Informationsförmedlare
Information och styrning av informationshanteringen 3.5.2024

FÖRESKRIFT OM KLASSIFICERING OCH CERTIFIERING AV INFORMATIONSSYSTEM OCH VÄLBEFINNANDEAPPLIKATIONER INOM SOCIAL- OCH HÄLSOVÅRDEN

Bestämmelser om bemyndigande

Lag om behandling av kunduppgifter inom social- och hälsovården (703/2023) 79 § 4 moment, 82 § 4 moment, 84 § 4 moment och 85 § 3 moment.

Målgrupper

Producenter av informationssystemtjänster och tillverkare av informationssystem för social- och hälsovården

Tillverkare av välbefinnandeapplikationer

Producenter av informationsförmedlingstjänster för kunduppgifter

Tjänstetillhandahållare inom social- och hälsovården

Apotek

Folkpensionsanstalten

Bedömningsorgan för informationssäkerhet

Mellanhänder

Ikraftträdande

Föreskriften träder i kraft den 10. maj 2024 och gäller tills vidare.

Denna föreskrift ersätter THL:s tidigare föreskrifter 4/2021 (föreskrift om klassificering och certifiering av informationssystem för social- och hälsovården) och 6/2021 (om de väsentliga kraven på och certifieringen av välbefinnandeapplikationer som behandlar uppgifter om välbefinnande och som ansluts till datalagret för egna uppgifter). Lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023) upphäver lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (784/2021), som gett fullmakt att utfärda den tidigare föreskriften. De författningar på lägre nivå som utfärdats med stöd av lagen om klientuppgifter upphävs.

Innehåll

1 Föreskriftens syfte

I denna föreskrift beskrivs de förfaranden och ansvar som ska genomföras i samband med klassificeringen av informationssystem och välbefinnandeapplikationer inom social- och hälsovården samt vid verifieringen och certifieringen av de väsentliga krav som ställs på dem. Föreskriften styr:

- lämnandet av de utredningar som krävs för överensstämmelse
- den samtestning som ingår i certifieringen
- den bedömning av informationssäkerheten som ingår i certifieringen
- registreringen och ibruktagandet av informationssystem och välbefinnandeapplikationer.

2 Definitioner

I denna föreskrift och THL:s föreskrift 5/2024 används följande begrepp:

- **Tillverkare av ett informationssystem** (lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023), nedan lagen om kunduppgifter), 3 § 1 mom. 21 punkten)
  - den som ansvarar för planeringen och tillverkningen av ett informationssystem för social- och hälsovården.
- **Producent av en informationssystemtjänst** (lagen om kunduppgifter 3 § 1 mom. 20 punkten)
  - den som tillhandahåller eller genomför ett informationssystem för en tjänstetillhandahållare. Producenten av en informationssystemtjänst ansvarar i egenskap av informationssystemets tillverkare, för tillverkarens räkning eller för en eller flera tillverkares räkning, för de krav som ställs på informationssystemet.
  - Producenten av en informationssystemtjänst ansvarar också i enlighet med lagen om kunduppgifter, denna föreskrift och föreskrift 5/2024 för klassificeringen av informationssystem, certifieringen av informationssystem som hör till klass A och registreringen av informationssystem som hör till klass A eller B i Valviras register över informationssystem.
- **Tjänstetillhandahållare** (lagen om kunduppgifter 3 § 1 mom. 11 punkten)
  - Myndigheter, offentligrättsliga samfund och enskilda näringsidkare som ordnar eller tillhandahåller socialservice eller hälso- och sjukvårdstjänster samt arbetsgivare som avses i 7 § 1 mom. 2 punkten i lagen om företagshälsovård (1383/2001)[1]:
    - En yrkesutbildad person inom hälso- och sjukvården som är en självständig yrkesutövare (lagen om tillsynen över social- och hälsovården (741/2023) och lagen om yrkesutbildade personer inom hälso- och sjukvården (554/1994)).
    - Utöver definitionen i lagen om kunduppgifter gäller de skyldigheter som åläggs tjänstetillhandahållare i denna föreskrift på motsvarande sätt och i den omfattning som avses i lagen om elektroniska recept (61/2007) och 82, 84 och 90 § i lagen om kunduppgifter även apotek enligt 38 § i läkemedelslagen (395/1987)[2].

