

Informationsförmedlarna

Information och styrning av informationshanteringen

29.3.2022

FÖRESKRIFT 1/2022: FÖRESKRIFT OM FÖRFARANDE VID BEVILJANDE AV INFORMATIONSSÄKERHETSINTYG FÖR SLUTFÖRANDE AV CERTIFIERING

Bemyndigande

Lag om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021)
32 § 4 mom., 34 § 4 mom. och 35 § 3 mom.

Målgrupper

Producenter av informationssystemtjänster för social och hälsovården, som har inlett certifiering medan de tidigare bestämmelserna var i kraft före den 1 september 2021, och vars tidigare överensstämmelseintyg går ut under föreskriftens giltighetstid eller är föråldrat.

Folkpensionsanstalten

Bedömningsorgan för informationssäkerhet

Ikraftträdande

Föreskriften träder i kraft den 29 mars 2022 och den gäller till den 31 december 2022.

Innehåll

| | |
|---|---|
| 1 Föreskriftens syfte..... | 3 |
| 2 Föreskriftens tillämpningsområde och THL:s behörighet att meddela föreskrifter..... | 3 |
| 3 Tidsbundna förfaranden för påvisande av överensstämmelse med kraven vid certifiering..... | 4 |
| 4 Föreskriftens förhållande till andra föreskrifter..... | 6 |
| 5 Handledning och rådgivning | 6 |
| 6 Ikraftträdande | 7 |
| Bilaga 1. Undantag och preciseringar av förfaranden enligt föreskrifterna 4/2021 och 5/2021 | 8 |

FÖRÅLDRAD

1 Föreskriftens syfte

I denna föreskrift föreskrivs om undantag från och preciseringar av förfaranden enligt föreskrifterna 4/2021 och 5/2021.

Med föreskriften föreskrivs tidsbundna förfaranden som gäller till den 31 december 2022, med vilka man för påvisande av överensstämmelse med kraven följer lagen om elektronisk behandling av kunduppgifter inom social- och hälsovården (nedan lagen om kunduppgifter) (784/2021) samt THL:s föreskrifter 4/2021 och 5/2021 som har utfärdats med stöd av denna lag under ikraftträdandeperioden för de informationssystem som hör till klass A och som har beviljats överensstämmelseintyg enligt den tidigare lagen om klientuppgifter (159/2007), och som för förnyelse av intyget är under pågående certifiering utifrån förfaranden enligt tidigare bestämmelser och gällande krav. Tillämpningsområdet beskrivs närmare i kapitel 2.

Bestämmelserna om certifiering och registrering av informationssystem har till vissa delar förändrats i och med att den nya lagen om kunduppgifter (784/2021) trädde i kraft den 1 november 2021. Överensstämmelseintyg enligt den tidigare klientlagen motsvarar i den gällande lagen om kunduppgifter intyg över bedömning av informationssäkerhet (informationssäkerhetsintyg).

Den punkt i THL:s föreskrift 4/2021 (Föreskrift om klassificering och certifiering av informationssystem för social- och hälsovården, utfärdad 9.12.2021), där certifiering enligt tidigare förfaranden föreskrivs, kan inte som sådan kan tillämpas under föreskrifternas ikraftträdandeperiod (se Bilaga 1 punkt 7). Den ifrågavarande punkten gäller informationssystem, för vilka en bedömning av informationssäkerheten har genomförts med godkänt resultat och för vilka samtestning har ansökts före den 1 september 2021.

Bedömning av informationssäkerheten är enligt lagen om kunduppgifter en förutsättning för att ta i bruk ett informationssystem och den är nödvändig för att säkerställa informationssäkerheten och dataskyddet i informationssystem som är avsedda att användas för produktion av tjänster. Informationssäkerhetsintyg utfärdas endast för genomförda bedömningar av informationssäkerheten. Det är inte möjligt att utfärda ett tidsbundet informationssäkerhetsintyg utan en ny bedömning av informationssäkerheten med stöd av den gällande lagen om kunduppgifter. Förfaranden under ikraftträdandet behöver preciseras för att kunna säkerställa att certifieringar slutförs på sådant sätt, att kraven på informationssäkerhet och de krav som andra gällande lagar ställer uppfylls när informationssystemen tas i användning.

