Informationstjänster
Social- och hälsovårdsinformation och informationshantering 9.12.2021

FÖRESKRIFT OM KLASSIFICERING OCH CERTIFIERING AV INFORMATIONSSYSTEM FÖR SOCIAL- OCH HÄLSOVÅRDEN

Bemyndigande

Lag om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021) 35 § 3 mom., 29 § 4 mom., 32 § 4 mom.

Målgrupper

Producenter av informationssystemtjänster och tillverkare av informationssystem för social- och hälsovården
Producenter av informationsförmedlingsservice för kunduppgifter
Tillhandahållare av social- och hälsovårdstjänster
Apoteken
Folkpensionsanstalten
Bedömningsorgan för informationssäkerhet
Mellanhänder

Ikraftträdande

Föreskriften träder i kraft den 9 december 2021 och den gäller tills vidare.

Denna föreskrift upphäver de tidigare föreskrifterna THL 1/2015 och 2/2016. Tidigare föreskrifter har utfärdats med stöd av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården 159/2007. Lag 159/2007 har upphävts genom lag 784/2021.

Innehåll

1 Föreskriftens syfte

Denna föreskrift beskriver de förfaranden och ansvar som tillämpas vid klassificeringen av informationssystemen för social- och hälsovården samt vid uppfyllandet av de väsentliga krav som ställs på systemen och vid certifieringen av systemen. Föreskriften styr implementeringen av informationssystemen enligt kraven, lämnandet av de utredningar som krävs för systemen, den samtestning och bedömning av informationssäkerheten som hör till certifieringen samt registreringen och ibruktagandet av systemen.

2 Föreskriftens tillämpningsområde

Föreskriften gäller de förfaranden som ska iakttas vid klassificering av informationssystem som behandlar klient- eller patientuppgifter inom social- och hälsovården och vid påvisande av systemens överensstämmelse med kraven samt innehållet i den utredning som ska ges (7 kap. i lagen om kunduppgifter, ”Väsentliga krav på informationssystem och välbefinnandeapplikationer”). Institutet för hälsa och välfärd (nedan THL) har med stöd av 34 § 4 mom. i lagen om kunduppgifter bemyndigats att meddela närmare föreskrifter om innehållet i de väsentliga kraven och om vilka väsentliga krav som ska uppfyllas i de informationssystem som används i olika tjänster. Enligt 35 § i lagen om kunduppgifter har THL bemyndigats att meddela föreskrifter om de förfaranden som ska iakttas vid påvisande av överensstämmelse med kraven och om innehållet i den utredning som ska ges. Med stöd av 29 § i kunduppgiftslagen får THL meddela föreskrifter om klassificeringen av informationssystem.

Denna föreskrift gäller

- informationssystem som behandlar klient- och patientuppgifter som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna (Kanta-tjänsterna) (klass A),
- andra informationssystem och tjänster tillhandahållna av mellanhänder som certifieras på basis av sitt användningsändamål (klass A),
- andra system för social- och hälsovården vars användningsändamål är behandling av klient- och patientuppgifter (klass B).

3 Definitioner

I denna föreskrift avses med

- *Bedömning av informationssäkerhet* en del av certifieringsprocessen där ett godkänt bedömningsorgan för informationssäkerhet verifierar informationssäkerhetskraven och utfärdar ett sådant intyg över bedömning av informationssäkerhet som avses i 37 § i lagen om kunduppgifter.
- *Certifiering* ett förfarande genom vilket man verifierar att ett informationssystem uppfyller de väsentliga krav som ställs på det för att det ska få användas för produktion (lagen om kunduppgifter 3 §). Verifieringen av kraven för system som hör till klass A görs genom en bedömning av informationssäkerheten och vid behov genom samtestning. Resultaten av en godkänd samtestning av systemet och giltighetstiden för intyget över bedömning av informationssäkerhet antecknas i Valviras register över informationssystem.
- *Delsystem* ett informationssystem eller programvara som planerats och genomförts för motsvarande användning och som fungerar som en del av ett mer omfattande informationssystem eller en helhet av informationssystem och som är avsedd att anslutas till andra informationssystem eller delsystem som behandlar kunduppgifter. Ett delsystem kan certifieras och tas i bruk som en del av en större

informationssystemhelhet och registreras separat, om delsystemets användningsändamål och de väsentliga krav som gäller delsystemet har beskrivits och verifierats på motsvarande sätt som för informationssystem i allmänhet, och om delsystemets anslutning till andra informationssystem eller delsystem har beskrivits i enlighet med föreskrifterna.

- *Funktion* en funktionalitet eller ett datainnehåll i ett informationssystem som till sitt innehåll motsvarar en funktion eller ett datainnehåll som ingår i de väsentliga kraven på funktionalitet som beskrivs i klassificeringen i bilaga 2 till föreskrift 5/2021.

- *Informationsförmedlingsservice för kunduppgifter* ett informationssystem eller ett delsystem som en organisation inom social- och hälsovården eller ett apotek använder för att ansluta sig till Kanta-tjänsterna. Via systemet eller delsystemet överförs kunduppgifter som produceras av ett annat informationssystem eller delsystem till Kanta-tjänsterna eller utnyttjas kunduppgifter som finns i Kanta-tjänsterna med ett annat informationssystem eller delsystem. Systemet eller delsystemet har inga egenskaper som riktas till slutanvändarna av informationssystemet som ansluts till Kanta-tjänsterna. Mer information finns i bilaga 1.

- *Informationssystem* ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling som det i enlighet med de egenskaper som har planerats av tillverkaren är meningen att använda för elektronisk behandling av kunduppgifter och för registrering och uppdatering av kundhandlingar eller för anslutning till de riksomfattande informationssystemtjänsterna eller med vars hjälp en yrkesutbildad person inom social- och hälsovården kan använda uppgifter om välbefinnande (3 § i lagen om kunduppgifter).

- *Intyg över bedömning av informationssäkerhet* eller *informationssäkerhetsintyg* ett intyg utfärdat av ett godkänt bedömningsorgan över att informationssystemet eller delsystemet har godkänts vid en bedömning av informationssäkerheten.

- *Kanta-tjänsterna* de riksomfattande informationssystemtjänsterna för social- och hälsovården som enligt 6 § i lagen om kunduppgifter är informationssystemtjänster som ordnas av FPA.

- *Producent av en informationssystemtjänst* den som för en tjänstetillhandahållare tillhandahåller eller genomför ett informationssystem där kunduppgifter eller uppgifter om välbefinnande behandlas och som i egenskap av tillverkare av informationssystemet, för tillverkarens räkning eller för en eller flera tillverkares del ansvarar för de krav som ställs på informationssystemet (3 § i lagen om kunduppgifter). Producenten av en informationssystemtjänst kan också ansvara för integreringen av delsystem.

- *Profil* ett dokument som beskriver de nationella minimikraven för ett informationssystem som används för ett visst ändamål i fråga om de funktioner, datainnehåll och informationssäkerhetskrav som implementeras i systemet.

