Beslut om krav för ackreditering av certifieringsorgan

Diarienummer:
IMY-2022-9835

Datum:
2024-08-14

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) fastställer, i enlighet med artikel 43.3 i dataskyddsförordningen,[1] de krav – utöver kraven enligt EN-ISO/IEC 17065:2012[2] – som Styrelsen för ackreditering och teknisk kontroll (Swedac) ska tillämpa vid ackreditering av certifieringsorgan, enligt artikel 43.1 i dataskyddsförordningen. Kraven framgår av bilagan till detta beslut.

Redogörelse för ärendet

Enligt artikel 42.1 i dataskyddsförordningen[3] ska medlemsstaterna, tillsynsmyndigheterna, Europeiska dataskyddsstyrelsen (EDPB) och Europeiska kommissionen uppmuntra införandet av certifieringsmekanismer för dataskydd och sigill samt märkningar för dataskydd som syftar till att visa att personuppgiftsansvariga eller personuppgiftsbiträdens behandling är förenlig med förordningen.

Enligt artikel 43.1 i dataskyddsförordningen ska ackrediterade certifieringsorgan utfärda och förnya certifieringar, i enlighet med kriterier som godkänts av behörig tillsynsmyndighet eller EDPB, enligt artikel 43.3 i dataskyddsförordningen. IMY är behörig tillsynsmyndighet för att godkänna certifieringskriterier som är avsedda att tillämpas i Sverige, enligt 3 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (kompletteringsförordningen).

Enligt 4 § kompletteringsförordningen är Swedac ensamt behörigt ackrediteringsorgan för ackreditering av certifieringsorgan enligt artikel 43.1 i dataskyddsförordningen. Ackreditering av certifieringsorgan, med stöd av artikel 43.1 i dataskyddsförordningen, ska ske i enlighet med ackrediteringsförordningen ((EU) 765/2008),[4] den europeiska standarden EN-ISO/IEC 17065:2012,[5], de krav som följer av Swedacs föreskrifter och allmänna råd (STAFS 2020:1) om ackreditering, samt de ytterligare krav som IMY fastställer enligt artikel 43.3 i dataskyddsförordningen. Vid fastställandet av ytterligare krav ska IMY beakta EDPB:s riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (ackrediteringsriktlinjerna).

Mot denna bakgrund utarbetade IMY ett utkast till krav för ackreditering av certifieringsorgan, i enlighet med artikel 43.1 b i dataskyddsförordningen och

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).
[2] Conformity assessment – Requirements for bodies certifying products, processes and services (EN-ISO/IEC 17065:2012).
[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).
[4] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EGT L 218 13.8.2008, s. 30) (ackrediteringsförordningen), ändrad genom Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 (EGT L 218 13.8.2008, s. 30).
[5] Conformity assessment – Requirements for bodies certifying products, processes and services (EN-ISO/IEC 17065:2012).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

ackrediteringsriktlinjerna. Utkastet anmäldes, i enlighet med artikel 64.1 c i dataskyddsförordningen, till EDPB för ett yttrande, enligt artikel 64.3.

EDPB yttrade sig den 23 maj 2024[6] och rekommenderade att IMY:

- preciserar kraven enligt p. 4.1.1.1 om att genomföra riskanalyser eller konsekvensbedömningar,
- ändrar kraven enligt p. 4.1.1.1, med följd att den sökande i samband med certifieringsavtalets undertecknande ska informeras om skyldigheten att på begäran ge behörig tillsynsmyndighet fullständig tillgång till dokumentation m.m., inbegripet sådan dokumentation som är konfidentiell,
- ändrar kraven enligt p. 4.1.1.2, med innebörden att en sökande alltid ska uppfylla de kriterier som godkänts av behörig tillsynsmyndighet eller EDPB, och som certifieringen prövas mot,
- inkluderar ett krav p. 4.1.2.2 om att den sökande ska informera certifieringsorganet om rättsliga eller faktiska ändringar som kan inverka på utvärderingsobjektet och efterlevnaden av kriterierna i certifieringsordningen, i synnerhet ändringar som direkt avser utvärderingsobjektet,
- lägger till ett krav i p 4.1.2.3 om att informationen, som certifieringsorganet ska ge till den sökande innan avtal tecknas, ska dokumenteras i certifieringsavtalet,
- lägger till ett krav enligt p. 4.1.2.3 om att den sökande ska informeras om att ett erhållande av ett certifikat inte påverkar efterlevnaden av dataskyddsförordningen eller den behöriga tillsynsmyndighetens uppgifter och befogenheter,
- klargör enligt p. 4.2.3 att certifieringsorganets uppgifter och skyldigheter inte får ge upphov till en intressekonflikt, enligt artikel 43.2 e i dataskyddsförordningen,
- lägger till ett krav enligt p. 4.2.3 om att certifieringsorganet inte får vara gemensamt personuppgiftsansvarig med den sökande,
- ändrar p. 4.2.3 om hur finansieringen av certifieringsorganet inverkar på dess oberoende,
- lägger till att kraven enligt p. 4.3.1 inte enbart ska gälla i de jurisdiktioner utan också i de geografiska områden där certifieringsorganet är verksamt,
- lägga till i p. 6.1.1.2 att personal med juridisk kompetens ska ha relevant och lämplig kunskap och expertis,
- ändrar kompetenskraven enligt p. 6.1.1.2, i enlighet med avsnitt 6.1 i bilagan till ackrediteringsriktlinjerna,
- lägger till ett krav, i p. 6.1.1.2, på *betydande* arbetslivserfarenhet för personal med teknisk kompetens,
- om lämpligt ersätter begreppet *revision* (på eng: *audit*) med begreppet *granskning* i p. 6.1.1.2,
- i p. 6.2.2 klargör att om certifieringsorganet använder underleverantörer, så kvarstår certifieringsorganets ansvar för beslutsfattandet,
- i p. 7.4.6 tydliggör kravet på certifieringsorgan att fastställa vilken typ av information som sökande ska få, om organet identifierar avvikelser under en utvärdering,
- ändrar p. 7.4.9, med följd att all dokumentation från utvärderingen ska tillgängliggöras för IMY, men *inte* för andra berörda tillsynsmyndigheter, på begäran,

[6] Opinion 10/2024 on the draft decision of the competent supervisory authority of Sweden regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR) (23.05.2024). Tillgänglig: https://www.edpb.europa.eu/system/files/2024-06/edpb_opinion_202410_se-sa_accreditationrequirements_certificationbodies_en_0.pdf (07.08.2024).

- ändrar p. 7.7.1, med följd att certifieringsorganet ska ange namnet på utvärderingsobjektet (personuppgiftsbehandlingen) i certifieringsdokumentationen,
- lägger till ett krav i p. 7.7.1 om att giltighetstiden för certifikat inte får överstiga tre år,
- ändrar p. 7.11.1 med följd att information till behörig tillsynsmyndighet ska skickas omedelbart,
- inkluderar, enligt avsnitt 8 i bilagan till ackrediteringsriktlinjerna, ett krav på att certifieringsorganets ledningssystem ska säkerställa att organet permanent och fortlöpande offentliggör information om vilka certifikat som utfärdats, i enlighet med vilken certifieringsmekanism och hur länge certifikaten gäller.