2 Föreskriftens tillämpningsområde och THL:s behörighet att meddela föreskrifter

Föreskriften gäller förfaranden som ska iaktas vid påvisande av överensstämmelse med kraven i informationssystem som behandlar klient- eller patientuppgifter inom social- och hälsovården, i enlighet med kapitel 7 i lagen om kunduppgifter, Väsentliga krav på informationssystem och välbefinnandeapplikationer.

Denna föreskrift gäller informationssystem och producenter av informationssystemtjänster, som uppfyller alla följande krav:

1. producenten av informationssystemtjänsten har före den 1 september 2021 ansökt om samtestning för ett informationssystem som hör till klass A;
2. informationssystemet har tidigare genomgått en bedömning av informationssäkerheten enligt den tidigare klienthandlingslagen (159/2007);
3. producenten av en informationssystemtjänsten avser att som en del av certifieringen förnya det överensstämmelseintyg som har utfärdats under den tidigare lagens giltighetstid till ett informationssäkerhetsintyg i enlighet med den nya lagen; och

4. producenten av informationssystemtjänsten och FPA håller på att testa en eller flera av helheterna i FPA:s Kanta-samtestning: uppgradering av specifikationsversionen 2014–2016, sköta ärenden för minderåriga i Recepttjänsten, sköta ärenden för minderåriga i Patientdataarkivet.

I dessa informationssystem förutsätts den bedömning av informationssäkerheten som krävs för erhållande av ett informationssäkerhetsintyg, och i vilka tidigare gällande krav och förfaranden kan tillämpas enligt kapitel 12 i föreskrift 4/2021.

Institutet för hälsa och välfärd har behörighet att meddela föreskrifter inom tillämpningsområdet för denna föreskrift enligt följande: förfaranden som ska iakttas vid påvisande av överensstämmelse med kraven och innehållet i den utredning som ska ges (35 § 3 mom. i lagen om kunduppgifter); vad som är betydande avvikelser i väsentliga krav som ställs på informationssystem och om hur anmälningar om sådana ska göras (32 § 4 mom. i lagen om kunduppgifter) samt innehållet i de väsentliga kraven och vilka väsentliga krav som ska uppfyllas i de informationssystem som används i olika tjänster (34 § 4 mom. i lagen om kunduppgifter).

Bestämmelser om förutsättningarna för att ta ett system i användning för produktion av tjänster finns bland annat i 31 § i lagen om kunduppgifter (784/2021). En förutsättning för att ta ett informationssystem i användning är bland annat ett gällande intyg över bedömning av informationssäkerheten. Ett informationssystem kan inte tas i användning för produktion av tjänster, om dess tidigare överensstämmelseintyg har löpt ut eller om det inte finns aktuella uppgifter om informationssystemet i Valviras register över informationssystem. Denna föreskrift påverkar inte de ovan nämnda förutsättningarna för användning för produktion av tjänster, vilka gäller både producenter av informationssystemtjänster och tillhandahållare av social- och hälsovårdstjänster. Föreskriften och de bemyndiganden som ligger till grund för den inverkar inte på med vilken tidtabell tjänestetillhandahållarna tar nya systemversioner i användning. Föreskriften inverkar dock på certifieringen av systemen samt de förfaranden som tillämpas härvid och med vars hjälp förutsättningarna för att ta ett system i användning för produktion kan uppfyllas.

Föreskriften gäller inte välbefinnandeapplikationer.

De definitioner som har använts i denna föreskrift är i enlighet med kapitel 3 i THL:s föreskrift 4/2021.

3 Tidsbundna förfaranden för påvisande av överensstämmelse med kraven vid certifiering

Vid påvisande av överensstämmelse med kraven ska iakttas ett förfarande enligt antingen THL:s föreskrifter 4/2021 och 5/2021 eller ett förfarande enligt denna föreskrift.

Med ett förfarande enligt denna föreskrift avses följande.