- *Samtestning* interoperabilitetstestning enligt 36 § i lagen om kunduppgifter som ordnas av FPA och som påvisar informationssystemets interoperabilitet med Kanta-tjänsterna och övriga anslutna informationssystem. Som resultat av samtestningen utarbetar FPA en samtestningsrapport och ger ett positivt utlåtande om uppfyllelsen av kraven på interoperabilitet (samtestningsutlåtande) när kraven som ska testas har verifierats med godkänt resultat.

- *Tillverkare av ett informationssystem* den som ansvarar för planeringen och tillverkningen av ett informationssystem för social- och hälsovården, (3 § i lagen om kunduppgifter), oberoende av om aktören också är producent av en informationssystemtjänst.

- *Tjänstetillhandahållare* en sådan tjänstetillhandahållare som avses i 3 § 1 mom. i lagen om kunduppgifter:
    - verksamhetsenhet för hälso- och sjukvård (lag om patientens ställning och rättigheter 785/1992 2 § 1 mom.)
    - arbetsgivare (lag om företagshälsovård 1383/2001 7 § 2 mom.)
    - en yrkesutbildad person inom hälso- och sjukvården som är självständig yrkesutövare (lagen om privat hälso- och sjukvård 152/1990, 2 § 3 mom.)
    - enligt 3 § 3 punkten i lagen om klienthandlingar inom socialvården en myndighet som ordnar, producerar eller lämnar socialvård eller socialservice, eller en sådan serviceproducent som avses i lagen om privat socialservice (922/2011)
    - utöver definitionen i lagen om kunduppgifter gäller i denna föreskrift skyldigheterna som riktar sig mot tjänstetillhandahållaren även apotek enligt 38 § i läkemedelslagen (395/1987) och i den omfattning som avses i lagen om elektroniska recept (61/2007, inklusive ändringar enligt lag 786/2021).

- *Verifiering* ett förfarande som påvisar att ett system uppfyller de krav som ställs på det. Verifieringssätten är bland annat testning av programvaran, genomgång av informationssystemets dokumentation eller anvisningar eller genomgång av meddelanden, loggar eller andra produkter som programvaran producerar. Verifieringen kan också omfatta en dokumenterad intervju med programvarutillverkaren eller producenten av en informationssystemtjänst. Verifiering behandlas närmare i kapitel 10 i föreskrift 5/2021.

- *Väsentligt krav* ett nationellt fastställt krav på informationssystemets funktionalitet, interoperabilitet eller informationssäkerhet enligt 34 § i lagen om kunduppgifter. Kravet kan grunda sig på de källdokument som det hänvisas till i kravet, såsom olika författningar eller specifikationer.

4 Föreskriftens begränsningar och förhållande till andra föreskrifter och dokument

THL har utfärdat en separat föreskrift om väsentliga krav på funktionalitet och informationssäkerhetskrav hos system avsedda för behandling av klient- och patientuppgifter (THL:s föreskrift 5/2021: föreskrift om väsentliga krav hos informationssystem för social- och hälsovården).

THL har utfärdat en separat föreskrift om de utredningar och krav som ska ingå i informationssäkerhetsplanen (THL:s föreskrift 3/2021).

I denna föreskrift beskrivs inte de väsentliga kraven på välbefinnandeapplikationer enligt 3 § i lagen om kunduppgifter eller certifieringsförfarandena i anslutning till dem. När det gäller ett informationssystem som också uppfyller definitionen av en välbefinnandeapplikation tillämpas på dess certifiering a) i första hand och i fråga om behandlingen av kunduppgifter som hör till tjänstetillhandahållarens personregister denna föreskrift samt föreskrift 5/2021 och b) i andra hand och i fråga om egenskaperna hos behandlingen av uppgifter om välbefinnande föreskrift 6/2021.

Genom lag 784/2021 upphävs THL:s tidigare föreskrifter 1/2015 föreskrift om väsentliga krav på informationssäkerhet hos informationssystem av klass A inom social- och hälsovården och 2/2016 föreskrift om väsentliga krav på funktionalitet hos informationssystem för social- och hälsovården. Denna föreskrift ersätter innehållet i ifrågavarande föreskrifter om informationssystemens klassificering och certifiering samt väsentliga krav enligt tidigare författningar.

Denna föreskrift eller dess ikraftträdandetider påverkar inte de tidsfrister enligt lagen om klientuppgifter för tjänstetillhandahållares skyldigheter att ansluta sig som användare av de riksomfattande informationssystemtjänsterna.

Föreskriften gäller informationssystem avsedda för behandling av kunduppgifter inom social- och hälsovården. Ett system, ett delsystem eller en programvara som hör till klass B, A1, A2 eller A3 kan vara en *medicinteknisk produkt* eller utrustning som innehåller komponenter/moduler med ett medicinskt användningsändamål. Överensstämmelsen med kraven hos dessa utrustningar och program ska verifieras i enlighet med EU-förordning 2017/745 om medicintekniska produkter, och utrustningarna ska anmälas till Fimeas register. Denna föreskrift och föreskrift 5/2021 är oberoende av på vilket sätt programvaror eller utrustningar klassificeras enligt bestämmelserna om medicintekniska produkter. Tillverkaren av ett informationssystem ska ta ställning till om systemet eller en del av det ska klassificeras som en medicinteknisk produkt.

Certifiering enligt denna föreskrift och föreskrift 5/2021 avser inte sådan frivillig certifiering av den personuppgiftsansvarige eller personuppgiftsbiträdet som avses i artikel 42–44 i EU:s allmänna dataskyddsförordning. Certifiering enligt denna föreskrift betraktas således inte som en utredning om att dataskyddsförordningen efterlevs eller att ansvarsskyldigheten enligt dataskyddsförordningen uppfylls. Den certifiering som föreskrivs i lagen om kunduppgifter påverkar inte de befogenheter som dataombudsmannens byrå har på basis av dataskyddslagstiftningen.

I denna föreskrift sammanställs också innehållet i separata anvisningar som hänför sig till de tidigare föreskrifterna. Föråldrade anvisningar anges som upphävda i samband med att föreskrifterna träder i kraft.

5 Klassificering av informationssystem

Informationssystem för social- och hälsovården delas in i klasserna A och B. *Producenten av en informationssystemtjänst ansvarar för klassificeringen.* Klassificeringen påverkar vilka åtgärder för certifiering och registrering (se kapitel 7) som ska vidtas för systemet.

Utöver klassificeringen ska producenten av en informationssystemtjänst bedöma riskerna i anslutning till informationssystemet och den behandling av kunduppgifter som görs via systemet samt planera och dimensionera systemets informationssäkerhet utifrån riskbedömningen. Med tanke på certifieringen av informationssystem och de väsentliga kraven som ställs på systemen ska en bedömning av *risknivån* och *omfattningen av behandlingen av kunduppgifter* göras på de grunder som beskrivs i bilaga 1 till denna föreskrift.