Med anledning av ovanstående rekommendationer ändrade IMY kraven och anmälde ett förnyat beslutsutkast till EDPB, enligt artikel 64.7 i dataskyddsförordningen. EDPB bekräftade mottagande av det förnyade beslutsutkastet och avslutade ärendet den 1 augusti 2024.[7]

Motivering av beslutet

Certifieringar, enligt artikel 42.5 i dataskyddsförordningen, är ett användbart verktyg för personuppgiftsansvariga och personuppgiftsbiträden när de ska visa efterlevnad av dataskyddsförordningens krav.[8] Kriterierna för att uppfylla en certifiering kan vara generella och avse hela eller stora delar av dataskyddsförordningens krav. De kan också vara specifika för vissa typer av personuppgiftsbehandlingar och innehålla mer specifika krav, exempelvis vad gäller tekniska och organisatoriska säkerhetsåtgärder. Det (eller de) objekt som utvärderas[9] i en certifiering enligt dataskyddsförordningen är personuppgiftsbehandlingar, inbegripet de processer och it-system som är nödvändiga för att genomföra en behandling.[10]

Som redogjorts för ovan ska certifieringar, enligt artikel 42.5 i dataskyddsförordningen, i Sverige utfärdas av ackrediterade certifieringsorgan. Ackrediteringen utförs av Swedac och den sker i enlighet med den europeiska standarden EN-ISO/IEC 17065:2012, som är en standard för organ som certifierar produkter, processer och tjänster. EN-ISO/IEC 17065:2012 är i grunden en global standard som införlivats i den europeiska standardiseringsordningen som en harmoniserad standard.[11] Därutöver tillkommer de krav som följer av ackrediteringsförordningen, STAFS 2020:1, samt de ytterligare krav som IMY ska fastställa, enligt artikel 43.3 i dataskyddsförordningen.

Om IMY inte fastställer några ytterligare krav, är det inte möjligt för Swedac att ackreditera certifieringsorgan och dessa organ kan då inte påbörja sin verksamhet i Sverige. Det är därför angeläget att IMY fastställer ytterligare krav för ackreditering av certifieringsorgan.

Som framgår ovan anmälde IMY ett utkast till ytterligare krav till EDPB för granskning och till följd av EDPB:s yttrande har kraven ändrats i vissa delar. I och med detta yttrande och de efterföljande ändringarna bedömer IMY att de ytterligare kraven har utformats i enlighet med artikel 43.3 i dataskyddsförordningen och

[7] Dnr IMY-2022-9835-30.
[8] Skäl 77 och artikel 24.3 i dataskyddsförordningen.
[9] På engelska *target of evaluation* (ToE).
[10] Certifieringsriktlinjerna, p. 50-51.
[11] Artikel 2.1 p. c) i Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering m.m. (EGT L 316 14.11.2012, s. 12); EN-ISO/IEC 17065:2012 är införlivad för svensk del som SS-EN-ISO/IEC 17065:2012.

ackrediteringsriktlinjerna. De ytterligare kraven för ackreditering av certifieringsorgan som framgår av bilagan ska därför fastställas.

Detta beslut har fattats av vikarierande generaldirektören David Törngren efter föredragning av juristen Cedric Voss. Vid den slutliga handläggningen har även tillförordnade rättschefen Cecilia Agnehall medverkat.

David Törngren, 2024-08-14 (Det här är en elektronisk signatur)

Bilaga

Ytterligare krav för ackreditering av certifieringsorgan

Bilaga – Ytterligare krav för ackreditering av certifieringsorgan

Innehållsförteckning

Förord

Enligt artikel 42.1 i dataskyddsförordningen[12] ska medlemsstaterna, tillsynsmyndigheterna, Europeiska dataskyddsstyrelsen (EDPB) och Europeiska kommissionen uppmuntra införandet av certifieringsmekanismer för dataskydd och sigill samt märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdes behandling av personuppgifter är förenlig med förordningen.

Enligt artikel 43.1 i dataskyddsförordningen ska ackrediterade certifieringsorgan utfärda och förnya certifieringar, i enlighet med kriterier som godkänts av behörig tillsynsmyndighet eller EDPB, enligt artikel 43.3 i dataskyddsförordningen. Integritetsskyddsmyndigheten (IMY) är behörig tillsynsmyndighet för att godkänna certifieringskriterier som är avsedda att tillämpas i Sverige, enligt 3 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (kompletteringsförordningen).

Enligt 4 § kompletteringsförordningen är Styrelsen för ackreditering och teknisk kontroll (Swedac) ensamt behörigt ackrediteringsorgan, för ackreditering av certifieringsorgan enligt artikel 43.1 i dataskyddsförordningen. Ackreditering av certifieringsorgan, med stöd av artikel 43.1 i dataskyddsförordningen, ska ske i enlighet med ackrediteringsförordningen ((EU) 765/2008),[13] EN-ISO/IEC 17065:2012,[14] de krav som följer av Swedacs föreskrifter och allmänna råd (STAFS 2020:1) om ackreditering, samt de ytterligare krav som IMY fastställer enligt artikel 43.3 i dataskyddsförordningen. I enlighet med artikel 7.3 i förordning (EG) 765/2008 får Swedac begära att ett annat nationellt ackrediteringsorgan utför delar av bedömningen, enligt artikel 43.1 b i dataskyddsförordningen.

Ett beslut om att bevilja eller förnya en ackreditering ska, i enlighet med artikel 43.4 i dataskyddsförordningen, inte sträcka sig längre än högst fem år.

Vid fastställandet av ytterligare krav ska IMY beakta EDPB:s riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (ackrediteringsriktlinjerna).

Formerna för samverkan mellan Swedac och IMY fastställs i en gemensam överenskommelse mellan myndigheterna.

[12] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).
[13] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EGT L 218 13.8.2008, s. 30) (ackrediteringsförordningen), ändrad genom Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 (EGT L 218 13.8.2008, s. 30).
[14] Conformity assessment – Requirements for bodies certifying products, processes and services (EN-ISO/IEC 17065:2012).

1 Tillämpningsområde

Kraven nedan utgör de ytterligare krav, utöver kraven enligt EN-ISO/IEC 17065:2012 och Swedacs föreskrifter och allmänna råd (2020:1), som certifieringsorgan ska uppfylla och som Swedac ska tillämpa i ackrediteringsförfarandet enligt artikel 43.1 i dataskyddsförordningen.

Ackrediteringen omfattar certifieringsorgans kvalifikationer för att utfärda certifiering av personuppgiftsbehandlingar, enligt artikel 42.5 i dataskyddsförordningen, med hänsyn till ett organs kompetens, varaktighet och oberoende, samt i förhållande till den certifieringsmekanism och det tillämpningsområde som ett organ ska tillämpa.

Swedac ska i ackrediteringsförfarandet särskilt beakta om tillämpningsområdet för den certifieringsmekanism som ett certifieringsorgan tillämpar inverkar på organets expertis eller utvärderingsmetoder.

2 Referenser

Följande rättsakter, riktlinjer och standarder ska beaktas vid tillämpningen av dessa ytterligare krav:[15]

EU:s allmänna dataskyddsförordning ((EU) 2016/679) (dataskyddsförordningen)

Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering m.m. (ackrediteringsförordningen)[16]

Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen)

Förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (kompletteringsförordningen)

Swedacs föreskrifter och allmänna råd (STAFS 2020:1) om ackreditering

Riktlinjer 4/2018 om ackreditering av certifieringsorgan enligt artikel 43 i allmänna dataskyddsförordningen (ackrediteringsriktlinjerna)

Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen (certifieringsriktlinjerna)

Conformity assessment – Requirements for bodies certifying products, processes and services (EN-ISO/IEC 17065:2012)

3 Termer och definitioner

Om det i kraven i detta beslut, EN-ISO/IEC 17065:2012 eller i certifieringsmekanismer hänvisas till andra internationella standarder, ska dessa standarder tolkas i enlighet med bestämmelserna i dataskyddsförordningen.