[1] Definitionen av en tjänstetillhandahållare i 3 § 1 mom. 11 punkten i lagen om kunduppgifter kommer sannolikt att ändras i regeringens proposition med förslag till lag om ändring av lagen om kunduppgifter, som bereds av Social- och hälsovårdsministeriet. Den eventuella ändringen ska också beaktas vid tillämpningen av föreskrifterna 4/2024 och 5/2024.

[2] Mer information om tillämpningen av föreskrifterna 4/2024 och 5/2024 i apotekens informationssystem och webbtjänster finns i kapitel 6.6 i bilaga 1 till föreskrift 5/2024.

- **Informationssystem** (lagen om kunduppgifter 3 § 1 mom. 19 punkten)
    - En programvara eller ett system eller delsystem som används i enlighet med de egenskaper som har planerats av tillverkaren för elektronisk behandling av kundhandlingar, för registrering av handlingarna i de riksomfattande informationssystemtjänsterna eller anslutning till dessa tjänster, eller med vars hjälp en yrkesutbildad person inom social- eller hälsovården kan använda uppgifter om välbefinnande. I denna föreskrift och i föreskrift 5/2024 med tillhörande bilagor används även den kortare termen ”system” för att beteckna informationssystem.

- **Delsystem** (lagen om kunduppgifter 3 § 1 mom. 19 punkten)
    - Ett informationssystem eller en 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 avsett att anslutas till andra informationssystem eller delsystem som behandlar kunduppgifter. Ett delsystem kan certifieras och tas i bruk som en del av en större modulär informationssystemhelhet och registreras separat, om a) delsystemets användningsändamål och de väsentliga krav som gäller delsystemet beskrivs och verifieras på motsvarande sätt som för informationssystem i allmänhet, och om b) delsystemets anslutning till andra informationssystem eller delsystem beskrivs i enlighet med föreskrifterna[3].

- **Uppgifter om välbefinnande** (lagen om kunduppgifter 3 § 1 mom. 9 och 18 punkten)
    - Sådana uppgifter som en person producerat och administrerar om sin hälsa och sitt välbefinnande och som personen själv har fört in i datalagret för egna uppgifter.
    - Enligt motiveringen till den gällande lagen om kunduppgifter (RP 246/2022 rd) kan det också vara fråga om sådana uppgifter som en anordning som personen använder producerar.
    - Begreppet ”uppgift om välbefinnande” används också i vidare bemärkelse, som beskrivs i tjänsten Ordlistor för social- och hälsovården; föreskrifterna 4/2024 och 5/2024 utgår dock från definitionerna och avgränsningarna i lagen om kunduppgifter.

- **Datalagret för egna uppgifter** (lagen om kunduppgifter 3 § 1 mom. 17 punkten, där benämningen informationsresursen för egna uppgifter används)
    - En inom de riksomfattande informationssystemtjänsterna upprättad centraliserad informationsresurs för bevarande och behandling av uppgifter om välbefinnande.

- **Välbefinnandeapplikation** (lagen om kunduppgifter 3 § 1 mom. 18 punkten)
    - En applikation i anslutning till datalagret för egna uppgifter med vilken uppgifter om välbefinnande behandlas, samt en applikation till vilken en person (medborgare) kan få sina kunduppgifter från den riksomfattande informationsresursen för kunduppgifter, receptcentret och informationshanteringstjänsten.
        - Välbefinnandeapplikationen kan anknyta till verksamheten hos en tjänstetillhandahållare inom social- och hälsovården eller vara oberoende av den[4].
        - Begreppet ”välbefinnandeapplikation” används också i vidare bemärkelse, som beskrivs i tjänsten Ordlistor för social- och hälsovården; föreskrifterna 4/2024 och 5/2024 utgår dock från definitionerna och avgränsningarna i lagen om kunduppgifter.
        - Programvaran eller informationssystemet kan till sitt användningsändamål vara både ett informationssystem enligt definitionen i 3 § 19 punkten i lagen om kunduppgifter och en välbefinnandeapplikation enligt 18 punkten.

[3] Ytterligare information: föreskrift 5/2024 bilaga 1, kapitel 6.3.
[4] Ytterligare information: föreskrift 5/2024 bilaga 1, kapitel 6.5.