Till klass A hör system som är anslutna till Kanta-tjänsterna direkt eller via informationsförmedlingsservicen eller som producerar handlingar som förmedlas till Kanta-tjänsterna eller vars användningsändamål i övrigt är sådant att uppfyllandet av informationssäkerhetskraven ska verifieras. Klass A delas i sin tur in i klasserna A1, A2 och A3 utifrån systemets användningsändamål, typen och omfattningen av kunduppgifter som behandlas i systemet samt systemets risknivå och hur kritiskt systemet är.

- A1: System som kräver en extern bedömning av informationssäkerheten och som inte kräver samtestning. Till klass A1 hör informationsförmedlingsservice för kunduppgifter samt system eller delsystem vars interoperabilitetskrav har verifierats via ett annat system, men som omfattas av informationssäkerhetskrav som ska verifieras. Till klass A1 hör också sådana informationssystem eller delsystem som inkluderar omfattande bevarande eller behandling av klient- och patientuppgifter, även om de inte är anslutna till Kanta-tjänsterna eller hör till klasserna A2 eller A3. Risknivån för ett informationssystem i klass A1 kan vara basnivå eller hög nivå.

- A2: System som kräver samtestning och bedömning av informationssäkerheten och som betjänar ett begränsat datainnehåll eller användningsändamål. Systemen är direkt anslutna till Kanta-tjänsternas gränssnitt eller producerar eller använder handlingar som skickas till Kanta-tjänsterna. Ett system i klass A2 kan inte ensamt uppfylla samtliga krav som ställs på en organisation som producerar social- och hälsovårdstjänster, till exempel i fråga om allt datainnehåll som behövs i verksamheten eller alla skyldigheter i samband med Kanta-tjänsterna. Till klassen hör till exempel a) system som endast registrerar eller utnyttjar administrativa uppgifter i Kanta-tjänsterna; b) separata system som innehåller uppgifter om ett visst specialområde eller en viss avdelning och som ansluts till Kanta-tjänsterna. Utöver dessa använder organisationen ett bassystem som hör till klass A3; c) delsystem som ansluts till Kanta-tjänsterna och som utför en begränsad funktion eller innehåller administrativa eller vårdrelaterade uppgifter i en modulär systemhelhet. Risknivån för ett informationssystem i klass A2 kan vara basnivå eller hög nivå.

- A3: Huvudsystem som kräver samtestning och bedömning av informationssäkerheten, som ansluts till Kanta-tjänsterna och som på ett omfattande sätt eller i fråga om skyldigheterna att ansluta sig till Kanta-tjänsterna helt och hållet uppfyller kraven på en organisation som producerar social- och hälsovårdstjänster. I systemen behandlas i stor utsträckning kunduppgifter som hänför sig till vården eller tjänsternas innehåll. Risknivån för ett informationssystem i klass A3 är som standard hög.

    - *Kritiska system i klass A3* är de informationssystem i klass A3 som används inom den specialiserade sjukvården, på sjukhus i kommuner eller välfärdsområden eller inom den offentliga primärvårdens öppna sjukvård för att tillgodose jouransvaret och inom den prehospitala akutsjukvården för diagnostisering, undersökning och behandling av sjukdomar och hantering av kunduppgifter i anslutning till dessa. Det är möjligt att utvidga gruppen av kritiska system senare.

Klasserna A1, A2 och A3 styr på vilken nivå och med vilka förfaranden (testning, dokumentation, validering osv.) kraven på systemen ska verifieras vid samtestning eller bedömning av informationssäkerheten som ingår certifieringen enligt kapitel 7.

En extern bedömning av informationssäkerheten krävs alltid för Kanta-tjänster. För Kanta-tjänster som innehåller gränssnitt avsedda för tillhandahållare av social- och hälsovårdstjänster eller kunder förutsätts certifiering enligt nivå A3 i tillämpliga delar. Dessa åtgärder kan kombineras med de bedömningar av informationssäkerheten enligt lag 1405/2011 som genomförs åt FPA som myndighetsaktör.

Till *klass B* hör system som är avsedda för behandling av klient- eller patientuppgifter, men som inte är direkt anslutna till Kanta-tjänsterna och vars informationssäkerhetskrav uppfylls och verifieras via andra system eller via åtgärder i informationssäkerhetsplanen för en tjänstetillhandahållare som använder systemet. Till klass B hör också sådana system avsedda för behandling av kunduppgifter som fungerar i en till alla delar tekniskt och fysiskt skyddad driftsmiljö eller som är en del av en större helhet av medicintekniska produkter som består av utrustning och programvara. De ovan beskrivna informationssystemen kan i enlighet med bestämmelserna om medicintekniska produkter omfatta program som klassificeras som medicintekniska produkter[1] i klasserna I, IIa, IIb eller III. Dessa system kan höra till klass B om deras beredskap för patientsäkerhets- och kvalitetsrisker uppfyller kraven på medicintekniska produkter och certifieringen av dem, och om dessa krav och certifieringar samt användarorganisationernas informationssäkerhetsplaner täcker informationssäkerheten för den behandling av klientuppgifter som görs med systemet. System som producerar eller använder som producerar eller använder enskild information om klientuppgifter i mycket begränsad utsträckning kan också tillhöra klass B.

[1] enligt definitionen av medicintekniska produkter i artikel 2 i EU-förordning 2017/745

Exempel på klassificeringen av olika typer av system finns i bilaga 1 till denna föreskrift.

Om producenten av en informationssystemtjänst är någon annan än den ursprungliga tillverkaren av informationssystemet eller delsystemet, ska tillverkaren och producenten av informationssystemtjänsten sinsemellan komma överens om vem som ansvarar för att beskriva systemets användningsändamål, klassificera och registrera systemet och följa upp de väsentliga kraven på systemet. För system som hör till klass A ska man också komma överens om certifieringen och verifieringen av väsentliga krav och om förnyelsen av överensstämmelsen med kraven.

För att uppfylla de väsentliga kraven kan ett informationssystem stöda sig på informationssystemet för en annan tillverkare eller en annan producent av en informationssystemtjänst eller på en tredje parts plattform eller tjänst. Producenten av en informationssystemtjänst ska se till att informationssystemets överensstämmelse med kraven kan verifieras och beskrivas även i dessa fall. Detta kan ske som en del av utredningen eller certifieringen av informationssystemet, antingen i informationssystemet som ska certifieras eller registreras eller genom hänvisning till en tidigare utförd gällande certifiering eller registrering där överensstämmelsen med kraven för lösningen i fråga har beskrivits eller verifierats.

6 Beskrivning av informationssystemets användningsändamål och utredning av hur de väsentliga kraven uppfylls

Producenten av en informationssystemtjänst i ett informationssystem som hör till klass A eller B ska beskriva användningsändamålet för informationssystemet eller delsystemet samt hur systemet uppfyller de väsentliga kraven (lagen om kunduppgifter, 29 §). Denna utredning om informationssystemets eller delsystemets användningsändamål och uppfyllande av de väsentliga kraven ges på en systemblankett enligt föreskrift 5/2021.

