjektet – dette inkluderer også grensesnitt og overføringer til andre systemer og virksomheter, protokoller og andre garantier
2. spesifisere hvorvidt databehandlere benyttes – når en databehandler er søkeren skal dets ansvar og oppgaver beskrives, og søknaden skal inneholde relevant(e) avtal(er) mellom den behandlingsansvarlige og databehandler
3. spesifisere om felles behandlingsansvarlige er involvert i behandlingen, og hvis den felles behandlingsansvarlige er søkeren, skal dets ansvar og oppgaver beskrives, og avtalen skal legges ved søknaden
4. fremlegge informasjon om eventuelle nåværende eller nylige undersøkelser, etterforskninger eller regulatoriske handlinger fra Datatilsynet eller tilsynsmyndigheter i andre områder som søkeren er underlagt, hvis disse undersøkelsene, etterforskninger eller regulatoriske handlinger gjelder behandling av personopplysninger relatert til omfanget av sertifiseringen og sertifiseringsobjektet
5. i tilfelle overføring av personopplysninger til tredjeland eller en internasjonal organisasjon, inneholder en spesifisering av de overførte personopplysningene, mottakerne av personopplysningene, spesifisering av mottakerland og spesifisering av de angitte personverngarantiene

5 I denne forbindelse, se avsnitt 44 i Personvernrådet sin retningslinje for sertifisering.

7.3 Gjennomgåelse av søknad

I tillegg til kravene i punkt 7.3 i ISO 17065, skal akkrediteringsorganet kreve

1. at bindende evalueringsmetoder med hensyn til sertifiseringsobjektet er nedfelt i sertifiseringsavtalen
2. at vurderingen, nevnt i punkt 7.3.1 bokstav e i ISO 17065, av om det er tilstrekkelig ekspertise, tar hensyn til både teknisk og juridisk ekspertise innen personvern i et passende omfang
3. at søknadsgjennomgangen tar hensyn til overholdelse av personvernkravene referert til i punkt 7.2 i dette dokumentet – sertifiseringsorganet pålegges å sikre at søkeren er en egnet kandidat for personvernsertifisering

7.4 Evaluering

I tillegg til kravene i punkt 7.4 i ISO 17065, skal sertifiseringsmekanismen beskrive tilstrekkelige evalueringsmetoder for å vurdere om behandlingsoperasjonen(e) samsvarer med sertifiseringskriteriene, herunder:

1. en metode for å vurdere nødvendigheten og forholdsmessigheten av behandlingsaktiviteter i forhold til deres formål og de berørte registrerte
2. en metode for å evaluere dekning, sammensetning og vurdering av alle risikoer vurdert av den behandlingsansvarlige og databehandleren med hensyn til de rettslige konsekvensene etter personvernforordningen artikkel 30, 32, 35 og 36, og med hensyn til definisjonen av tekniske og organisatoriske tiltak etter artikkel 24, 25 og 26, i den grad de nevnte artiklene gjelder for sertifiseringsobjektet
3. en metode for å vurdere rettsmidler, inkludert garantier, sikkerhetstiltak og prosedyrer for å sikre beskyttelse av personopplysninger i forbindelse med behandlingen som skal tilskrives sertifiseringsobjektet og for å påvise at de rettslige kravene fastsatt i sertifiseringskriteriene overholdes
4. dokumentasjon av metoder og resultater

Sertifiseringsorganet skal pålegges å sikre at disse evalueringsmetodene er standardiserte og brukes konsekvent. Dette betyr at sammenlignbare evalueringsmetoder brukes på sammenlignbare sertifiseringsobjekter. Ethvert avvik fra denne fremgangsmåten må begrunnes av sertifiseringsorganet.

I tillegg til kravene i punkt 7.4.2 i ISO 17065, kan evalueringen utføres av underleverandører som er anerkjent av sertifiseringsorganet og som anvender de samme personellkravene i kapittel punkt 6 i dette dokumentet. Dersom evalueringen utføres av en underleverandør må underleverandøren overholde de respektive kravene i ISO 17065, samt Datatilsynets tilleggskrav. Bruk av underleverandører fritar ikke sertifiseringsorganet fra dets ansvar.