- **Digital tjänst**
  - Den allmänna termen digital tjänst används i föreskrifterna 4/2024 och 5/2024 med hänvisning till både välbefinnandeapplikationer och digitala ärendetjänster. Termen omfattar både informationssystem och välbefinnandeapplikationer med egenskaper som är avsedda att vara direkt tillgängliga för medborgarna. Till de digitala tjänsterna kan räknas både digitala ärendetjänster och sådana välbefinnandeapplikationer som är anslutna till Kanta-tjänster såsom datalagret för egna uppgifter. Det är också möjligt att ett informationssystem eller en digital tjänst uppfyller definitionen av både välbefinnandeapplikation och informationssystem i lagen om kunduppgifter.
- **Digital ärendetjänst**
  - Ett informationssystem eller delsystem som tjänstetillhandahållaren tillhandahåller sina kunder, som är avsett för behandling av klient- eller personuppgifter och som används av en medborgare och också kan användas av yrkesutbildade personer. En digital ärendetjänst kan till exempel uppfylla kraven i profilen ”Tjänstetillhandahållarens digitala ärendetjänst” (föreskrift 5/2024 bilaga 3h), som beskriver kraven på tjänsten förutsatt att det inte är fråga om en välbefinnandeapplikation. Se även *välbefinnandeapplikation*, *digital tjänst*[5].
- **Kanta-tjänsterna** (lagen om kunduppgifter 65 §)
  - De riksomfattande informationssystemtjänster inom social- och hälsovården som ordnas och förvaltas av Folkpensionsanstalten (nedan FPA).
- **Informationsförmedlingsservice för kunduppgifter**
  - Ett informationssystem eller delsystem som en organisation inom social- och hälsovården eller ett apotek använder vid anslutningen till Kanta-tjänsterna och via vilket kunduppgifter som producerats i ett annat system överförs till Kanta-tjänsterna eller via vilket kunduppgifter som finns i Kanta-tjänsterna används. Informationsförmedlingsservicen för kunduppgifter har inga egenskaper som riktas till slutanvändarna av informationssystemet som ansluts till Kanta-tjänsterna. Mer information finns i bilaga 1: Exempel på klassificeringen av system.
- **Väsentliga krav** (lagen om kunduppgifter 84 §)
  - Nationellt uppställda krav på informationssystemets och välbefinnandeapplikationens funktionalitet, interoperabilitet, informationssäkerhet eller tillgänglighet. Ett väsentligt krav stöder sig på de källdokument som det hänvisar till, såsom olika författningar eller definitioner.
- **Funktionellt krav** (lagen om kunduppgifter 80 §, 84–86 §, krav på funktionalitet)
  - Funktionalitet eller förmåga att behandla datainnehåll om vars genomförande i informationssystemet eller välbefinnandeapplikationen det föreskrivs i 84 § i lagen om kunduppgifter och THL:s föreskrift 5/2024 om väsentliga krav. De funktionella krav som ingår i de väsentliga kraven beskrivs i förteckningen över väsentliga krav i bilaga 2 till THL:s föreskrift 5/2024 under avsnitten ”Toiminnot” (funktioner) och ”Tietosisällöt” (datainnehåll).
- **Profil**
  - Dokument som beskriver de nationella minimikraven på funktioner, datainnehåll och informationssäkerhetskrav som ska implementeras i informationssystemet eller välbefinnandeapplikationen i enlighet med systemets eller välbefinnandeapplikationens användningsändamål.

[5] Den allmänna termen ”ärendetjänst” används ofta om digitala tjänster som också har egenskaper för välbefinnandeapplikationer eller kundkommunikation.