På systemblanketten ska man

- med en kortfattad fritt formulerad text beskriva för vilket ändamål informationssystemet är avsett (användningsändamål)
    - av beskrivningen av användningsändamålet bör det framgå i korthet vilken användargrupp (till exempel vilka social- och hälsovårdstjänster eller vilka yrkesgrupper) och för vilket syfte (vilka uppgifter som behandlas, vilka tjänster som produceras eller vilken verksamhet som stöds) systemet är avsett

- ange de funktioner och datainnehåll som omfattas av de väsentliga kraven och som hör till systemets användningsändamål och som implementeras via systemet

- ange de väsentliga informationssäkerhetskrav som implementeras eller uppfylls via systemet med beaktande av systemets användningsändamål

- ange om någon funktion eller något datainnehåll endast delvis implementeras, om funktionen eller datainnehållet implementeras under vissa förutsättningar (förutsättningarna ska beskrivas) eller om funktionen eller datainnehållet implementeras via ett annat informationssystem eller delsystem

- ange alla de profiler för väsentliga krav som motsvarar systemets användningsändamål.

Dessa uppgifter utgör den utredning om uppfyllandet av de väsentliga kraven som avses i lagen om kunduppgifter. Ytterligare information och detaljer beskrivs i föreskrift 5/2021.

Systemblanketten ska

- lämnas in till FPA i samband med ansökan om samtestning av ett informationssystem i klass A2 eller A3
- lämnas in till bedömningsorganet för informationssäkerhet för ett informationssystem i klass A1, A2 eller A3 som genomgår en bedömning av informationssäkerheten
- lämnas in till Tillstånds- och tillsynsverket för social- och hälsovården (nedan Valvira) i samband med anmälan till registret av ett system i klass A1, A2, A3 eller klass B
- lämnas som en del av ett anbud på ett informationssystem eller delsystem till en tillhandahållare av social- och hälsovårdstjänster, som i anbudsförfrågan eller i ett annat förfarande i upphandlingsprocessen förutsätter att de väsentliga kraven eller de profiler som dessa bildar uppfylls i det informationssystem eller delsystem som motsvarar kraven i anbudsförfrågan.

Producenten av en informationssystemtjänst ansvarar för att systemet har de egenskaper som anges på blanketten och att dessa har beaktats i planeringen och utvecklingen av systemet när blanketten används i ovannämnda situationer.

Producenten av en informationssystemtjänst ska göra nödvändiga korrigeringar eller preciseringar i de uppgifter som anges på blanketten för att säkerställa att blanketten är tydlig eller korrekt, om FPA, bedömningsorganet för informationssäkerhet, Institutet för hälsa och välfärd eller Valvira kräver detta på goda grunder.

Producenten av en informationssystemtjänst eller tillverkaren ska själv planera, implementera och testa hur de väsentliga kraven som angetts på systemblanketten uppfylls innan certifieringsprocessen för ett system i klass A inleds eller innan ett system i klass B registreras.

7 Certifieringsprocessen

Ett informationssystem eller delsystem som hör till klass A ska certifieras. Ansvaret för att inleda och genomföra certifieringen ligger hos den aktör som producerar informationssystemtjänsten, som också kan vara systemtillverkaren (lagen om kunduppgifter 33 §, 34 § och 35 §).

7.1 Skyldigheter i anknytning till certifieringsprocessen

Producenten av en informationssystemtjänst eller tillverkaren ska implementera och testa de egenskaper hos informationssystemet som ska certifieras innan den ansöker om samtestning eller bedömning av informationssäkerheten. Implementeringen av de väsentliga kraven ska dokumenteras så att det inte råder oklarheter om hur systemet uppfyller de väsentliga kraven och så att den dokumentation som behövs för verifieringen finns tillgänglig om de krav som verifieras på basis av dokumentationen (se kapitel 6).

Certifieringen omfattar

- samtestning av ett informationssystem, en informationssystemhelhet eller delsystem som hör till klass A2 eller A3 och som ska anslutas till Kanta-tjänsterna. FPA ger ett positivt utlåtande om interoperabiliteten för system eller delsystem som på ett godtagbart sätt uppfyller de testade kraven på interoperabilitet.
- en bedömning av informationssäkerheten. Bedömningsorganet för informationssäkerhet utfärdar ett informationssäkerhetsintyg för informationssystem i klass A1, A2 eller A3 som godkänns vid bedömningen.

Producenten av en informationssystemtjänst ska anmäla uppgifter om ett certifierat system eller delsystem till Valvira i enlighet med kapitel 8.

Producenten av en informationssystemtjänst och den tjänstetillhandahållare som använder ett informationssystem ansvarar för att ett system som kräver certifiering tas i användning för produktion av tjänster i enlighet med kapitel 9.

I certifieringsprocessen testas eller bedöms alla väsentliga krav som motsvarar systemets användningsändamål och egenskaper och för vilka det har specificerats åtgärder för samtestning eller bedömning av informationssäkerheten i enlighet med föreskrift 5/2021. De väsentliga kraven som gäller Kanta-tjänsterna ska uppfyllas i enlighet med specifikationerna för Kanta-tjänsterna.

Om ett väsentligt krav på systemet vid samtestning eller bedömning av informationssäkerheten på ett godtagbart sätt uppfylls delvis eller kompenseras, ska detta nämnas i samtestningsutlåtandet eller i informationssäkerhetsintyget.

Om betydande ändringar görs i ett informationssystem som hör till klass A, ska producenten av en informationssystemtjänst underrätta Folkpensionsanstalten och bedömningsorganet för informationssäkerhet samt Valvira om ändringarna i enlighet med bilaga 2 till denna föreskrift. Betydande ändringar är sådana som förändrar informationssystemets funktion avseende uppfyllandet av de väsentliga kraven i bilaga 2 och 3 till föreskrift 5/2021. Beroende på ändringarna och hur stora effekterna av dem är kan man genomföra en ny samtestning och en ny bedömning av informationssäkerheten eller endast en av dem. Ändringarna kan också vara sådana som inte förutsätter en ny samtestning eller bedömning av informationssäkerheten.

För system i klass A ska uppfyllandet av kraven verifieras enligt beskrivningen i föreskrift 5/2021 som en del av certifieringen även när kraven uppfylls via andra informationssystem eller delsystem än det informationssystem som ska certifieras.