I tillegg til kravene i punkt 7.4.5 i ISO 17065, skal det sørges for at eksisterende sertifiseringer i henhold til personvernforordningen artikkel 42 og 43, som relateres til samme sertifiseringsobjekt, kan tas i betraktning som en del av en ny vurdering. Sertifikatet alene vil imidlertid ikke være tilstrekkelig bevis, og sertifiseringsorganet er forpliktet til å kontrollere samsvar med sertifiseringskriteriene med hensyn til sertifiseringsobjektet. Den fullstendige evalueringsrapporten og annen relevant informasjon som muliggjør

evaluering av den eksisterende sertifiseringen og dens resultater skal vurderes for å kunne ta en informert beslutning.

I tilfeller der eksisterende sertifiseringer tas i betraktning som del av en ny evaluering, bør omfanget av slik sertifisering også vurderes i detalj med hensyn til overholdelse av de relevante sertifiseringskriteriene.

I tillegg til kravene i punkt 7.4.6 i ISO 17065, skal det kreves at sertifiseringsorganet skal angi i detalj i sin sertifiseringsordning hvordan informasjonen som kreves i punkt 7.4.6 i ISO 17065 opplyser søkeren om avvik med den. I denne sammenheng skal i det minste arten og tidspunktet for slik informasjon defineres. Dette gjelder kun for sertifiseringsorganer som også er eieren av sertifiseringsordningen. Sertifiseringsorganet skal angi dette i et skriftlig dokument som enten kan være sertifiseringsordningen, eller dersom sertifiseringsorganet ikke er eieren av sertifiseringsordningen, et annet dokument knyttet til sertifiseringsprosessen.

I tillegg til kravene i punkt 7.4.9 i ISO 17065, skal det kreves at evalueringsdokumentasjonen er fullt tilgjengelig for Datatilsynet på forespørsel.

7.5 Gjennomgåelse

I tillegg til kravene i punkt 7.5 i ISO 17065, kreves det prosedyrer for utstedelse, regelmessig gjennomgåelse og tilbaketrekking av de respektive sertifiseringene, jf. personvernforordningen artikkel 43 nr. 2 og 43 nr. 3.

7.6 Sertifiseringsbeslutning

I tillegg til kravene i punkt 7.6.1 i ISO 17065, skal sertifiseringsorganet angi i detalj i sine prosedyrer hvordan dets uavhengighet og ansvar med hensyn til individuelle sertifiseringsbeslutninger er sikret.

I tillegg til kravene i punkt 7.6.2 i ISO 17065, skal sertifiseringsorganet umiddelbart før utstedelse eller fornyelse av sertifisering, sende inn utkast til den positive sertifiseringsbeslutningen, inkludert sammendraget av evalueringsrapporten til Datatilsynet. Sammendraget skal tydelig beskrive hvordan kriteriene oppfylles, og dermed gi begrunnelse for utstedelse eller fornyelse av sertifiseringen. Hensikten med dette kravet er økt åpenhet og kravet innebærer ikke et tilsyn av utkast til den positive sertifiseringsbeslutningen.

I tillegg til kontrollen utført på søknadsstadiet, skal sertifiseringsorganet – før utstedelse av sertifisering – være pålagt å bekrefte overfor søkeren at de ikke er gjenstand for undersøkelse, etterforskning eller regulatoriske tiltak fra Datatilsynet i relasjon til sertifiseringsobjektet som kan forhindre at sertifisering utstedes. Datatilsynet kan bekrefte hvorvidt dette er tilfelle før sertifiseringsorganet utsteder eller fornyer sertifiseringen. Dersom det oppdages at søkeren ikke har opplyst om slike forhold til sertifiseringsorganet, kan dette føre til at sertifiseringen ikke blir utstedt.

I tillegg til kravene i punkt 7.6.6 i ISO 17065, skal sertifiseringsorganet angi hvor, hvordan og når søkeren kan klage på sertifiseringsorganets beslutning om ikke å utstede sertifisering, eller søke om overprøving av dette vedtaket.

7.7 Sertifiseringsdokumentasjon

I tillegg til kravene i punkt 7.7.1 bokstav e i ISO 17065, og i henhold til personvernforordningen artikkel 42 nr. 7, skal gyldighetsperioden for sertifiseringer ikke overstige tre år.