1. Ett intyg över bedömning av informationssäkerheten kan beviljas utifrån en bedömning av informationssäkerheten som har utförts av ett bedömningsorgan för informationssäkerhet innan de pågående samtestningar (FPA:s samtestningsutlåtande) som krävs har slutförts med godkänt resultat. Benämningen på ett intyg som har beviljats på detta sätt är i denna föreskrift "tidsbundet informationssäkerhetsintyg".
2. I det intyg över bedömning av informationssäkerheten som utfärdas ska då tydligt antecknas "Intyget är tidsbundet medan de pågående samtestningarna slutförs och förutsätter en ny bedömning av informationssäkerheten i den samtestade systemversionen och utfärdande av ett nytt intyg". I intyget specificeras inte vilka samtestningar som är under arbete.

3. Det intyg som avses i punkt 1 kan utfärdas till att gälla högst till den 31 december 2022, och innan dess ska ett nytt intyg över bedömning av informationssäkerheten som gäller i högst tre år efter att lagen om kunduppgifter trätt i kraft utfärdas.
4. Efter bedömningen av informationssäkerheten enligt punkterna 1–3 ska systemet registreras i Valviras register över informationssystem.
5. I THL:s föreskrift 5/2021 (10.4 kapitlet, 6 punkten) fastställs att egenskaper hos ett system som används för produktion av tjänster som grundar sig på en föråldrad specifikationsversion är en betydande avvikelse¹. Den ifrågasättande betydande avvikelsen förhindrar inte användning för produktion av tjänster under giltighetstiden för denna föreskrift, om ett förfarande enligt denna föreskrift tillämpas på systemet.
6. Det är möjligt att ta i användning en version för produktion av tjänster även hos andra tjänstetillhandahållare än de som för närvarande använder systemet eller i situationer då organisationen hos den tjänstetillhandahållare som använder systemet förändras. Enligt den gällande lagen är en förutsättning för ibruktage ett sådant gällande intyg över bedömning av informationssäkerheten som beskrivs ovan och registrering av systemet i Valviras register över informationssystem.
7. De pågående samtestningarna ska slutföras för att påvisa att de gällande kraven på interoperabilitet i fråga om följande testningshelheter för samtestning uppfylls: uppgradering av specifikationsversionen 2014–2016, sköta ärenden för minderåriga i Recepttjänsten, sköta ärenden för minderåriga i Patientdataarkivet. Bedömningen av informationssäkerheten ska genomföras på nytt när samtestningen har slutförts i den systemversion som har samtestats eller som motsvarar kraven på samtestning av informationssäkerheten.
8. Efter bedömningen av informationssäkerheten enligt punkt 7 ska systemet registreras på nytt i Valviras register över informationssystem. I samband med registreringen ska producenten av informationssystemtjänsten till Valvira anmäla uppgifter om resultaten av godkända samtestningar och genomförandet av en ny bedömning av informationssäkerheten enligt bestämmelserna i föreskrift 4/2021.
9. I punkterna 1–3 och 7 i bedömningen av informationssäkerheten tillämpas såsom beskrivs i kapitel 12 i föreskrift 4/2021 antingen de informationssäkerhetskrav i föreskrift 1/2015 som gällde vid inledandet av certifieringsprocessen eller informationssäkerhetskraven enligt föreskrift 5/2021.
10. I system där man följer ett förfarande enligt föreskriften använder man systemblanketten enligt bilaga 4 till föreskrift 2/2016, och inte systemblanketten enligt bilaga 4 till föreskrift 5/2021, när man anmäler informationssystemets uppgifter till samtestning, bedömning av informationssäkerheten samt Valviras register över informationssystem. I punkten ”Systemets klass” på systemblanketten antecknar man dock den noggrannare klassen (t.ex. A2 eller A3) enligt föreskrift 4/2021. För en version av informationssystemet används endast en version av systemblanketten. Blanketten enligt föreskrift 5/2021 används dock senast i den fas, när det informationssäkerhetsintyg som har beviljats systemet enligt punkt 7 senare ska förnyas i enlighet med kraven i föreskrift 5/2021.

¹ Egenskaperna hos ett system som används för produktion av tjänster grundar sig på en föråldrad specifikationsversion, vars giltighetstid har löpt ut eller vars stöd i Kanta-tjänsterna har tagits bort eller håller på att tas bort så att systemet inte har kunnat eller inte kan övergå till implementering enligt gällande krav inom den tidsfrist som fastställts i författningar eller av tillsynsmyndigheten.