Föremålet för samtestning och certifiering kan vara en systemhelhet som innehåller flera olika delsystem. Informationssystemhelheten eller alla delsystem som hör till den ska ha en producent av en informationssystemtjänst. Delsystemen kan ha en producent av en informationssystemtjänst också i situationer där informationssystemhelheten har en producent av en informationssystemtjänst som ansvarar för integreringen av delsystemen. Producenten av informationssystemtjänsten för varje delsystem ansvarar för sin del för namngivningen, beskrivningen av användningsändamålet och klassificeringen av delsystemet, anmälningen av de väsentliga krav som ställs på delsystemet på systemblanketten samt registreringen. Producenten av en informationssystemtjänst ska i samband med ansökan om samtestning eller bedömning av informationssäkerheten av en större systemhelhet meddela om det för dess delsystem produceras ett separat utlåtande om de delar av samtestningen och ett separat intyg över de informationssäkerhetskrav som verifieras via delsystemet i fråga. I samtestningsutlåtandet eller samtestningsrapporten och i informationssäkerhetsintyget eller den tillhörande rapporten ska det specificeras med vilka andra informationssystem eller delsystem man har verifierat kraven på delsystemet. Om flera producenter av informationssystemtjänster eller andra parter deltar i certifieringen av en informationssystemhelhet ska dessa sinsemellan komma överens om deltagandet i certifieringen och om ansvaren för delsystemen.

Om ett informationssystem eller ett delsystem som har certifierats som en del av systemhelheten har fått ett separat godkänt utlåtande om de delar av samtestningen eller ett separat intyg över de informationssäkerhetskrav som har verifierats via delsystemet i fråga, kan systemet användas i motsvarande omfattning även tillsammans med andra informationssystem eller delsystem än de som har certifierats i samma systemhelhet. I certifieringen av delsystemet kan man stödja sig på krav som ska uppfyllas via andra tidigare verifierade informationssystem eller delsystem. Då får inte de andra tidigare certifierade informationssystemen eller delsystem ett nytt

samtestningsutlåtande eller informationssäkerhetsintyg. Programvara som ingår i systemhelheten kan vara installerad i en driftsmiljö som förvaltas av en eller flera tjänstetillhandahållare eller producenter av informationssystemtjänster.

Det förutsätts inte att en tjänstetillhandahållare som är kund hos en producent av en informationssystemtjänst deltar i certifieringen eller de verifieringar som hör till certifieringen, om inte tjänstetillhandahållaren och producenten av informationssystemtjänsten har kommit överens om något annat.

Som en del av certifieringen går man igenom de krav som gäller informationssystemets driftsmiljö och som producenten av en informationssystemtjänst eller tillverkaren av informationssystemet ansvarar för när informationssystemet används. Beroende på systemets och den anslutna tjänstens karaktär och avtal kan en del av kraven som gäller driftsmiljön riktas mot de tjänstetillhandahållare som använder systemet.

Till exempel är det vanligtvis tjänstetillhandahållarens ansvar att skydda den fysiska driftsmiljön för systemets slutanvändare, men producenten av en informationssystemtjänst kan stödja skyddet genom anvisningar och stödtjänster. De server- eller nätverksmiljöer som hör till driftsmiljön kan beroende på avtalsarrangemangen skötas av producenten av en informationssystemtjänst, tjänstetillhandahållaren eller en tredje part som producerar tjänster åt dessa. Producenten av en informationssystemtjänst och tjänstetillhandahållaren ska vid behov komma överens om vilka av de väsentliga krav som gäller driftsmiljön som producenten av informationssystemtjänsten ansvarar för och vilka som är tjänstetillhandahållarens ansvar. Då ska ansvaret som hör till producenten av informationssystemtjänsten enligt kapitel 5 beaktas.

De dokument som uppkommer och används i certifieringsprocessen ska vara korrekta och okontroversiella. Den som upprättar respektive dokument ansvarar för dess riktighet. Centrala dokument är systemblanketten och registeranmälan till Valviras register över informationssystem som upprättas av producenten av en informationssystemtjänst, samtestningsutlåtandet och samtestningsrapporten från FPA:s samtestning, informationssäkerhetsintyget som utfärdas av bedömningsorganet för informationssäkerhet och de uppgifter som ska antecknas i Valviras register över informationssystem.

Verifieringen av väsentliga krav och överensstämmelsen med olika typer av krav behandlas mer detaljerat i föreskrift 5/2021. föreskrift 5/2021 och dess bilaga 1 innehåller ytterligare information om tillämpningen av certifieringsprocessen, uppfyllandet av de väsentliga kraven och bedömningen av hur de väsentliga kraven uppfylls.

7.2 Innehållet i och resultaten av samtestningen

Vid samtestningen testas de krav som ingår i profilerna som hör till systemets användningsändamål och andra sådana funktioner och datainnehåll som systemet tillämpar i anslutning till Kanta-tjänsterna och som utgör testfall för samtestning. FPA kan ge ett informationssystem flera samtestningsutlåtanden om samtestningen av olika funktioner eller innehåll eller koppla flera testhelheter till samma samtestningsutlåtande.

Av samtestningsutlåtandet ska det åtminstone framgå uppgifter om systemets namn och version, klass (till exempel A2 eller A3), tidpunkten för utlåtandet, innehållet i de samtestningar som utförts för systemet (till exempel rubriker för de testade helheterna), de profiler som enligt anmälan har implementerats i systemet och observationer som ska beaktas vid ibruktagandet av systemet eller i verksamhet som följer bestämmelserna. FPA ska lämna samtestningsutlåtandet jämte bilagor åtminstone till producenten av en informationssystemtjänst och Valvira. Om en bedömning av informationssäkerheten pågår för informationssystemet ska FPA också lämna samtestningsutlåtandet till bedömningsorganet för informationssäkerhet.

De krav som genomgår samtestning ska grunda sig på de krav som ställs i de publicerade specifikationerna och materialen samt på testning av egenskaperna enligt systemets användningsändamål i förhållande till Kanta-tjänsterna eller de nationella specifikationerna.

I systemet som ska samtestas ska de väsentliga krav som genomgår samtestning implementeras utifrån de senaste publicerade eller på annat sätt gällande specifikationsversionerna. Ikraftträdandet av specifikationsversionerna och stödet för olika versioner beskrivs också i kapitel 10.3 i föreskrift 5/2021.

Om en del av systemkraven i det system som är föremål för samtestning uppfylls via ett annat system eller delsystem, ska det av testutlåtandet framgå med vilka andra system eller delsystem samtestningen eventuellt har utförts. I samtestningsutlåtandet antecknas dessutom om producenten av en informationssystemtjänst *avseende de krav som samtestats* meddelar vilka eller vilken typ av andra informationssystem eller delsystem som fungerar tillsammans med det testade systemet via andra gränssnitt än Kanta-gränssnitten.

7.3 Innehållet i och resultaten av bedömningen av informationssäkerheten

Som kriterier för bedömning av informationssäkerheten enligt denna föreskrift används informationssäkerhetskraven i föreskrift 5/2021. Inga andra kriterier ska ingå i samma informationssäkerhetsintyg, även om kraven enligt andra kriterier bedöms i samband med samma bedömning.