- **Certifiering** (lagen om kunduppgifter 3 § 1 mom. 23 punkten)
    - Ett förfarande genom vilket det verifieras att informationssystem och välbefinnandeapplikationer uppfyller de väsentliga krav som ställs på dem för att de ska få användas för produktion.
- **Verifiering**
    - Ett förfarande som påvisar att ett informationssystem eller en välbefinnandeapplikation uppfyller de krav som ställs på den. Verifieringssätten är bland annat testning av programvaran, genomgång av informationssystemets eller välbefinnandeapplikationens dokumentation eller anvisningar eller genomgång av meddelanden, loggar eller andra produkter som programvaran producerar. Verifieringen kan också omfatta en dokumenterad intervju med programvarutillverkaren, producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation. Verifiering behandlas närmare i kapitel 10 i THL:s föreskrift 5/2024.
- **Samtestning** (lagen om kunduppgifter 86 §).
    - Interoperabilitetstestning där informationssystemets eller välbefinnandeapplikationens interoperabilitet med Kanta-tjänsterna och andra informationssystem eller välbefinnandeapplikationer som anslutits till dem verifieras. FPA ordnar samtestning och utfärdar ett intyg enligt 86 § i lagen om kunduppgifter över att kraven på interoperabilitet uppfylls (positivt samtestningsutlåtande) när de krav som ska testas har verifierats med godkänt resultat. Som bilaga till samtestningsutlåtandet bifogas en mer detaljerad samtestningsrapport.
- **Bedömning av informationssäkerhet** (lagen om kunduppgifter 87 §)
    - En del av certifieringsprocessen där ett godkänt bedömningsorgan för informationssäkerhet verifierar informationssäkerhetskraven i enlighet med 87 § i lagen om kunduppgifter och utfärdar ett intyg över bedömning av informationssäkerhet.
- **Intyg över bedömning av informationssäkerhet eller informationssäkerhetsintyg** (lagen om kunduppgifter 87 §)
    - Ett intyg som ett godkänt bedömningsorgan utfärdar när ett system, ett delsystem eller en välbefinnandeapplikation har genomgått en bedömning av informationssäkerhet med godkänt resultat.

Många av de begrepp som används grundar sig på definitionerna i lagen om kunduppgifter och tidigare föreskrifter. Centrala begrepp finns också i THL:s tjänst Ordlistor för social- och hälsovården, och denna föreskrift fungerar som en källa till begreppen. I föreskrifterna 4/2024 och 5/2024 hänvisas med termen ”föreskrift” till THL:s föreskrifter, och när det hänvisas till andra myndigheters föreskrifter preciseras vilken myndighets föreskrift det är fråga om.

3 Föreskriftens tillämpningsområde

Institutet för hälsa och välfärd (nedan THL) har med stöd av 84 § 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 system och välbefinnandeapplikationer som används i olika tjänster. Enligt 85 § 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 79 § i kunduppgiftslagen får THL meddela föreskrifter om klassificeringen av system.

Denna föreskrift gäller de förfaranden som ska iakttas och utredningar som ska ges vid klassificering av informationssystem och välbefinnandeapplikationer som behandlar klient- eller patientuppgifter inom social- och

hälsovården och vid påvisande av systemens och välbefinnandeapplikationernas överensstämmelse med kraven.[6] Föreskriften gäller

- system som behandlar klient- och patientuppgifter och som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna (Kanta-tjänsterna) (klass A)
- andra system 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)
- välbefinnandeapplikationer som ansluts till datalagret för egna uppgifter och med vilka uppgifter om välbefinnande behandlas (klass A)
- välbefinnandeapplikationer till vilka en person kan få sina kunduppgifter från den riksomfattande informationsresursen för kunduppgifter, receptcentret och informationshanteringstjänsten (klass A).

Största delen av skyldigheterna att certifiera, klassificera och verifiera väsentliga krav ankommer på producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation. Vissa skyldigheter inom ämnesområdet gäller dock även tillhandahållare av social- och hälsovårdstjänster och apotek, se bl.a. föreskrift 4/2024 kap. 9 ”Förutsättningar för ibruktagandet av informationssystem och välbefinnandeapplikationer” och föreskrift 5/2024 kap. 9 ”Uppfyllandet av väsentliga krav/tjänstetillhandahållare”. Om producenten av en informationssystemtjänst är en annan aktör än den som tillverkar informationssystemet är det viktigt att komma överens om aktörernas ansvar (mer information finns i föreskrift 5/2024, bilaga 1 kapitel 2 ”Översikt över användningen av väsentliga krav”).

Denna föreskrift gäller inte uppföljningen eller övervakningen av överensstämmelsen med kraven. Producenten av en informationssystemtjänst och tjänstetillhandahållaren ansvarar dock för överensstämmelsen med kraven för system som används för produktion av tjänster.