Det förfarande som beskrivs ovan vid påvisande av överensstämmelse med kraven kan tillämpas under giltighetstiden för denna föreskrift till den 31 december 2022. I fråga om övriga förfaranden och omständigheter som inte preciseras i denna föreskrift iakttas förfaranden enligt föreskrifterna 4/2021 och 5/2021.

Om producenten av informationssystemtjänsten iakttar det förfarande som beskrivs i denna föreskrift, ska producenten lämna en skriftlig anmälan om detta till bedömningsorganet för informationssäkerhet, FPA och Valvira innan bedömningen av informationssäkerheten inleds, dock senast den 9 juni 2022. Producenten av informationssystemtjänsten ska i samband med detta ange, huruvida man i bedömningen av informationssäkerheten iakttar kraven enligt föreskrift 1/2015 eller föreskrift 5/2021 såväl i fråga om bedömningen enligt punkt 1 som punkt 7².

Om producenten av informationssystemtjänsten iakttar det förfarande som beskrivs i denna föreskrift, ska producenten meddela detta skriftligt senast den 9 juni 2022 till de tjänstetillhandahållare som är dess kunder och vars användning för produktion av tjänster berörs. I samband med detta ska producenten av informationssystemtjänsten meddela, att systemet inte uppfyller kraven gällande samtestning med godkänt resultat av det testhelheter som föreskrivs i punkt 7.

4 Föreskriftens förhållande till andra föreskrifter

I bilaga 1 till denna föreskrift specificeras i detalj de punkter i THL:s föreskrifter 4/2021 och 5/2021 som inte tillämpas eller som tillämpas på ett avvikande sätt i informationssystem som är föremål för denna föreskrift. I bilaga 1 föreskrivs också hur de nämnda punkterna ska tillämpas med stöd av denna föreskrift i ifrågavarande informationssystem.

Alla punkter i föreskrifterna 4/2021 och 5/2021 som anges i bilaga 1 till denna föreskrift, tillämpas med de ändringar som föreskrivs i bilaga 1 till denna föreskrift. Tillämpningen gäller endast de informationssystem som definieras i kapitel 2 och som iakttar förfarandet enligt kapitel 3 i denna föreskrift under föreskriftens giltighetstid. Denna föreskrift påverkar inte innehållet i andra föreskrifter eller bestämmelser eller tidsfrister utöver det som beskrivs i kapitel 3 och 4 samt bilaga 1. Även omständigheter i bilagorna till föreskrifterna 4/2021 och 5/2021 tillämpas enligt denna föreskrift och bilaga 1.

5 Handledning och rådgivning

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.

Folkpensionsanstalten styr ibrukttagandet av informationssystem som ska anslutas till Kanta-tjänsterna.

² Det är möjligt att tillämpa kriterierna för bedömning av informationssäkerheten såväl enligt föreskrift 1/2015 och 5/2021 under giltighetstiden för den här föreskriften. Om man som kriterier för bedömning av informationssäkerheten i punkt 7 iakttar kraven enligt föreskrift 1/2015, kan informationssäkerhetsintyget utfärdas att gälla i högst tre år efter att lagen om kunduppgifter trätt i kraft enligt kapitel 12 i föreskrift 4/2021. Om man som kriterier för bedömning av informationssäkerheten iakttar kraven enligt föreskrift 5/2021, kan informationssäkerhetsintyget utfärdas att gälla i högst tre år efter att intyget har beviljats, se även bilaga 1 punkt 7.

6 Ikraftträdande

Den här föreskriften träder i kraft den 29 mars 2022 och den gäller till den 31 december 2022.

Sirpa Soini
Avdelningsdirektör

Jarmo Kärki
Enhetschef

Sändlista

Folkpensionsanstalten
Bedömningsorgan för informationssäkerhet
Tillverkare av klient- och patientdatasystem samt producenter av informationssystemtjänster för social- och hälsovården
Producenter av informationsförvaltningstjänster och ICT-tjänster för social- och hälsovården
Tillhandahållare av social- och hälsovårdstjänster
Social- och hälsovårdsministeriet
Finlands Kommunförbund rf
Tillstånds- och tillsynsverket för social- och hälsovården Valvira
Transport- och kommunikationsverket Traficom
Dataombudsmannens byrå
Regionförvaltningsverken