Av informationssäkerhetsintyget ska det framgå uppgifter om åtminstone systemets namn och version, klass (A1, A2 eller A3) och vilka profiler som enligt anmälan har implementerats i systemet som genomgått bedömningen. Intyget ska innehålla eventuella preciserande observationer och förutsättningar som ska beaktas, särskilt i de organisationer som använder systemen, för att uppfylla kraven vid ibruktagandet av systemet, i verksamhet som följer bestämmelserna eller vid datasäker användning. Om det är fråga om ett kritiskt system i klass A3 enligt kapitel 5 ska detta nämnas i intyget. Intyget ska också innehålla andra uppgifter enligt Traficoms anvisningar för bedömningsorgan.

I bedömningen av informationssäkerheten verifieras alla sådana väsentliga informationssäkerhetskrav som ska verifieras med beaktande av systemets användningsändamål, klass, omfattning och kritiska karaktär och typen av uppgifter som behandlas. De krav som ska verifieras omfattar informationssäkerhetskraven enligt de profiler som motsvarar systemets användningsändamål och andra krav som har implementerats eller som uppfylls via systemet. Även andra krav på informationssäkerhet än de som gäller användningen och utnyttjandet av Kanta-tjänsterna och som anges i de väsentliga informationssäkerhetskraven i föreskrift 5/2021 är krav som ska gås igenom och verifieras. Vid verifieringen av informationssäkerhetskraven används de administrativa och i tillämpliga delar även tekniska verifieringssätt som beskrivs i föreskrift 5/2021 och i Traficoms anvisningar.

Verifieringen görs enligt föreskrift 5/2021 på den nivå som varje krav förutsätter med beaktande av systemets klass, risknivå, kritiska karaktär och typen av uppgifter som behandlas. Verifieringen av informationssäkerhetskraven ska utföras i en omfattning som motsvarar systemets användningsändamål, risknivå och omfattningen av behandlingen av kunduppgifter och endast till den del som uppfyllandet av kraven inte har verifierats via eventuella andra system som anslutits till systemet.

Om informationssystemet används för produktion av tjänster ska det genomgå en bedömning av informationssäkerheten som syftar till ett nytt intyg, och ett informationssäkerhetsintyg ska skrivas innan det tidigare intygets giltighetstid löper ut i enlighet med kapitel 10.

Om en anmälan om ändringar i ett informationssystem leder till en bedömning av informationssäkerheten som görs med anledning av ändringarna, ska man i denna bedömning gå igenom de krav som påverkas av ändringarna. Om de övriga kraven enligt producenten av en informationssystemtjänst uppfylls på samma nivå som tidigare, kan

det befintliga informationssäkerhetsintyget uppdateras så att giltighetstiden för det tidigare intyget inte ändras. Producenten av en informationssystemtjänst kan också besluta att bedömningen ska göras med sikte på ett nytt informationssäkerhetsintyg om det till följd av ändringarna behövs en bedömning av informationssäkerheten. Då går man i bedömningen av informationssäkerheten i enlighet med kapitel 10 igenom alla informationssäkerhetskrav som implementerats eller uppfyllts via systemet och skriver ett nytt intyg med en ny giltighetstid.

Eventuella uppföljande auditeringar av informationssäkerheten som informationssystemet genomgår ska särskiljas från bedömningar av informationssäkerheten som syftar till att förnya intyget. Ett nytt informationssäkerhetsintyg skrivs inte för uppföljande auditeringar och giltighetstiden för ett gammalt intyg förlängs inte som ett resultat av en uppföljande auditering. Om den uppföljande auditeringen inte leder till ett nytt informationssäkerhetsintyg eller till att uppgifterna i Valviras register över informationssystem måste uppdateras, behöver man inte göra någon anteckning om den uppföljande auditeringen i Valviras register över informationssystem.

I det uppdaterade eller nya informationssäkerhetsintyget inkluderas vid behov även de observationer som antecknats i det tidigare intyget om omständigheter som ska beaktas.

Det senaste giltiga eller uppdaterade intyget ersätter tidigare intyg som beviljats samma informationssystem.

Ett informationssäkerhetsintyg ska skrivas så att det gäller i tre år, om inte en kortare giltighetstid är nödvändig på grund av myndigheternas föreskrifter eller anvisningar eller på grund av att väsentliga krav eller andra bestämmelser förnyas.

För ett system i klass A2 eller A3 kan ett informationssäkerhetsintyg utfärdas först efter att systemet har godkänts vid samtestning.

Om ett informationssystem i klass A2 eller A3 ska certifieras så att det genomgår både samtestning och bedömning av informationssäkerheten, ska producenten av en informationssystemtjänst se till att samtestningen och bedömningen av informationssäkerheten gäller samma systemversion eller en sådan version där eventuella systemändringar relaterade till de väsentliga kraven som ska samtestas inte påverkar de informationssäkerhetskrav som ska bedömas. Innan ett informationssäkerhetsintyg utfärdas för ett system som hör till klass A2 eller A3 ska bedömningsorganet för informationssäkerhet säkerställa hos producenten av en informationssystemtjänst och Folkpensionsanstalten att det system som är föremål för samtestning inte kommer att genomgå ändringar som kan påverka uppfyllandet av informationssäkerhetskraven.

Resultaten av samtestningen nämns inte i informationssäkerhetsintyget.

Förfarandena för bedömning av informationssäkerheten beskrivs närmare även i kapitel 5 och 6 i bilaga 1 till föreskrift 5/2021.

8 Registrering av informationssystem

Producenten av en informationssystemtjänst ska registrera ett informationssystem som hör till klass A eller B i det register över informationssystem som förs av Valvira. I samband med registreringen ska en systemblankett enligt föreskrift 5/2021 lämnas in. Producenten av informationssystemtjänsten ansvarar för att de uppgifter som lämnas på systemblanketten är korrekta och exakta och motsvarar de väsentliga krav som har implementerats i systemet eller som har uppfyllts genom systemet.

Om informationssystemet hör till klass A1, A2 eller A3 och ska certifieras, förutsätter registreringen i Valviras register över informationssystem att de väsentliga krav som motsvarar systemets användningsändamål har verifierats med godkänt resultat vid samtestningen och bedömningen av informationssäkerheten. Då ska anmälan och systemblanketten lämnas in till Valvira när systemets samtestning eller bedömning av informationssäkerhet har slutförts med godkänt resultat.

Producenten av en informationssystemtjänst som ansvarar för ett informationssystem som hör till klass A2 eller A3 ska i samband med registeranmälningar till Valvira specificera alla FPA:s samtestningsutlåtanden som gäller testhelheter som implementerats och samtestats i systemet. Endast det senaste samtestningsutlåtandet om varje testad helhet ska anmälas så att de samtestade egenskaperna bildar en helhetsbild.

Producenten av en informationssystemtjänst som ansvarar för ett informationssystem i klass A ska i samband med anmälningar till Valvira specificera identifikationskoden för ett giltigt informationssäkerhetsintyg. Endast det senaste och gällande informationssäkerhetsintyget över en godkänd bedömning av informationssäkerheten ska anmälas.