Därutöver används följande termer i detta beslut:

ackreditering

Intygande av ett nationellt ackrediteringsorgan, eller tillsynsmyndighet, att ett certifieringsorgan är behörigt, enligt artikel 43 i dataskyddsförordningen och i enlighet

[15] I händelse av konflikt ska dataskyddsförordningen ha företräde framför de kraven i detta beslut, kraven enligt EN-ISO/IEC 17065:2012 och kraven enligt aktuell certifieringsordning.
[16] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering m.m. (EGT L 218 13.8.2008, s. 30) (ackrediteringsförordningen) ändrad genom Europaparlamentets och rådets förordning (EU) 2019/1020 (EUT L 169, 25.6.2019, s. 1).

med EN-ISO/IEC 17065:2012 samt IMY:s ytterligare krav, att utfärda certifikat, enligt artikel 42.5 i dataskyddsförordningen.

ackrediteringsorgan

Det nationella ackrediteringsorgan som utsetts i enlighet med artikel 4.1 i ackrediteringsförordningen och som ackrediterar certifieringsorgan, enligt artikel 43.1 b) i dataskyddsförordningen. För svensk del avses Swedac.[17]

behörig tillsynsmyndighet

Avser Integritetsskyddsmyndigheten (IMY).

berörd tillsynsmyndighet

En annan tillsynsmyndighet än IMY, enligt artikel 4.22 i dataskyddsförordningen.

certifiering

En bedömning av ett kompetent och oberoende organ som intygar att en sökande uppfyller kriterierna i en certifieringsordning, enligt artikel 42.5 i dataskyddsförordningen.

certifieringskriterier

Krav som följer av en certifieringsordning och vars uppfyllnad är nödvändig för att en sökande ska kunna få ett certifikat, enligt artikel 42.5 i dataskyddsförordningen.

certifieringsorgan

Ett kompetent och i förhållande till den sökande oberoende organ som är ackrediterat, enligt artikel 43 i dataskyddsförordningen, och som bedömer om den sökande uppfyller kraven i en certifieringsordning, som är godkänd enligt artikel 42.5 i dataskyddsförordningen.

kund

En personuppgiftsansvarig eller ett personuppgiftsbiträde som uppfyllt kraven i en certifieringsordning och blivit certifierad av ett certifieringsorgan.

sökande
En personuppgiftsansvarig eller ett personuppgiftsbiträde som till ett certifieringsorgan ansöker om certifiering av en eller flera personuppgiftsbehandlingar, och som i förekommande fall erhåller en certifiering och blir en kund.

utvärderingsobjektet

En eller flera personuppgiftsbehandlingar, inbegripet berörda personuppgifter, tekniska system och processer och förfaranden som hänger samman med behandlingsåtgärder,18 och som kan bli föremål för certifiering, enligt artikel 42.5 i dataskyddsförordningen.

ytterligare och kompletterande krav

Ytterligare krav hänvisar till krav för certifieringsorgan som inte följer av EN-ISO/IEC 17065:2012.

Kompletterande krav hänvisar till krav som kompletterar redan förekommande krav i EN-ISO/IEC 17065:2012.

[17] 4 § kompletteringsförordningen.
[18] Certifieringsriktlinjerna, p. 51.

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
4	-	**4 Allmänna krav för ackreditering**
4.1	-	**4.1 Rättsliga och avtalsrelaterade frågor**
4.1.1	Kompletterande krav	**4.1.1 Rättsligt ansvar** Ett certifieringsorgan ska kunna visa att det tillämpar kontinuerligt uppdaterade förfaranden som överensstämmer med det rättsliga ansvar som anges i villkoren för ackreditering, kraven i detta beslut, samt kraven som följer av EN-ISO/IEC 17065:2012.
-	Ytterligare krav	**4.1.1.1 *Efterlevnad av dataskyddsförordningen*** Certifieringsorganet ska, i egenskap av personuppgiftsansvarig, visa att det genomfört en riskanalys, enligt artikel 24.1 i dataskyddsförordningen, och i förekommande fall en konsekvensbedömning, enligt artikel 35.1 i dataskyddsförordningen, samt visa att det finns inrättade och dokumenterade förfaranden och åtgärder för dataskydd, inbegripet tekniska och organisatoriska skyddsåtgärder, för den personuppgiftsbehandling som ingår i certifieringsförfarandet. **Vägledning:** Förfaranden och åtgärder inkluderar, men är inte begränsat till, en dataskyddspolicy, utbildning av personal, utnämnande av ett dataskyddsombud, förandet av ett register enligt artikel 30 i dataskyddsförordningen, rutiner och riktlinjer, behörighetsregler m.m. Om certifieringsorganet är föremål för en pågående eller avslutad utredning av en behörig tillsynsmyndighet, som kan leda till eller har lett till att certifieringsorganet blir föremål för en korrigerande åtgärd enligt artikel 58.2 i dataskydds-förordningen, ska certifieringsorganet kunna visa att den korrigerande åtgärden i fråga inte påverkar organets efterlevnad av kraven för ackreditering, enligt artikel 43.1 b i dataskyddsförordningen. Certifieringsorganet ska informera Swedac om organet blir, eller riskerar att bli, föremål för korrigerande åtgärder, enligt artikel 58.2 i dataskyddsförordningen.
4.1.2	-	**4.1.2 Certifieringsavtal**
4.1.2.1	Inga ytterligare krav	-
4.1.2.2	Kompletterande krav	**4.1.2.2 *Certifieringsavtalets innehåll*** Utöver kraven enligt p. 4.1.2.2 i EN-ISO/IEC 17065:2012 ska certifieringsorganet kunna påvisa att dess certifieringsavtal åtminstone innehåller följande krav på sökanden att: a) alltid uppfylla de kriterier som följer av en certifieringsordning, som godkänts enligt artikel 42.5 i dataskyddsförordningen och som certifieringsorganet tillämpar,

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		b) informera certifieringsorganet om betydande rättsliga eller faktiska ändringar som kan inverka på utvärderingsobjektet och efterlevnaden av kriterierna i certifieringsordningen, i synnerhet ändringar som direkt avser utvärderingsobjektet, c) på uppmaning av certifieringsorganet vidta nödvändiga åtgärder när det sker ändringar i certifieringsordningen som inverkar på certifieringsobjektet och efterlevnaden av kriterierna i certifieringsordningen, d) följa de av certifieringsorganet utfästa tidsfristerna och procedurerna inom ramen för certifieringsförfarandet, vilka ska vara fastställda i certifieringsavtalet, **Vägledning:** Om tidsfrister och procedurer följer av certifieringsordningen ska certifieringsorganet tillämpa dessa. e) ge certifieringsorganet tillgång till uppgifter samt tillträde till nödvändiga resurser för att kunna genomföra certifieringsförfarandet, inbegripet dokumentation och register, teknisk utrustning och it-system, fysiska lokaler samt personal. Om nödvändiga uppgifter eller resurser finns hos ett av den sökande anlitat personuppgiftsbiträde ska biträdet ge motsvarande tillgång, och f) den sökande ska informera certifieringsorganet om en behörig tillsynsmyndighet informerar den sökande att den fastställer, eller har för avsikt att fastställa, en överträdelse av dataskyddsförordningen – eller nationell lagstiftning som kompletterar dataskyddsförordningen – som inverkar eller kan inverka på certifikatets giltighet.
-	**Ytterligare krav**	**4.1.2.3** ***Information till den sökande*** Innan certifieringsorganet och den sökande undertecknar certifieringsavtalet ska certifieringsorganet informera den sökande om följande: a) Att certifieringsavtalet eller erhållandet av ett certifikat inte undanröjer ansvarsskyldigheten, enligt artiklarna 5.2 och 24.1 i dataskyddsförordningen, eller påverkar IMY:s uppgifter och befogenheter, enligt artiklarna 57–58 i dataskyddsförordningen. b) Certifieringsordningens regler för giltighet, förnyelse och återkallelse av certifikat, inbegripet regler om lämpliga intervall för omprövning eller granskning. c) Certifieringsordningens regler om utredning av klagomål, samt de förfaranden och åtgärder som certifieringsorganet inrättat för hantering av klagomål, enligt artikel 43.2 d i dataskyddsförordningen. d) Konsekvenserna för den sökande om certifieringsorganets ackreditering återkallas eller tillfälligt upphävs.