Denna föreskrift har publicerats i myndigheternas föreskriftssamlingar

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

registratorskontoret vid Institutet för hälsa och välfärd samt på

Internet-adressen <https://thl.fi/fi/web/tiedonhallinta-sosiaalija-terveysalalla/maaraykset-ja-maarittelyt/maaraykset>

Bilaga 1. Undantag och preciseringar av förfaranden enligt föreskrifterna 4/2021 och 5/2021

Samtliga undantag och preciseringar i bilagan iakttas endast under giltighetstiden för denna föreskrift 1/2022 och endast enligt avgränsningen av målgruppen för denna föreskrift.

1.

Originaltext (THL:s föreskrift 4/2021, 7.3 kap. 10 mom.): *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.*

Specifisering: Ett tidsbundet informationssäkerhetsintyg för slutförande av certifiering kan enligt kapitel 3 i denna föreskrift utfärdas att gälla till den 31 december 2022. Ett intyg över bedömning av informationssäkerheten i en samtestad version ska enligt föreskrift 4/2021 utfärdas att gälla tre år efter att lagen om kunduppgifter trätt i kraft, om man vid bedömningen iakttar kriterierna enligt föreskrift 1/2015 och tre år efter att intyget har beviljats om kriterierna enligt föreskrift 5/2021 iakttas vid bedömningen.

2.

Originaltext (THL:s föreskrift 4/2021, 7.3 kap. 11 och 12 mom.): *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 FPA att det system som är föremål för samtestning inte kommer att genomgå ändringar som kan påverka uppfyllandet av informationssäkerhetskraven.*

Undantag: Tillämpas inte på tidsbundet informationssäkerhetsintyg enligt kapitel 3: ett tidsbundet informationssäkerhetsintyg kan utfärdas efter en godkänd bedömning av informationssäkerheten, även om det inte finns tillgång till FPA:s utlåtande över godkänt resultat av samtestning för pågående samtestning. Punkten enligt originaltexten tillämpas på det informationssäkerhetsintyg som beviljas den samtestade versionen efter det tidsbundna intyget.

3.

Originaltext (THL:s föreskrift 4/2021, 8 kap. 2 mom.): *Om informationssystemet hör till klass A1, A2 eller A3 och ska certifieras, förutsätter registreringen i Valvira 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.*

Undantag: Registreringen görs enligt 3 kapitlet 4 punkten i denna föreskrift med stöd av det tidsbundna informationssäkerhetsintyget. Registreringen ska förnyas enligt kapitel 3 och föreskrift 4/2021 för en samtestad systemversion, då samtestningen i förhållande till nyare versioner av föreskriften och bedömningen av informationssäkerheten i den samtestade versionen har genomförts.

4.

Originaltext (THL:s föreskrift 4/2021, 9 kap. 1 mom.): *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.*

Specificering: Punkten tillämpas så att informationssystem som är föremål för sådana pågående samtestningar som avses i kapitel 2 i denna föreskrift och som grundar sig på krav enligt tidigare föreskriftsversioner, inte utgör en sådan betydande avvikelse som förhindrar ibruktagande. De krav som är föremål för pågående samtestning ska uppfyllas och samtestningen av dem ska genomföras med godkänt resultat innan denna föreskrift upphör att gälla och innan det tidsbundna informationssäkerhetsintyget enligt kapitel 3 upphör att gälla. Se även punkt 3.

5.

Originaltext (THL:s föreskrift 4/2021, 9 kap. 4 mom.): *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 i denna föreskrift). 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.*

Undantag: Tillämpas på så sätt, att av ett system som hör till förordningens målgrupp och som ska anslutas till Kanta-tjänsterna krävs det ett förfarande enligt kapitel 3 i punkterna 1–6, om att det redan används för produktion av tjänster enligt tidigare specifikationer för godkända samtestningar och som stöds för närvarande i Kanta-tjänsterna, och samtestning av de krav enligt punkt 7 i kapitel 3 i denna föreskrift som gäller systemets användningsändamål enligt nyare specifikationsversioner som förutsätts i Kanta-tjänsterna har inletts.

6.

Originaltext (THL:s föreskrift 4/2021, 10 kap. 3 mom.): *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.*

Undantag: Tillämpas inte på tidsbundet informationssäkerhetsintyg, se kapitel 3.