De uppgifter om ett informationssystem som publiceras i registret grundar sig på

a) uppgifterna på systemblanketten: beskrivningen av användningsändamålet, profilerna i systemet, risknivån och de väsentliga krav som uppgetts på systemblanketten

b) samtestningsrapporterna

c) det senaste gällande informationssäkerhetsintyget och

d) andra utredningar och myndighetsbeslut som Valvira anser nödvändiga.

Valvira kan ge närmare anvisningar om registeranmälningarna och be producenten av en informationssystemtjänst, FPA eller bedömningsorganet om ytterligare information för att säkerställa att uppgifterna i registret över informationssystem är korrekta.

9 Ibruktagandet av informationssystem

Både informationssystem som hör till klass A och B ska uppfylla de väsentliga krav som motsvarar systemets användningsändamål (se kapitel 6) innan systemet kan tas i användning för produktion av tjänster. Förutsättningarna för att ta ett system i användning för produktion av tjänster beskrivs i 31 § i lagen om kunduppgifter.

Ett informationssystem eller delsystem som hör till klass B får tas i användning för produktion av tjänster efter det att producenten av en informationssystemtjänst har gett en sådan skriftlig utredning om uppfyllandet av de väsentliga funktionella kraven och informationssäkerhetskraven som avses i lagen och i denna föreskrift och när uppgifterna om systemet finns i Valviras register över informationssystem.

För system som hör till klass A krävs en godkänd certifiering och ett giltigt informationssäkerhetsintyg (se kapitel 7) innan informationssystemet får tas i användning för produktion av tjänster. En förutsättning för produktionsanvändning är också att producenten av informationssystemtjänsten har gett en sådan skriftlig utredning om att de väsentliga kraven uppfylls som avses i lagen och i denna föreskrift och att aktuella uppgifter om systemet finns i Valviras register över informationssystem.

Ett informationssystem i klass A som är tänkt att anslutas till Kanta-tjänsterna ska ha godkänts vid samtestning enligt gällande specifikationer för att kunna anslutas till Kanta-tjänsterna. Samtestningen utförs i den omfattning som systemets användningsändamål förutsätter (se kapitel 6). De funktioner och datainnehåll som anknyter till egenskaper som implementeras via Kanta-tjänsterna och som ingår i testhelheterna som samtestas med Kanta-tjänsterna ska ha ett utlåtande från FPA om godkänd samtestning. Systemimplementeringen, samtestningen och det positiva utlåtandet ska grunda sig på sådana specifikationer och specifikationsversioner som vid respektive tidpunkt krävs av ett system som ansluts till Kanta-tjänsterna. FPA och THL publicerar uppgifter om vilka specifikationer och specifikationsversioner som krävs av de system som ansluts till Kanta-tjänsterna och vilka specifikationsversioner som är i kraft. I Kanta-tjänsterna är det möjligt att stöda flera versioner av specifikationerna med olika funktioner och datainnehåll. Specifikationernas versionshantering i förhållande till helheterna som testas beskrivs i kapitel 10.3 i föreskrift 5/2021.

Avvikelser från de väsentliga kraven behandlas i kapitel 10.4 i föreskrift 5/2021. Producenten av en informationssystemtjänst eller tjänstetillhandahållaren får inte börja använda ett system som enligt de uppgifter som finns i Valviras register över informationssystem är föremål för en betydande avvikelse som förhindrar att systemet tas i användning för produktion av tjänster.

Tillhandahållare av social- och hälsovårdstjänster eller apotek ska säkerställa att uppgifterna om det informationssystem som är avsett för behandling av klient- eller patientuppgifter och som tas i användning för produktion av tjänster i deras verksamhet finns i registret som förs av Valvira. Dessutom ska tjänstetillhandahållaren eller apoteket säkerställa att de informationssystem som används i sin helhet motsvarar tjänstetillhandahållarens verksamhet och att man med dem kan uppfylla de allmänna och eventuella tjänstespecifika minimikraven enligt 7 § och 34 § i lagen om kunduppgifter och föreskrift 5/2021 i tjänstetillhandahållarens eller apotekets verksamhet.

10 Förnyande av överensstämmelse med kraven

När giltighetstiden håller på att gå ut för ett informationssäkerhetsintyg eller ett överensstämmelseintyg enligt tidigare lag som utfärdats för ett informationssystem eller delsystem, ska producenten av en informationssystemtjänst kontakta bedömningsorganet för informationssäkerhet för att förnya informationssäkerhetsintyget. Producenten av en informationssystemtjänst ska också kontakta FPA för att behovet av samtestning av systemet ska kunna bedömas på nytt.

Bedömningsorganet för informationssäkerhet och FPA ska kontaktas senast sex månader innan det tidigare intyget löper ut.

Informationssystemet ska vid behov samtestas i förhållande till gällande specifikationer eller de specifikationer som förutsätts vid samtestning innan förnyade intyg över bedömning av informationssäkerheten utfärdas. FPA ger ett positivt samtestningsutlåtande för samtestning som utförts med godkänt resultat.

För den ovan beskrivna bedömningen ska producenten av en informationssystemtjänst ge FPA aktuell information om vilka av de krav som ska samtestas i anslutning till Kanta-tjänsterna som har implementerats och vilka specifikationsversioner implementeringarna baseras på. En implementering ska ändras så att den grundar sig på en aktuell eller erforderlig specifikationsversion innan man ansöker om samtestning, om

- implementeringen grundar sig på en föråldrad specifikation och tidsfristen för när den nya specifikationsversionen ska tas i bruk, som fastställts i samband med den nya ersättande specifikationen eller i författningar, har löpt ut; eller

- implementeringen inte motsvarar den publicerade specifikationen eller specifikationsversionen som krävs i Kanta-tjänsternas produktionsmiljö; eller

- implementeringen inte motsvarar den publicerade specifikationsversionen som krävs för samtestning med Kanta-tjänsterna, även om implementeringar enligt den äldre versionen som försvinner fortfarande skulle stödas i Kanta-tjänsternas produktionsmiljö.

Bedömningsorganet för informationssäkerhet utför en bedömning av informationssäkerheten i syfte att förnya informationssäkerhetsintyget genom att verifiera alla väsentliga informationssäkerhetskrav som är relevanta för systemet. Vid verifieringen av respektive krav kan man stödja sig på samma förfaranden och dokumentation som i det tidigare beviljade informationssäkerhetsintyget, om inte sätten att implementera eller uppfylla kravet har ändrats i systemet eller om det inte har skett förändringar i systemets driftsmiljö som påverkar uppfyllandet av kraven. Bedömningsorganet för informationssäkerhet skriver ett informationssäkerhetsintyg över godkänd bedömning av informationssäkerheten i enlighet med kapitel 7.3.

Till följd av att överensstämmelsen med kraven förnyas ska producenten av en informationssystemtjänst uppdatera uppgifterna om systemet i Valviras register över informationssystem. Även de centrala uppgifterna i det nya gällande informationssäkerhetsintyget och eventuella nya samtestningsutlåtanden blir tillgängliga i Valviras register över informationssystem i enlighet med kapitel 8.