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		e) De utvärderingsmetoder som kommer att tillämpas för det utvärderingsobjekt som den sökande ansöker om certifiering för. f) Den information som certifieringsorganet är skyldigt att tillhandahålla till tillsynsmyndigheten, enligt p. 9.1 nedan. g) Den behöriga tillsynsmyndighetens utredningsbefogenheter, enligt artikel 58.1 c i dataskyddsförordningen. Informationen som tillhandahålls enligt p. 4.1.2.3 st. 1 ska dokumenteras i certifieringsavtalet.
4.1.3	-	**4.1.3 Användning av sigill för dataskydd och märkningar**
4.1.3.1	Inga ytterligare krav	-
4.1.3.2	Inga ytterligare krav	-
-	Ytterligare krav	**4.1.3.1** Utöver kraven enligt p. 4.1.3 i EN-ISO/IEC 17065:2012 får certifikat, sigill och märkningar enbart användas i enlighet med artiklarna 42 och 43 i dataskydds-förordningen och riktlinjerna för ackreditering respektive certifiering.
4.2	-	**4.2 Förvaltning av oberoende**
4.2.1	Inga ytterligare krav	-
4.2.2	Inga ytterligare krav	-
4.2.3	Kompletterande krav	**4.2.3** Utöver kraven enligt p. 4.2.3 i EN-ISO/IEC 17065:2012 får: a) certifieringsorganets uppgifter och skyldigheter inte ge upphov till en intressekonflikt, enligt artikel 43.2 e i dataskyddsförordningen, b) certifieringsorganet och den sökande inte ingå i samma företag, företagsgrupp eller annan gemensam organisation, och c) certifieringsorganet inte vara gemensamt personuppgiftsansvarig eller befinna sig i ett personuppgiftsbiträdesförhållande med den sökande. Certifieringsorganet ska, i enlighet med artikel 43.2 a i dataskyddsförordningen, visa de förhållanden, i synnerhet finansiella relationer, som organet har, eller har haft, med den sökande, utöver de förhållanden som uppstår till följd av ansökan om certifiering, i den mån sådana förhållanden kan inverka på certifieringsorganets oberoende.
4.2.4	Inga ytterligare krav	-
4.2.5	Inga ytterligare krav	-

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
4.2.6	Kompletterande krav	**4.2.6** Utöver kraven enligt p. 4.2.6 i EN-ISO/IEC 17065:2012 får certifieringsorganet inte fastställa ändamålen och medlen för den personuppgiftsbehandling som ingår i utvärderingsobjektet.
4.2.7	Inga ytterligare krav	-
4.2.8	Inga ytterligare krav	-
4.2.9	Inga ytterligare krav	-
4.2.10	Inga ytterligare krav	-
4.2.11	Inga ytterligare krav	-
4.2.12	Inga ytterligare krav	-
4.2.13	Ytterligare krav	**4.2.13** Certifieringsorganet ska visa hur dess verksamhet för certifieringar, enligt artikel 42.5 i dataskyddsförordningen, är finansierad och detaljredovisa intäkter i form av avgifter från sökande och certifierade organisationer.
4.3	-	**4.3 Ansvar och finansiering**
4.3.1	Kompletterande krav	**4.3.1** Certifieringsorganet ska, utöver kravet enligt p. 4.3.1 i ISO/IEC 17065:2012, regelbundet – och åtminstone årligen – kontrollera att organet har vidtagit lämpliga åtgärder (t.ex. genom att inneha nödvändiga försäkringar eller finansiella tillgångar) för att fullgöra sina skyldigheter i de geografiska områden eller jurisdiktioner där det verkar.
4.3.2	Inga ytterligare krav	-
4.4	-	**4.4 Icke-diskriminering**
4.4.1	Inga ytterligare krav	-
4.4.2	Inga ytterligare krav	-
4.4.3	Inga ytterligare krav	-
4.4.4	Inga ytterligare krav	-
4.5	-	**4.5 Konfidentialitet**
4.5.1	Inga ytterligare krav	-
4.5.2	Inga ytterligare krav	-
4.5.3	Inga ytterligare krav	-
4.6	Kompletterande krav	**4.6 Offentligt tillgänglig information** Certifieringsorganet ska, utöver kraven enligt p. 4.6 i EN-ISO/IEC 17065:2012, se till att:

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		a) alla versioner av godkända kriterier som följer av certifieringsordningar, såväl gällande och tidigare, i den mening som avses i artikel 42.5 i dataskyddsförordningen, offentliggörs och är lätt tillgängliga för allmänheten, liksom alla certifieringsförfaranden, varvid respektive giltighetsperiod ska anges, och **Vägledning:** Kravet på offentliggörande av de godkända kriterierna kan uppfyllas genom att certifieringsorganet på sin webbplats hänvisar till publiceringen av kriterierna i certifieringsordningar på Europeiska dataskyddsstyrelsens webbplats. b) att information om förfaranden för hantering av klagomål och överklaganden offentliggörs, i enlighet med artikel 43.2 d i dataskyddsförordningen.
5	-	**5 Strukturella krav**
5.1	-	**5.1 Organisationsstruktur och högsta ledning**
5.1.1	Inga ytterligare krav	-
5.1.2	Inga ytterligare krav	-
5.1.3	Inga ytterligare krav	-
5.1.4	Inga ytterligare krav	-
5.2	-	**5.2 Mekanismer för säkerställande av opartiskhet**
5.2.1	Inga ytterligare krav	-
5.2.2	Inga ytterligare krav	-
5.2.3	Inga ytterligare krav	-
5.2.4	Inga ytterligare krav	-
6	-	**6 Resurskrav**
6.1	-	**6.1 Certifieringsorganets personal**
6.1.1	-	**6.1.1 Generella krav**
6.1.1.1	Inga ytterligare krav	-
6.1.1.2	Kompletterande krav	**6.1.1.2** Utöver kraven enligt p. 6.1.1.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganets personal uppfylla följande krav: a) Personalen ska kunna uppvisa lämplig och varaktig expertis, innebärande aktuell kunskap och erfarenhet om dataskydd, enligt kraven i certifieringsordningen,