7.

Originaltext (THL:s föreskrift 4/2021, 12 kap. 5 mom.): *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. (...) System vars tidigare överensställelseintyg (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 överensställelseintyget blir ogiltigt.*

Undantag: Förfaranden enligt föreskrift 4/2021 tillämpas på informationssystem som är föremål för denna föreskrift med de preciseringar och avvikelser som beskrivs i denna föreskrift under dess giltighetstid. På system vars samtestning har inletts före den 1 september 2021 kan certifieringsprocessen slutföras under giltighetstiden för denna föreskrift, och inte endast inom sex månader efter att föreskrift 4/2021 trädde i kraft. Specifiering: Om bedömningen av informationssäkerheten enligt 3 kapitlet 7 punkten genomförs utifrån krav som gällt tidigare, kan överensstämmelseintyget i enlighet med föreskrift 4/2021 utfärdas att gälla i högst tre år efter att den gällande lagen om kunduppgifter trädde i kraft.

8.

Originaltext (THL:s föreskrift 4/2021, 12 kap. 8 mom.): *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.*

Undantag: I system som hör till målgruppen för denna föreskrift är det frågan om förnyelse av intyg som har beviljats med stöd av den tidigare lagen, och som redan har föräldrats eller som går ut, till ett informationssäkerhetsintyg enligt den gällande lagen. Tidigare överensstämmelseintyg ska förnyas till informationssäkerhetsintyg enligt den gällande lagen om kunduppgifter och föreskrift 4/2021 på det sätt och med den tidtabell som beskrivs i kapitel 3 i denna föreskrift, och innan dess kan ett tidsbundet informationssäkerhetsintyg utfärdas att gälla enligt kapitel 3 i denna föreskrift.

9.

Originaltext (THL:s föreskrift 5/2021, 7 kap. 6 och 8 mom.): *Implementering eller uppfyllande av de krav som förutsätts av profilerna som ingår i systemets användningsändamål samt verifiering av dem vid samtestning eller bedömning av informationssäkerheten till den del kraven kan verifieras vid certifieringen, är en förutsättning för att certifieringen av informationssystem i klass A ska godkännas och för att de ska kunna tas i användning för produktion av tjänster.*

Om det är fråga om ett informationssystem i klass A förutsätter registreringen i Valviras register över informationssystem att de krav på interoperabilitet och informationssäkerhet som hänför sig till funktionerna enligt profilen har verifierats med godkänt resultat vid samtestning och bedömning av informationssäkerheten och att informationssystemet har fått ett informationssäkerhetsintyg.

Specifiering: I fråga om kraven vid samtestning tillämpas kapitel 3 i denna föreskrift jämte punkterna 2, 3, 4, 5 och 6 i denna bilaga.

10.

Originaltext (THL:s föreskrift 5/2021, 8 kap. 13 punkten, 7 och 13 mom.): *De krav på systemets funktionalitet (funktioner och datainnehåll, punkterna 3–8) som gäller specifikationerna i anslutning till Kanta-tjänsterna har implementerats, uppfyllts och dokumenterats så att systemet kan genomgå nödvändiga samtestningar med godkänt resultat enligt anvisningarna för FPA:s samtestning med Kanta-tjänsterna.*

En förutsättning för att ta i användning ett informationssystem i klass A2 eller A3 för produktion av tjänster är att alla funktioner och datainnehåll i systemet som är anslutna till Kanta-tjänsterna och som är föremål för samtestning har samtestats med godkänt resultat (se även föreskrift 4/2021, kap. 9).

Producenten av en informationssystemtjänst ska i enlighet med 32 § ge akt på ändringar i väsentliga krav och göra justeringar i enlighet med ändringarna. Om ändringarna förutsätter en ny samtestning eller en ny bedömning av informationssäkerheten, ska dessa åtgärder vidtas innan den version av informationssystemet som innehåller ändringarna tas i användning för produktion av tjänster.

Specifisering: I fråga om kraven vid samtestning tillämpas kapitel 3 i denna föreskrift jämte punkterna 2, 3, 4, 5, 6 och 9 i denna bilaga.

11.