I tillegg til kravene i punkt 7.7.1 bokstav e i ISO 17065, skal det kreves at perioden for tiltenkt overvåking i henhold til punkt 7.9 dokumenteres.

I tillegg til kravene i punkt 7.7.1 bokstav f i ISO 17065, skal sertifiseringsorganet være pålagt å navngi sertifiseringsobjektet i sertifiseringsdokumentasjonen (med angivelse av versjonsstatus eller lignende egenskaper, hvis aktuelt).

Ved utstedelse av sertifikatet skal sertifiseringsorganet gi Datatilsynet en kopi av sertifiseringsdokumentasjonen nevnt i 7.7.1 i ISO 17065.

7.8 Register over sertifiserte produkter

I tillegg til kravene i punkt 7.8 i ISO 17065, skal sertifiseringsorganet være pålagt å holde informasjonen om sertifiserte produkter, prosesser og tjenester tilgjengelig internt og offentlig.

Sertifiseringsorganet skal offentliggjøre et sammendrag av evalueringsrapporten. Målet med dette sammendraget er å bidra til åpenhet rundt hva som er sertifisert og hvordan det ble vurdert. Det vil forklare forhold som:

a) omfanget av sertifiseringen og en meningsfull beskrivelse av sertifiseringsobjektet
b) de respektive sertifiseringskriteriene (inkludert versjon eller funksjonsstatus)
c) evalueringsmetoder og utførte tester
d) resultatene
e) dato for utstedelse og utløp av den nåværende sertifiseringen
f) dato for den første sertifiseringen og alle re-sertifiseringsdatoene

I tillegg til kravene i punkt 7.8 i ISO 17065, og i henhold til personvernforordningen artikkel 43 nr. 5, skal sertifiseringsorganet underrette Datatilsynet skriftlig om begrunnelsene for utstedelse eller tilbaketrekking av sertifiseringen.

7.9 Overvåking

I tillegg til kravene i punkt 7.9.1, 7.9.2 og 7.9.3 i ISO 17065, og i henhold til personvernforordningen artikkel 43 nr. 2 bokstav c, skal det kreves at regelmessige overvåkingstiltak er obligatoriske for å opprettholde sertifiseringen i overvåkingsperioden. Slike tiltak skal være risikobaserte og forholdsmessige, og den maksimale perioden mellom overvåkingsaktiviteter skal ikke overstige 12 måneder.

7.10 Endringer med innvirkning på sertifisering

I tillegg til kravene i punkt 7.10.1 og 7.10.2 i ISO 17065, skal endringer som påvirker sertifiseringen, og som skal vurderes av sertifiseringsorganet, omfatte:

- ethvert brudd på personopplysningssikkerheten, eller brudd personvernforordningen eller personopplysningsloven som er fastslått av Datatilsynet, tilsynsmyndigheter i andre områder og/eller rettsmyndigheter som relateres til sertifiseringen, rapportert av klienten eller Datatilsynet
- endringer i den teknologiske utvikling (så langt det er relevant for fremtidig sertifisering og overvåking)
- endringer i personvernlovgivningen
- vedtakelse av delegerte rettsakter fra Europakommisjonen i samsvar med personvernforordningen artikkel 43 nr. 8 og 43 nr. 9
- beslutninger, uttalelser, retningslinjer, anbefalinger, beste praksis eller andre dokumenter vedtatt av Personvernrådet
- rettsavgjørelser knyttet til personvern

Endringsprosedyrene som skal implementeres av sertifiseringsorganet skal omfatte: overgangsperioder, godkjenningsprosess med Datatilsynet, revurdering av det aktuelle sertifiseringsobjektet, og passende tiltak for å tilbaketrekke sertifiseringen dersom den sertifiserte behandlingsoperasjonen ikke lenger samsvarer med de oppdaterte sertifiseringskriteriene.

7.11 Oppheving, reduksjon, suspensjon eller tilbaketrekking av sertifisering

I tillegg til kravene i punkt 7.11.1 i ISO 17065, og punkt 7.1 nr. 3 i dette dokumentet, skal sertifiseringsorganet være pålagt å underrette Datatilsynet og akkrediteringsorganet skriftlig og umiddelbart der det er relevant, om iverksetting av tiltak og om videreføring, restriksjoner, suspensjon og tilbaketrekking av sertifisering.