Hur de väsentliga kraven förhåller sig till specifikationerna och specifikationsversionerna beskrivs också i kapitel 10.3 i föreskrift 5/2021.

Kraven som gäller stöd för olika versioner av strukturer och uppgifter i klienthandlingar inom socialvården beskrivs i THL:s föreskrift 1/2021.

Om producenten av en informationssystemtjänst är någon annan än den ursprungliga tillverkaren av informationssystemet, ska tillverkaren och producenten av informationssystemtjänsten sinsemellan komma överens om vem som ansvarar för uppföljningen av kraven och förnyandet av överensstämmelsen med kraven.

11 Handledning och rådgivning

Mer information om tillämpningen av denna föreskrift och certifieringsprocessen i förhållande till de väsentliga krav som ställs på informationssystem finns i föreskrift 5/2021 och dess bilaga 1.

Institutet för hälsa och välfärd ger på begäran råd och handledning om tillämpningen av denna föreskrift. Mer information om de väsentliga kraven och certifieringsprocessen finns också på THL:s webbplats och på webbplatsen Kanta.fi.

12 Ikraftträdande och övergångsbestämmelser

Denna föreskrift träder i kraft den 9 december 2021 och gäller tills vidare.

Ett certifierat system som godkänts med stöd av den tidigare lagen om klientuppgifter 159/2007 samt föreskrifterna 1/2015 och 2/2016 kan användas för produktion av tjänster i nuvarande omfattning och kan tas i användning för produktion av tjänster hos nya tjänstetillhandahållare enligt tidigare godkända krav så längde det tidigare överensstämmelseintyget är giltigt.

Enligt föreskriften krävs inte att det gällande överensstämmelseintyget för ett system i klass A omedelbart förnyas, såvida inte de övriga kraven för förnyelse uppfylls. En systemblankett enligt föreskrift 5/2021 ska lämnas in till FPA för bedömning av behovet av en ny samtestning och till bedömningsorganet för informationssäkerhet för bedömning av behovet av en ny bedömning av informationssäkerheten senast sex månader innan det tidigare överensstämmelseintyget (enligt lag 159/2007) eller informationssäkerhetsintyget upphör att gälla.

En systemblankett enligt föreskrift 5/2021 krävs efter att denna föreskrift har trätt i kraft när man ansöker om FPA:s samtestning eller bedömning av ett bedömningsorgan för informationssäkerhet för ett informationssystem i klass A.

De klassificerings- och certifieringsförfaranden som beskrivs i föreskriften tillämpas på alla system som ska certifieras *senast sex månader efter att föreskriften har trätt i kraft*. För ett system vars samtestning har inletts före den 1 september 2021 kan certifieringsprocessen slutföras *inom sex månader efter att föreskriften trätt i kraft* i enlighet med de krav, författningar och förfaranden som gällde när processen inleddes. Informationssäkerhetsintyget kan då gälla i högst tre år efter att lagen om kunduppgifter trätt i kraft, och intyget ska innehålla en tydlig anteckning om att bedömningen har utförts i enlighet med kraven i lag 159/2007. På begäran av producenten av en informationssystemtjänst kan man dock även i dessa fall tillämpa förfaranden och krav enligt föreskrifterna 4/2021 och 5/2021. System vars tidigare överensstämmelseintyg (enligt lag 159/2007) upphör att gälla mer än sex månader efter att denna föreskrift trätt i kraft eller senare, ska verifiera de väsentliga kraven i enlighet med denna föreskrift och föreskrift 5/2021 innan överensstämmelseintyget blir ogiltigt.

Klassificeringen av ett tidigare certifierat system som hör till klass A ska vid behov preciseras i samband med ansökan om samtestning, ansökan om bedömning av informationssäkerheten och anmälan till Valvira som görs efter att denna föreskrift trätt i kraft.

Om kraven enligt föreskrift 4/2021 eller 5/2021 förutsätter att uppgifterna i ett system i klass B eller A preciseras eller uppdateras i Valviras register över informationssystem, men inte kräver en ny certifiering, ska en uppdaterad anmälan om systemet lämnas till Valviras register senast *inom 1 år* från det att lagen om kunduppgifter trätt i kraft, om inte Valvira bestämmer något annat.

Överensstämmelseintyget för system som certifierats med stöd av den tidigare lagen om klientuppgifter 159/2007 samt föreskrifterna 1/2015 och 2/2016 ska förnyas till ett informationssäkerhetsintyg enligt denna föreskrift innan överensstämmelseintyget enligt den tidigare lagen upphör att gälla, *dock senast inom tre år* från det att lagen om kunduppgifter trätt i kraft. I samband med förnyelsen ska producenten av en informationssystemtjänst säkerställa att alla väsentliga krav som motsvarar dess användningsändamål har implementerats och certifierats i systemet.

Om ett informationssystem flyttas från klass B till klass A enligt de kriterier som beskrivs i denna föreskrift och dess bilagor, ska systemet certifieras i enlighet med gällande väsentliga krav *senast inom tre år efter att lagen om kunduppgifter trätt i kraft*. Om ett informationssystem som inte har anslutit till Kanta-tjänsterna ansluter direkt, via ett annat system eller via informationsförmedlingsservicen, ska informationssystemet klassificeras och certifieras innan anslutningen.

Producenten av en informationssystemtjänst ska underrätta de tjänstetillhandahållare eller apotek som använder ett system för produktion av tjänster om att systemets klass har ändrats eller preciserats.

Mer information om när profilerna för de väsentliga minimikraven träder i kraft och hur de påverkar bland annat socialvårdens klientdatasystem finns i föreskrift 5/2021.

Pekka Rissanen
t.f. Direktör för informationstjänsterna

Jarmo Kärki
Enhetschef

Bilagor

Bilaga 1: Exempel på klassificeringen av system

Bilaga 2: Anmälan om ändringar i informationssystem för social- och hälsovården som hör till klass A

Sändlista

Tillhandahållare av social- och hälsovårdstjänster
Mellanhänder
Folkpensionsanstalten
Tillverkare av klient- och patientdatasystem samt producenter av informationssystemtjänster för social- och hälsovården
Producenter av informationsförvaltningstjänster och ICT-tjänster för social- och hälsovården
Kompetenscentrum inom det sociala området
Social- och hälsovårdsministeriet
Finlands Kommunförbund rf
Valvira
Traficom
FIMEA
Finansministeriet
Arbets- och näringsministeriet
Befolkningsregistercentralen
Dataombudsmannens byrå
Regionförvaltningsverken

Denna föreskrift finns på webbadressen

https://www.finlex.fi/fi/viranomaiset/normi/561001/ (FINLEX ® – Myndigheternas föreskriftssamlingar: Institutet för hälsa och välfärd) samt

på registratorskontoret vid Institutet för hälsa och välfärd samt

på webbadressen https://thl.fi/sv/web/informationshantering-inom-social-och-halsovarden/foreskrifter-och-specifikationer/foreskrifter