Originaltext (THL:s föreskrift 5/2021, 8 kap. 14 mom.) *Producenten av en informationssystemtjänst ska åtminstone vid ansökan om förnyelse av informationssäkerhetsintyget kontrollera att informationssystemets egenskaper som ska anslutas till Kanta-tjänsterna har samtestats i enlighet med gällande specifikationer och specifikationsversioner samt kapitel 10 i föreskrift 4/2021.*

Undantag: Tillämpas enligt kapitel 3 och punkt 4 i denna bilaga: punkten tillämpas inte för de krav, som är föremål för pågående samtestning, när man vill ansöka om ett tidsbundet informationssäkerhetsintyg.

12.

Originaltext (THL:s föreskrift 5/2021, 10.3 kap. 1 punkten): *Ett system som används för produktion av tjänster eller som certifieras ska uppfylla alla väsentliga krav som implementerats i systemet i enlighet med gällande specifikationer, om specifikationerna innehåller krav som motsvarar systemets klass och användningsändamål.*

Specifisering: Tillämpas enligt kapitel 3 och punkt 4 i denna bilaga: punkten tillämpas i fråga om krav som är föremål för samtestning i de system där man iakttar ett förfarande enligt denna föreskrift endast i fråga om 3 kapitlet 7–8 punkten, då samtestningen och bedömningen av informationssäkerheten slutförs inom tidsfristerna enligt denna föreskrift.

13.

Originaltext (THL:s föreskrift 5/2021, 10.4 kap. 5 punkten): *Ett föråldrat överensstämmelseintyg eller intyg över bedömning av informationssäkerhet för ett system som används för produktion av tjänster, särskilt om förnyandet av intyget drar ut på tiden av orsaker som beror på tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst.*

Specifisering: Ett överensstämmelseintyg som går ut eller har gått ut kan förnyas för viss tid innan samtestningen och bedömningen av informationssäkerheten i en samtestad version har slutförts i enlighet med kapitel 3 i denna föreskrift. Valvira fattar beslut om anteckning av betydande avvikelser i registret över informationssystem.

14.

Originaltext (THL:s föreskrift 5/2021, 10.4 kap. 6 punkten): *Egenskaperna hos ett system som används för produktion av tjänster grundar sig på en föråldrad specifikationsversion, vars giltighetstid har löpt ut eller vars stöd i Kanta-tjänsterna har tagits bort eller håller på att tas bort så att systemet inte har kunnat eller inte kan övergå till implementering enligt gällande krav inom den tidsfrist som fastställts i författningar eller av tillsynsmyndigheten.*

Specifisering: Den ifrågavarande omständigheten är inte en betydande avvikelse som förhindrar att systemet tas i bruk under giltighetstiden för denna föreskrift i informationssystem som hör till målgruppen för denna föreskrift,

om en nyare specifikationsversion är föremål för samtestning under pågående certifiering av systemet. Valvira kan dock göra en anteckning om betydande avvikelse i registret över informationssystem.

15. Originaltext (THL:s föreskrift 5/2021, 10.4 kap. 3 och 4 mom.): *Om man i certifieringsprocessen upptäcker en sådan avvikelse från de väsentliga kraven som skulle leda till en betydande avvikelse i användningen för produktion av tjänster, kan certifieringen inte slutföras med godkänt resultat innan den omständighet som orsakar avvikelsen har justerats eller innan de fellägen som beror på avvikelsen har förhindrats på annat sätt. Krav som inte uppfylls eller som uppfylls på ett bristfälligt sätt kan medföra behov av korrigeringsåtgärder innan samtestningen eller bedömningen av informationssäkerheten godkänns, enligt beskrivningen i avsnitt 10.2.*

Specifisering: För det system som används tillämpas ett tidsbundet informationssäkerhetsintyg och ett förfarande enligt kapitel 3 i föreskriften och punkt 13 i denna bilaga samt punkt 1 i de övriga bilagorna: i samband med beviljande av ett tidsbundet informationssäkerhetsintyg granskas inte de krav, som är föremål för en pågående samtestning. Både när det gäller ett tidsbundet informationssäkerhetsintyg och bedömning av informationssäkerhetskraven för en version som samtestats ska informationssäkerhetskraven uppfyllas enligt originaltexten.

FÖRÅLDRAD