4 Föreskriftens begränsningar och förhållande till andra författningar och dokument

THL har utfärdat en separat föreskrift om väsentliga krav på funktionalitet och informationssäkerhetskrav hos system och välbefinnandeapplikationer avsedda för behandling av klient- och patientuppgifter (THL:s föreskrift 5/2024: Föreskrift om väsentliga krav på informationssystem och välbefinnandeapplikationer inom social- och hälsovården).

THL har utfärdat en separat föreskrift om de redogörelser och krav som ska tas in i informationssäkerhetsplanen (föreskrift 3/2024).

Med denna föreskrift ersätts THL:s tidigare föreskrifter 4/2021: Föreskrift om klassificering och certifiering av informationssystem för social- och hälsovården samt 6/2021: Föreskrift om de väsentliga kraven på och certifieringen av välbefinnandeapplikationer som behandlar uppgifter om välbefinnande och som ansluts till datalagret för egna uppgifter. Denna föreskrift ersätter innehållet i ifrågavarande föreskrifter om klassificering och certifiering samt verifiering av väsentliga krav enligt tidigare författningar.

Denna föreskrift och dess ikraftträdandedatum och övergångsbestämmelser påverkar inte tidsfristerna för tjänstetillhandahållarnas skyldigheter enligt 67 och 102 § i lagen om kunduppgifter att ansluta sig som användare av de riksomfattande informationssystemtjänsterna.

Denna föreskrift tillämpas inte på system vars användningsändamål uteslutande är ändamål enligt föreskrift 1/2022, som utfärdats av Tillståndsmyndigheten för social- och hälsovårdsdata (Findata) (Krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer). Findatas föreskrift tillämpas på alla de användningsändamål

[6] lagen om kunduppgifter, 12 kap. ”Väsentliga krav på informationssystem och välbefinnandeapplikationer”

som föreskrivs i lagen om sekundär användning, för vilka det enligt lagen om sekundär användning behövs dataanvändningstillstånd. Dessa användningsändamål är vetenskaplig forskning, statistikföring, undervisning samt myndigheternas planerings- och utredningsuppgifter.

Målområdet för denna föreskrift är inte bestämmelserna om medicintekniska produkter. Denna föreskrift gäller system avsedda för behandling av kunduppgifter inom social- och hälsovården samt välbefinnandeapplikationer enligt definitionen i kapitel 2. 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. Om informationssystemet eller välbefinnandeapplikationen uppfyller definitionen av en medicinteknisk produkt ska man beakta både lagen om kunduppgifter och bestämmelserna om medicintekniska produkter, såsom Europaparlamentets och rådets förordning (EU) 2017/745, förordningen om medicintekniska produkter för in vitro-diagnostik (EU) 2017/746 samt lagen om medicintekniska produkter 719/2021. Produkterna ska anmälas till Säkerhets- och utvecklingscentret för läkemedelsområdet Fimeas register eller till EUDAMED-databasen i enlighet med bestämmelserna ovan. Denna föreskrift och föreskrift 5/2024 är oberoende av på vilket sätt programvaror eller utrustningar klassificeras enligt bestämmelserna om medicintekniska produkter. Tillverkaren av ett system eller en välbefinnandeapplikation ska ta ställning till om systemet, en del av systemet eller välbefinnandeapplikationen ska klassificeras som en medicinteknisk produkt.

Med certifiering enligt denna föreskrift och föreskrift 5/2024 avses inte frivillig certifiering av personuppgiftsansvariga eller personuppgiftsbiträden ((EU) 2016/679 (artikel 42–44 i *den allmänna dataskyddsförordningen*[7] Certifiering enligt denna föreskrift betraktas således inte som en utredning av huruvida dataskyddsförordningen efterlevs eller ansvarsskyldigheten enligt dataskyddsförordningen uppfylls. Den certifiering som föreskrivs i lagen om kunduppgifter påverkar inte de befogenheter som dataombudsmannens byrå har på basis av dataskyddslagstiftningen.

5 Klassificering av och allmänt ansvar för informationssystem och välbefinnandeapplikationer

Informationssystemen för social- och hälsovården delas in i klasserna A (kräver certifiering) och B (kräver inte certifiering). Välbefinnandeapplikationer hör till klass A. Informationssystem och välbefinnandeapplikationer i klass A klassificeras närmare i klasserna A1, A2 och A3 enligt denna föreskrift. Klassificeringsgrunderna beskrivs i detta kapitel, och exempel på klassificering av olika typer av system finns i bilaga 1.