I tilfeller hvor sertifiseringsorganet fastslår manglende etterlevelse, må de fastsette hvilke tiltak som skal iverksettes.

I henhold til personvernforordningen artikkel 58 nr. 2 bokstav h skal sertifiseringsorganet være pålagt å akseptere vedtak og pålegg fra Datatilsynet om å trekke tilbake eller ikke utstede sertifisering til en klient (søker) dersom kravene til sertifisering ikke er oppfylt. Sertifiseringsorganet skal i slike tilfeller fremlegge klare og dokumenterte bevis overfor Datatilsynet om at forsvarlige tiltak er iverksatt.

7.12 Registreringer

I tillegg til kravene i ISO 17065, er sertifiseringsorganet pålagt å holde all dokumentasjon komplett, forståelig, oppdatert og egnet for revisjon.

7.13 Klager og anker, Artikkel 43 nr. 2 bokstav d

I tillegg til kravene i punkt 7.13.1 i ISO 17065, skal sertifiseringsorganet fastsette

a. hvem som kan fremme klager eller innvendinger
b. hvem i sertifiseringsorganet som behandler dem
c. hvilke kontroller som finner sted i denne sammenheng
d. mulighetene for konsultasjon av interesserte parter

I tillegg til kravene i punkt 7.13.2 i ISO 17065, skal sertifiseringsorganet fastsette

a) hvordan og til hvem slik bekreftelse skal gis
b) tidsfristen for dette
c) hvilke prosesser som skal settes i gang i etterkant

I tillegg til kravene i punkt 7.13.7 og 7.13.8 i ISO 17065, skal sertifiseringsorganet fastsette rimelige frister for å informere klagerne om fremdriften, resultatet og avslutning av klageprosessen.

Sertifiseringsorganer skal gjøre sine klagebehandlingsprosedyrer offentlig tilgjengelige og lett tilgjengelige for de registrerte.

Sertifiseringsorganet skal underrette klageren om fremdriften og utfallet av klagen innen rimelig tid.

I tillegg til kravene i punkt 7.13.1 i ISO 17065, skal sertifiseringsorganet fastsette hvordan skillet mellom sertifiseringsaktiviteter og behandling av klager og anker sikres.

8 Krav til styringssystemer

Et generelt krav til styringssystemet i henhold til punkt 8 i ISO 17065, er at sertifiseringsorganets implementering av alle krav fra de foregående punktene, innenfor rammen av anvendelsen av sertifiseringsmekanismen, er dokumentert, evaluert, kontrollert og overvåket på en uavhengig måte.

Det grunnleggende prinsippet for styring er å fastsette et system hvor målene er virkningsfulle og effektive, nærmere bestemt: implementering av sertifiseringstjenestene ved hjelp av passende spesifikasjoner. Dette krever åpenhet og etterprøvbarhet av sertifiseringsorganets implementering av akkrediteringskravene og kontinuerlig overholdelse.

For dette formål må styringssystemet spesifisere en metodikk for å oppnå og kontrollere at disse kravene er i samsvar med personvernregelverket og for kontinuerlig å kontrollere dette med det akkrediterte sertifiseringsorganet selv.

I tillegg til kravene i punkt 8 i ISO 17065, skal styringsprinsippene og deres dokumenterte implementering være åpen og offentliggjøres av det akkrediterte sertifiseringsorganet på forespørsel fra Datatilsynet til enhver tid under en undersøkelse i form av personvernrevisjoner i henhold til personvernforordningen artikkel 58 nr. 1 bokstav b, eller en gjennomgang av sertifiseringene utstedt i samsvar med personvernforordningen artikkel 42 nr. 7, jf. artikkel 58 nr. 1 bokstav c.

Spesielt må det akkrediterte sertifiseringsorganet offentliggjøre permanent og fortløpende hvilke sertifiseringer som ble utført på hvilket grunnlag (eller sertifiseringsmekanismer eller -ordninger), samt hvor lenge sertifiseringene er gyldige, og under hvilke rammer og betingelser (se personvernforordningen fortalepunkt 100).

Prosedyrene ved suspensjon eller tilbaketrekking av akkrediteringen skal integreres i sertifiseringsorganets styringssystem, inkludert underretning til dets klienter.