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		b) Personalen ska ha aktuell expertis i fråga om certifieringsobjektet, enligt kraven i certifieringsordningen, och ha teknisk eller juridisk specialkompetens enligt p. c) och d) nedan, c) Personal med teknisk kompetens ska: i. ha erhållit en kvalifikation inom ett för certifieringsobjektet relevant tekniskt expertområde, enligt kraven i certifieringsordningen, som åtminstone ska ligga på nivå 6, enligt den Europeiska referensramen för kvalifikationer (EQF), inom det berörda reglerade yrket (t.ex. civilingenjör), eller ha relevant och betydande arbetslivserfarenhet, enligt kraven i certifieringsordningen, ii. ha relevant och lämplig kunskap samt minst två års arbetslivserfarenhet av tekniska och organisatoriska dataskyddsåtgärder, enligt kraven i certifieringsordningen. d) Personal med juridisk kompetens ska: i. ha genomfört juridikstudier vid ett universitet eller högskola, som tillämpar ramverket för kvalifikationer inom det Europeiska området för högre utbildning (EHEA) i minst åtta terminer och avlagt akademisk masterexamen (LL.M.), eller avlagt akademisk examen vid ett universitet eller högskola utanför EHEA som av behörig nationell myndighet eller annat behörigt organ inom EES-området erkänts som motsvarande, ii. ha minst två års arbetslivserfarenhet av arbete med tillämpning av svensk och europeisk dataskyddslagstiftning. e) Personal med ansvar för utvärderingar ska, utöver kraven enligt p. a) – d) ovan, ha kunskap om samt minst två års arbetslivserfarenhet av att genomföra utvärderingar, eller motsvarande arbetslivserfarenhet av att arbeta med jämförbara förfaranden (exempelvis inom ramen för certifieringsförfaranden eller granskning). **Vägledning:** Kompetenskraven kan uppfyllas gemensamt av flera medarbetare som arbetar i en grupp, i ett projekt eller liknande i samma certifieringsförfarande.
6.1.1.3	**Inga ytterligare krav**	-
-	**Ytterligare krav**	**6.1.1.4** Personal som inte uppfyller kompetenskraven enligt p. 6.1.1.2 ovan får delta i utförandet av certifieringsorganets uppgifter, men endast under övervakning av personal som uppfyller kompetenskraven och inte i en beslutsfattande roll.
6.1.2	**-**	**6.1.2 Kompetensförsörjning för personal som är involverad i certifieringsförfarandet**

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
6.1.2.1	Kompletterande krav	**6.1.2.1** Utöver kraven enligt p. 6.1.2.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganet, vid fortbildning eller annan kompetensutveckling av personalen, ta kraven enligt p. 7.4.10 nedan i beaktande. Certifieringsorganet ska kunna visa hur fortbildningen eller kompetens-utvecklingen uppfyller kompetenskraven enligt p. 6.1.1.2 ovan.
6.1.2.2	Inga ytterligare krav	-
6.1.3	Kompletterande krav	**6.1.3 Avtal med personal** Utöver kraven enligt p. 6.1.3 i EN-ISO/IEC 17065:2012 ska certifieringsorganet inför varje nytt certifieringsförfarande samt årligen kräva att dess personal förbinder sig till och lämnar de uppgifter som krävs enligt p. 6.1.3 a) – c) i EN-ISO/IEC 17065:2012.
6.2	-	**6.2 Utvärderingsresurser**
6.2.1	Inga ytterligare krav	**6.2.1 Interna resurser**
6.2.2	Inga ytterligare krav	**6.2.2 Externa resurser (utkontraktering)** **Vägledning:** Vid utkontraktering kvarstår certifieringsorganets ansvar och behörighet att fatta beslut, enligt p. 7.6.1 i EN-ISO/IEC 17065:2012.
6.2.2.1	Inga ytterligare krav	-
6.2.2.2	Inga ytterligare krav	-
6.2.2.3	Inga ytterligare krav	-
6.2.2.4	Inga ytterligare krav	-
7	-	**7 Förfaranderegler**
7.1	-	**7.1 Allmänt**
7.1.1	Kompletterande krav	Certifieringsorganet ska, utöver kraven enligt p. 7.1 i EN-ISO/IEC 17065:2012 vara skyldigt att säkerställa följande: a) När certifieringsorganen lämnar in en ansökan om ackreditering ska organet lämna en försäkran att det uppfyller kraven i detta beslut samt att dess uppgifter och skyldigheter inte ger upphov till intressekonflikter enligt p. 4.2 ovan. b) Innan ett certifieringsorgan som är etablerat i en annan medlemsstat, än den medlemsstat där certifieringsorganet huvudsakligen eller ursprungligen utfärdar certifikat enligt artikel 42.5 i dataskyddsförordningen, börjar använda ett godkänt europeiskt sigill för

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		dataskydd, ska certifieringsorganet meddela den behöriga tillsynsmyndigheten i den andra medlemsstaten.
7.1.2	Inga ytterligare krav	-
7.1.3	Inga ytterligare krav	-
7.2	-	**7.2 Ansökan**
-	Ytterligare krav	**7.2.1** Utöver kraven enligt p. 7.2 i EN-ISO/IEC 17065:2012 ska certifieringsorganet: a) fastställa regler, i enlighet med kraven i certifieringsordningen, för hur utvärderingsobjektet ska beskrivas i ansökan, inbegripet tekniska och organisatoriska gränssnitt samt överföringar av personuppgifter mellan it-system och överföringar till andra organisationer. b) säkerställa att den sökande i ansökan anger om personuppgiftsbiträden används. Personuppgiftsbiträdets ansvarsområden och uppgifter ska, oberoende av om det är den ansökande parten eller inte, beskrivas. Ansökan ska innehålla de avtal mellan personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av ansökans utvärderingsobjekt, inbegripet eventuella avtal med personuppgiftsbiträdens underbiträden. c) säkerställa att den sökande i ansökan anger om gemensamt personuppgiftsansvariga, utöver den sökande, ansvarar för delar av personuppgiftsbehandlingen enligt artikel 26.1 i dataskyddsförordningen, vilka delar som den sökande respektive andra personuppgiftsansvariga ansvarar för, samt redovisar den gemensamma överenskommelsen mellan den sökande och andra personuppgiftsansvariga. d) säkerställa att den sökande redogör för om certifieringsobjektet omfattar överföringar till tredjeland eller en internationell organisation, enligt kapitel V i dataskyddsförordningen, inbegripet: i. en allmän beskrivning av de aktuella överföringarna, ii. vilka kategorier av personuppgifter som överförs, iii. mottagarna, iv. rättsligt stöd för överföringarna, och, v. om det krävs, vilka skyddsåtgärder enligt artikel 46 i dataskyddsförordningen som vidtagits. e) säkerställa att den sökande informerar certifieringsorganet om den sökande är föremål för en pågående eller avslutad utredning som riskerar att leda till, eller har lett till, korrigerande åtgärder, enligt artikel 58.2 i dataskyddsförordningen, som avser, eller avsåg, certifieringsobjektet.
-	Ytterligare krav	**7.2.2**

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		Utöver kraven enligt p. 7.2 i EN-ISO/IEC 17065:2012 ska certifieringsorganet inrätta förfaranden och strukturer som underlättar kommunikation med den sökande vad gäller status för handläggningen av en ansökan.
7.3	-	**7.3 Granskning av ansökan**
7.3.1	Kompletterande krav	**7.3.1** Vid bedömningen enligt p. 7.3.1 p. e i EN-ISO/IEC 17065:2012 ska certifieringsorganet se till att det har betydande teknisk och juridisk expertis i fråga om dataskydd, enligt vad som framgår av p. 6.1.1.2 ovan. Granskningen av ansökan ska ta kraven enligt p. 7.2 ovan i beaktande och certifieringsorganet ska säkerställa att den sökande är en lämplig kandidat för certifiering enligt artikel 42.5 i dataskyddsförordningen.
7.3.2	Inga ytterligare krav	-
7.3.3	Inga ytterligare krav	-
7.3.4	Inga ytterligare krav	-
7.3.5	Inga ytterligare krav	-
7.3.6	Ytterligare krav	**7.3.6** Vid granskningen av ansökan ska certifieringsorganet, med beaktande av kraven enligt p. 7.2 ovan, göra en bedömning av om utvärderingsobjektet är lämpligt för certifiering mot kraven i den aktuella certifieringsordningen. Om certifieringsorganet bedömer att utvärderingsobjektet inte är lämpligt för certifiering ska organet fatta ett beslut i frågan samt informera den sökande om möjligheterna att, i enlighet med kraven i certifieringsordningen, överklaga eller få beslutet överprövat.
		7.3.7
7.4	-	**7.4 Utvärdering**
7.4.1	Kompletterande krav	**7.4.1** Utöver kraven enligt p. 7.4.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganet, i enlighet med kraven i certifieringsordningen, fastställa tillräckligt omfattande utvärderingsmetoder för att möjliggöra en bedömning av den sökandes efterlevnad av certifieringskraven. Utvärderingen ska åtminstone omfatta: a) en metod för att bedöma personuppgiftsbehandlingarnas nödvändighet och proportionalitet i förhållande till deras syfte och de berörda registrerade, b) en metod för att utvärdera omfattningen, sammansättningen och bedömningen av de risker som identifierats och bedömts av den sökande, med hänsyn till de rättsliga följderna enligt artiklarna 30, 32, 35 och 36 i dataskyddsförordningen, och med beaktande av lämpliga tekniska och

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		organisatoriska åtgärder enligt artiklarna 24, 25 och 32 i dataskyddsförordningen, i den mån ovannämnda lagrum utgör en del av utvärderingsobjektet, och c) en metod för att bedöma lösningarna, inbegripet garantier, skyddsåtgärder och förfaranden, för att säkerställa personuppgifternas skydd, inom ramen för de behandlingar som ingår i utvärderingsobjektet och för att visa att kraven i certifieringskriterierna är uppfyllda. Certifieringsorganet ska, med beaktande av certifieringsordningens krav, se till att utvärderingsmetoderna är standardiserade och allmänt tillämpliga. Detta innebär att jämförbara utvärderingsmetoder ska användas för jämförbara utvärderingsobjekt. Varje avvikelse från detta förfarande ska motiveras av certifieringsorganet.
7.4.2	**Inga ytterligare krav**	-
7.4.3	**Inga ytterligare krav**	-
7.4.4	**Kompletterande krav**	**7.4.4** Utöver kraven enligt p. 7.4.4 i EN-ISO/IEC 17065:2012 ska certifieringsorganet kunna visa att den externa personalen uppfyller kraven enligt p. 6.1 ovan, om utvärdering utförs av extern personal.
7.4.5	**Kompletterande krav**	**7.4.5** Utöver kraven enligt p. 7.4.5 i EN-ISO/IEC 17065:2012 ska certifieringsorganet om den sökande i delar av utvärderingen hänvisar till underlag, utvärderingar eller bedömningar från en vid tiden gällande certifiering, som utfärdats av ett ackrediterat certifieringsorgan i enlighet med artikel 42.5 i dataskydds-förordningen, göra en bedömning av och verifiera om dessa underlag, utvärderingar eller bedömningar uppfyller certifieringsordningens krav. Om certifieringsorganet bedömer att certifieringsordningens krav inte är uppfyllda ska organet informera den sökande om detta och begära komplettering. Certifieringsorganets bedömning ska dokumenteras i en utvärderingsrapport som gör det möjligt att utvärdera den tidigare certifieringen och dess resultat. Ett certifieringsintyg eller liknande förklaring utan tillhörande certifieringsdokumentation ska inte i sig vara tillräckligt för att visa överrensstämmelse med certifieringsordningens krav.
7.4.6	**Kompletterande krav**	**7.4.6** Utöver kraven enligt p. 7.4.6 i EN-ISO/IEC 17065:2012 ska certifieringsorganet, med beaktande av kraven i certifieringsordningen, ange under vilka omständigheter, vid vilken tidpunkt och på vilket sätt den sökande får information om avvikelser.
7.4.7	**Inga ytterligare krav**	-
7.4.8	**Inga ytterligare krav**	-

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
7.4.9	Kompletterande krav	**7.4.9** Utöver kraven enligt p. 7.4.9 i EN-ISO/IEC 17065:2012 ska certifieringsorganet dokumentera alla utvärderingsmetoder. Certifieringsorganet ska på begäran av IMY, lämna ut all dokumentation från utvärderingen.
7.4.10	Ytterligare krav	**7.4.10** Certifieringsorganet ska, i enlighet med kraven i certifieringsordningen, fastställa förfaranden för uppdatering av utvärderingsmetoder i samband med utvärderingen enligt p. 7.4 ovan. Oberoende av utvärderingar enligt p. 7.4 ska uppdateringar av utvärderingsmetoder alltid ske i samband med ändringar av: a) den rättsliga ramen, b) relevanta risker, eller c) de tekniska och organisatoriska åtgärdernas aktualitet (*state of the art*), med beaktande för åtgärdernas genomförandekostnader.
7.5	-	**7.5 Granskning**
7.5.1	Inga ytterligare krav	-
7.5.2	Inga ytterligare krav	-
7.5.3	Ytterligare krav	**7.5.1** Utöver kraven enligt p. 7.5 i EN-ISO/IEC 17065:2012 ska certifieringsorganet inrätta förfaranden, i enlighet med kraven i certifieringsordningen, som innebär återkommande granskning och, vid behov, återkallelse av utfärdade certifieringar, enligt artikel 42.5 i dataskyddsförordningen.
7.6	-	**7.6 Certifieringsbeslut**
7.6.1	Kompletterande krav	**7.6.1** Utöver kraven enligt p. 7.6.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganet vara skyldigt att i sina förfaranden införa procedurer som säkerställer dess oberoende och ansvar i fråga om enskilda certifieringsbeslut. Innan certifieringsorganet fattar sitt beslut ska det av den sökande bekräfta att organet inte är föremål för en utredning som omfattar certifieringsobjektet och som kan leda till att en tillsynsmyndighet vidtar korrigerande befogenheter. Certifieringsorganet ska informera behörig tillsynsmyndighet när det utfärdat eller förnyat ett certifikat, i enlighet med artikel 42.5 dataskyddsförordningen. Informationen ska omfatta följande: a) Namn och organisationsnummer på den sökande,