En klagebehandlingsprosess med nødvendige nivåer av uavhengighet skal etableres av sertifiseringsorganet som en integrert del av styringssystemet, som særlig skal implementere kravene i punkt 4.1.2.2 bokstav c, 4.1.2.2 bokstav j, 4.6 bokstav d og 7.13 i ISO 17065. Relevante klager og innsigelser skal deles med Datatilsynet.

8.1 Generelle krav til styringssystemer

Kravene i punkt 8.1 i ISO 17065 gjelder.

8.2 Generell dokumentasjon for styringssystemer

Kravene i punkt 8.2 i ISO 17065 gjelder.

8.3 Styring av dokumenter

Kravene i punkt 8.3 i ISO 17065 gjelder.

8.4 Styring av registreringer

Kravene i punkt 8.4 i ISO 17065 gjelder.

8.5 Ledelsens gjennomgåelse

Kravene i punkt 8.5 i ISO 17065 gjelder.

8.6 Interne revisjoner

Kravene i punkt 8.6 i ISO 17065 gjelder.

8.7 Korrigerende tiltak

Kravene i punkt 8.7 i ISO 17065 gjelder.

8.8 Forebyggende tiltak

Kravene i punkt 8.8 i ISO 17065 gjelder.

9 Ytterligere tilleggskrav

9.1 Oppdatering av evalueringsmetoder

Sertifiseringsorganet skal etablere prosedyrer for å oppdatere evalueringsmetoder for anvendelse i forbindelse med evalueringen under punkt 7.4 i ISO 17065 og dette dokumentet. Oppdateringer må skje i takt med endringer i det juridiske rammeverket, aktuelle risikoer, i den teknologiske utviklingen og i implementeringskostnadene ved tekniske og organisatoriske tiltak.

9.2 Opprettholdelse av kompetanse

Sertifiseringsorganet skal etablere prosedyrer for å sikre opplæring av sine ansatte med sikte på å oppdatere deres kompetanse, med hensyn til endringene oppført i punkt 9.1 i dette dokumentet.

9.3 Plikter og kompetanse

9.3.1 Kommunikasjon mellom sertifiseringsorganet og dets klienter og søkere

Prosedyrer skal være på plass for å implementere hensiktsmessige fremgangsmåter og kommunikasjonsstrukturer mellom sertifiseringsorganet og dets klienter. Dette skal inkludere:

1. dokumentasjon av oppgavene og pliktene til det akkrediterte sertifiseringsorganet, for å
    a. svare på informasjonsforespørsler
    b. muliggjøre kontakt ved klage på en sertifisering
2. å ha en søknadsprosess for at
    a. informasjon om status for søknader kan gis; og
    b. Datatilsynet kan gjennomføre evalueringer med hensyn til deres
        i. tilbakemeldinger
        ii. vedtak

9.3.2 Dokumentasjon av evalueringsmetoder

Systemer skal være på plass for å implementere hensiktsmessige prosedyrer og kommunikasjonsstrukturer mellom sertifiseringsorganet og Datatilsynet. Dette inkluderer et rapporteringssystem for å informere Datatilsynet

- om søkerens opplysninger ved mottak av søknad for å gjøre det mulig for Datatilsynet å sjekke sine registre for søkerens etterlevelseshistorikk i henhold til punkt 7.6 i dette dokumentet
- om grunnene til at sertifisering utstedes, tilbaketrekkes eller avvises i henhold til personvernforordningen artikkel 43 nr. 5 – dette skal skje umiddelbart før utstedelse, fornyelse, suspensjon eller tilbaketrekking av sertifiseringer i henhold til punkt 7.1 nr. 3 i dette dokumentet.

9.3.3 Håndtering av klager

Det skal etableres en klagebehandlingsprosedyre som en integrert del av styringssystemet, som særlig skal implementere kravene i punkt 4.1.2.2 bokstav c, 4.1.2.2 bokstav j, 4.6 bokstav d og 7.13 i ISO 17065.

Relevante klager og innsigelser skal deles med Datatilsynet på forespørsel.

9.3.4 Håndtering av tilbaketrekking

Prosedyrene ved suspensjon eller tilbaketrekking av akkrediteringen skal integreres i sertifiseringsorganets styringssystem, inkludert underretting til klienter.

Besøksadresse:
Trelastgata 3, Oslo

Postadresse:
Postboks 458 Sentrum,
0105 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no