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		b) Certifikatets beteckning samt versionsnummer, c) Datum för när certifikatet börjar gälla och dess giltighetstid, d) En sammanfattning av certifikatets omfattning, och e) En sammanfattning av certifieringsorganets utvärderingsrapport.
7.6.2	**Inga ytterligare krav**	-
7.6.3	**Inga ytterligare krav**	-
7.6.4	**Inga ytterligare krav**	-
7.6.5	**Inga ytterligare krav**	-
7.6.6	**Kompletterande krav**	**7.6.6** Om certifieringsorganet beslutar att inte utfärda eller förnya ett certifikat ska organet, utöver kraven enligt p. 7.6.6 i EN-ISO/IEC 17065:2012, informera den sökande hur denne kan överklaga eller begära överprövning av certifieringsorganets beslut, samt inom vilken tid överklagandet eller begäran om överprövning ska ske.
7.7	**-**	**7.7 Certifieringsdokumentation**
7.7.1	**Kompletterande krav**	**7.7.1** Utöver kraven enligt p. 7.7.1 i EN-ISO/IEC 17065:2012 ska utvärderingsobjektets beteckning anges, inklusive version eller liknande beteckning. Utöver kraven enligt p. 7.7.1 e) i EN-ISO/IEC 17065:2012 ska den avsedda övervakningsperioden, enligt p. 7.9 nedan, dokumenteras. **Vägledning:** Certifikatets giltighet, enligt p. 7.7.1 e) i EN-ISO/IEC 17065:2012, får inte överstiga tre år, enligt artikel 42.7 i dataskyddsförordningen.
7.7.2	**Inga ytterligare krav**	-
7.7.3	**Inga ytterligare krav**	-

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
7.8	Kompletterande krav	**7.8 Katalog över certifieringar** Utöver kraven enligt p. 7.8 i EN-ISO/IEC 17065:2012 ska certifieringsorganet hålla informationen om certifierade personuppgiftsbehandlingar, samt information om återkallelser av certifieringar, internt och offentligt tillgängliga. Informationen ska omfatta vilken certifieringsordning som ett certifikat är utfärdat enligt samt hur länge certifikatet är giltigt. Certifieringsorganet ska offentliggöra en sammanfattning av utvärderingsrapporter som åtminstone inbegriper: a) certifieringens omfattning och begripliga beskrivningar av utvärderingsobjektet, b) de certifieringskriterier som tillämpats i utvärderingen, angiven med aktuell version eller annan motsvarande beteckning, c) vilka utvärderingsmetoder som använts, genomförda tester och bedömningar, samt d) resultat. Utöver kraven enligt p. 7.8 i EN-ISO/IEC 17065:2012, och i enlighet med artikel 43.5 i dataskyddsförordningen, ska certifieringsorganet informera de behöriga tillsynsmyndigheterna om skälen till beviljande eller återkallelse av den begärda certifieringen.
7.9	-	**7.9 Övervakning**
7.9.1	Inga ytterligare krav	-
7.9.2	Inga ytterligare krav	-
7.9.3	Inga ytterligare krav	-
7.9.4	Inga ytterligare krav	-
7.9.5	Ytterligare krav	**7.9.5** Utöver kraven enligt punkterna 7.9.1, 7.9.2 och 7.9.3 i EN-ISO/IEC 17065:2012, och i enlighet med artikel 43.2 c i dataskyddsförordningen, ska certifieringsorganet inrätta förfaranden, i enlighet med certifieringsordningens krav, för återkommande och obligatoriska övervakningsåtgärder, som den sökanden ska efterleva för att bibehålla certifieringen under dess giltighetstid, enligt p. 7.7 ovan. Regelbundenheten för övervakningsåtgärder ska anpassas i förhållande till utvärderingsobjektets risknivå och ska genomföras åtminstone årligen, eller oftare om certifieringsordningens krav kräver det.
7.10	-	**7.10 Ändringar som påverkar certifieringen**

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
7.10.1	**Inga ytterligare krav**	-
7.10.2	**Inga ytterligare krav**	-
7.10.3	**Kompletterande krav**	**7.10.3** Förfarandet ska, utöver kraven enligt p. 7.10.3 i EN-ISO/IEC 17065:2012, åtminstone inkludera: a) lämpliga övergångsperioder för att genomföra ändringar, i enlighet med kraven i certifieringsordningen, b) en förnyad bedömning av utvärderingsobjektet, och c) möjligheten att återkalla certifieringen om utvärderingsobjektet inte längre är förenligt med ändringar av kraven i certifieringsordningen.
7.10.4	**Ytterligare krav**	**7.10.4** Utöver kraven enligt p. 7.10.1 och 7.10.2 i EN-ISO/IEC 17065:2012 ska certifieringsorganet bedöma åtminstone följande ändringar som påverkar eller kan påverka utfärdade certifieringar: a) Ändringar av kraven i certifieringsordningen, b) Ändringar av tillämplig dataskyddslagstiftning om skydd av personuppgifter, c) Antagande av delegerade akter från Europeiska kommissionen i enlighet med artikel 43.8 och 43.9 i dataskyddsförordningen, d) Europeiska dataskyddsstyrelsens beslut och riktlinjer, e) Behöriga tillsynsmyndigheters beslut, f) Domstolsbeslut från behöriga nationella domstolar, EU-domstolen eller Europadomstolen, och g) Personuppgiftsincidenter som sker inom ramen för eller kan påverka utvärderingsobjektet.
7.11	**-**	**7.11 Upphävande, begränsning, tillfälligt upphävande eller återkallelse av certifiering**
7.11.1	**Kompletterande krav**	**7.11.1** Utöver kraven enligt p. 7.11.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganet vara skyldigt att skriftligen underrätta behöriga tillsynsmyndigheter, kunder och, i förekommande fall, nationella ackrediteringsorgan om vilka åtgärder som vidtagits så vitt avser upphävande, begränsning, tillfälligt upphävande eller återkallelse av certifiering. Underrättelsen ska skickas omedelbart i samband

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		med att certifieringsorganet fattar sitt beslut och det ska av underrättelsen framgå vilka åtgärder som kan vidtas för att erhålla certifikatet på nytt. Enligt artikel 58.2 h i dataskyddsförordningen ska certifieringsorganet vara skyldigt att godta beslut och anvisningar från den behöriga tillsynsmyndigheten om att återkalla eller inte utfärda certifikat till en sökande, om kraven på certifiering inte är uppfyllda.
7.11.2	Inga ytterligare krav	-
7.11.3	Inga ytterligare krav	-
7.11.4	Inga ytterligare krav	-
7.11.5	Inga ytterligare krav	-
7.11.6	Inga ytterligare krav	-
7.12	-	**7.12 Register**
7.12.1	Inga ytterligare krav	-
7.12.2	Inga ytterligare krav	-
7.12.3	Inga ytterligare krav	-
7.12.4	Ytterligare krav	**7.12.4** Certifieringsorganet ska, utöver kraven enligt p. 7.12 i EN-ISO/IEC 17065:2012, se till att all dokumentation är fullständig, begriplig, uppdaterad och revisionsanpassad.
7.13	-	**7.13 Klagomål och överklaganden**
7.13.1	Kompletterande krav	**7.13.1** Utöver kraven enligt p. 7.13.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganet också ange och offentliggöra: a) vem som kan lämna in klagomål eller invändningar, b) vem inom certifieringsorganet som behandlar klagomål eller invändningar, c) vilka kontroller som äger rum vid klagomål eller invändningar, och d) möjligheter till samråd med berörda parter.
7.13.2	Kompletterande krav	**7.13.2** Utöver kraven enligt p. 7.13.2 i EN-ISO/IEC 17065:2012 ska certifieringsorganet också ange och offentliggöra: a) hur och vem som ska få en bekräftelse, b) gällande tidsfrister, och c) vilka förfaranden som därefter kommer att inledas.

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		Certifieringsorganet ska ange hur åtskillnad garanteras mellan organets certifieringsverksamhet och handläggningen av överklaganden och klagomål. Den klagande ska ha rätt att utan dröjsmål få information om handläggningen av ett klagomål och beslut ska fattas så snart som möjligt, med hänsyn till klagomålets komplexitet, och allra senast inom tre månader. **Vägledning:** Beslut till följd av klagomål bör i normalfallet kunna fattas inom en månad, men kan fattas inom en tidsram på upp till tre månader om klagomålet är av en komplex karaktär.
7.13.3	Inga ytterligare krav	-
7.13.4	Inga ytterligare krav	-
7.13.5	Inga ytterligare krav	-
7.13.6	Inga ytterligare krav	-
7.13.7	Inga ytterligare krav	-
7.13.8	Inga ytterligare krav	-
7.13.9	Inga ytterligare krav	-
8	-	**8 Krav på ledningssystemet**
8.1	-	**8.1 Valmöjligheter**
8.1.1	Inga ytterligare krav	-
8.1.2	Kompletterande krav	Certifieringsorganet ska inrätta och upprätthålla ett ledningssystem som uppfyller kraven enligt p. 8.1.2 i EN-ISO/IEC 17065:2012. Därutöver ska certifieringsorganet när det inrättar ledningssystemet: a) verka för en ledningsprincip som innebär att verkningsfulla och effektiva mål ställs upp, i synnerhet när det gäller tillhandahållandet av certifieringstjänster, genom att fastställa lämpliga strategier, b) utarbeta en metod som säkerställer att ledningssystemet uppnår efterlevnad av ackrediteringskraven och tillämplig dataskyddslagstiftning på ett kontinuerligt och långsiktigt hållbart sätt, c) se till att Swedac regelbundet hålls informerat om ledningssystemets förmåga att uppnå sina mål. Därutöver ska Swedac informeras så snart som möjligt om eventuella förändringar av ledningssystemet som kan påverka dess förmåga att uppnå sina mål, d) integrera förfarandena för hantering av upphävande, begränsning, tillfälligt upphävande eller återkallelse respektive klagomål i ledningssystemet, inklusive information till kunder,

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		e) se till att förfarandena för klagomålshantering är utformade så att certifieringsorganets bedömningar kan göras på ett oberoende sätt från organets certifieringsverksamhet och i enlighet med p. 4.1.2.2 p. c) och j), 4.6 p. d) och 7.13 i EN-ISO/IEC 17065:2012, och f) se till att certifieringsorganet inrättar förfaranden för att hantera kommunikation mellan organet och dess kunder.
8.1.3	Ej aktuell	-
8.2	Inga ytterligare krav	**8.2 Dokumentation av ledningssystemet** För dokumentation av ledningssystemet ska certifieringsorganet tillämpa p. 8.2 i EN-ISO/IEC 17065:2012.
8.2.1	Inga ytterligare krav	-
8.2.2	Inga ytterligare krav	-
8.2.3	Inga ytterligare krav	-
8.2.4	Inga ytterligare krav	-
8.2.5	Inga ytterligare krav	-
8.3	Inga ytterligare krav	**8.3 Dokumentstyrning** För dokumentstyrning ska certifieringsorganet tillämpa p. 8.3 i EN-ISO/IEC 17065:2012.
8.3.1	Inga ytterligare krav	-
8.3.2	Inga ytterligare krav	-
8.3.3	Ytterligare krav	Utöver kraven enligt p. 8.3 i EN-ISO/IEC 17065:2012 ska certifieringsorganet, som en del av ledningssystemet, se till att samtliga krav som följer av avsnitt 1-7 och 9 i denna bilaga är dokumenterade på ett fullständigt, begripligt, uppdaterat och granskningsanpassat sätt.
8.4	Inga ytterligare krav	**8.4 Kontroll av register** För kontroll av register ska certifieringsorganet tillämpa p. 8.4 i EN-ISO/IEC 17065:2012.
8.4.1	Inga ytterligare krav	-
8.4.2	Inga ytterligare krav	-
8.5	Inga ytterligare krav	**8.5 Granskning av ledningssystemet** För granskning av ledningssystemet ska certifieringsorganet tillämpa p. 8.5 i EN-ISO/IEC 17065:2012.
8.5.1	-	**8.5.1 Generellt**
8.5.1.1	Inga ytterligare krav	-
8.5.1.2	Inga ytterligare krav	-

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
8.5.1.3	Ytterligare krav	**8.5.1.3** Utöver kraven enligt p. 8.5.1 i EN-ISO/IEC 17065:2012 ska certifieringsorganet tillhandahålla strategin för ledningssystemet, metodiken för ledningssystemets genomförande och all annan relevant tillhörande dokumentation till Swedac och behörig tillsynsmyndighet på begäran. Vid granskning av ledningssystemet ska Swedac kunna verifiera att ledningssystemet är tillräckligt väldokumenterat och inrättat på ett sådant sätt att certifieringsorganet kan leva upp till kraven för ackreditering på ett kontinuerligt och långsiktigt hållbart sätt.
8.5.2	Inga ytterligare krav	-
8.5.3	Inga ytterligare krav	-
8.6	Inga ytterligare krav	**8.6 Internrevision** För internrevision ska certifieringsorganet tillämpa p. 8.6 i EN-ISO/IEC 17065:2012.
8.6.1	Inga ytterligare krav	-
8.6.2	Inga ytterligare krav	-
8.6.3	Inga ytterligare krav	-
8.6.4	Inga ytterligare krav	-
8.7	Inga ytterligare krav	**8.7 Korrigerande åtgärder** För korrigerande åtgärder ska certifieringsorganet tillämpa p. 8.7 i EN-ISO/IEC 17065:2012.
8.7.1	Inga ytterligare krav	-
8.7.2	Inga ytterligare krav	-
8.7.3	Inga ytterligare krav	-
8.8	Inga ytterligare krav	**8.8 Förebyggande åtgärder** För förebyggande åtgärder ska certifieringsorganet tillämpa p. 8.8 i EN-ISO/IEC 17065:2012.
8.8.1	Inga ytterligare krav	-
8.8.2	Inga ytterligare krav	-
8.8.3	Inga ytterligare krav	-
-	-	**9 Ytterligare krav**
-	Ytterligare krav	**9.1 Kommunikation mellan certifieringsorganet och behörig tillsynsmyndighet** Certifieringsorganet ska inrätta förfaranden och strukturer som underlättar kommunikation mellan organet och behörig tillsynsmyndighet, som åtminstone ska inkludera:

Avsnittsnumrering enligt EN-ISO/IEC 17065:2012	Ytterligare eller kompletterande krav	Integritetsskyddsmyndigheten kompletterande och ytterligare krav
		a) uppgifter om den som ansöker om certifiering, som ska göra det möjligt för en tillsynsmyndighet att informera om en sökande är föremål för en utredning som omfattar certifieringsobjektet och som kan leda till att tillsynsmyndigheten vidtar korrigerande befogenheter, i enlighet med p. 7.6.1 ovan, b) motiveringen för beslut om att utfärda eller förnya en certifiering, eller att inte utfärda eller förnya en certifiering, enligt p. 7.6 ovan, c) motiveringen för beslut om att upphäva, begränsa, tillfälligt upphäva eller återkalla en certifiering, enligt p. 7.11 ovan, d) relevanta uppgifter om inkomna klagomål och överklaganden, enligt p. 7.13 ovan. P. a) – d) ovan avser kommunikation som sker på initiativ eller begäran av behörig tillsynsmyndighet.