Producenten av informationssystemtjänsten ansvarar för klassificeringen. Klassificeringen påverkar vilka åtgärder för certifiering och registrering (se kapitel 7) som ska vidtas för systemen och välbefinnandeapplikationerna.

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska bedöma riskerna i anslutning till det system eller den välbefinnandeapplikation som klassificerats och i anslutning till den därtill hörande behandlingen av kunduppgifter. Systemets informationssäkerhet ska planeras och dimensioneras utifrån riskbedömningen. Bedömningen av systemets risknivå och av omfattningen av behandlingen av kunduppgifter ska utföras på de grunder som beskrivs i bilaga 1 till denna föreskrift, Exempel på klassificering av system och välbefinnandeapplikationer.

Till *klass A* hör system och välbefinnandeapplikationer 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.

[7] 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 95/46/EG (allmän dataskyddsförordning)

När det gäller system och välbefinnandeapplikationer är klass A vidare indelad i klasserna A1, A2 och A3 utifrån systemets och välbefinnandeapplikationens användningsändamål, typen och omfattningen av de uppgifter som behandlas i systemet samt risknivån och graden av kritikalitet, så som följer:

- 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 genom samtestning av interoperabilitet med ett annat system, men som är föremål för informationssäkerhetskrav som ska verifieras. Till klass A1 hör också sådana system eller delsystem som involverar omfattande bevarande eller behandling av kunduppgifter, även om systemen inte är anslutna till Kanta-tjänsterna eller hör till klasserna A2 eller A3. Risknivån för ett system i klass A1 kan vara basnivå eller hög nivå. Även en digital ärendetjänst eller välbefinnandeapplikation vars Kanta-anslutning sker via ett annat system eller en annan välbefinnandeapplikation kan höra till klass A1.
- A2: System eller välbefinnandeapplikationer som kräver samtestning och bedömning av informationssäkerheten och som används för ett begränsat datainnehåll eller användningsändamål. Systemen eller applikationerna 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 tillhandahållare av social- och hälsovårdstjänster, till exempel i fråga om allt datainnehåll som behövs i verksamheten eller alla skyldigheter i samband med Kanta-tjänsterna. Risknivån för ett system eller en välbefinnandeapplikation i klass A2 kan vara hög nivå eller basnivå.
- 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 för tjänstetillhandahållare inom social- och hälsovården. I systemen behandlas i stor utsträckning kunduppgifter som hänför sig till vården eller tjänsternas innehåll. Risknivån för ett system i klass A3 är som standard hög.
    - *Kritiska system i klass A3* är de system 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 och välbefinnandeapplikationerna ska verifieras vid samtestning eller bedömning av informationssäkerheten som ingår i certifieringen enligt kapitel 7 Certifieringsprocessen.

En extern bedömning av informationssäkerheten krävs alltid för Kanta-tjänster. För Kanta-tjänster som innehåller gränssnitt avsedda för tjänstetillhandahållare inom social- och hälsovården eller kunder förutsätts certifiering enligt klass A3 i tillämpliga delar. Dessa åtgärder kan kombineras med de bedömningar av informationssäkerheten som genomförs för FPA i egenskap av myndighetsaktör enligt lagen om bedömingsorgan för informationssäkerhet (1405/2011).

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. System i klass B omfattar inte en stor koncentration personuppgifter och har inte en hög risknivå. 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 systemen kan i enlighet med bestämmelserna om medicintekniska produkter omfatta program som klassificeras som medicintekniska produkter[8] 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,

[8] Enligt definitionen av medicintekniska produkter i artikel 2 i Europaparlamentets och rådets förordning (EU) 2017/745.

och om dessa krav och certifieringar samt användarorganisationernas informationssäkerhetsplaner täcker informationssäkerheten för den behandling av kunduppgifter som görs med systemet. Klass B kan också omfatta system som producerar eller använder enskild information i anslutning till kunduppgifterna i mycket begränsad utsträckning. Ett informationssystem som hör till klass B kan vara en digital tjänst där man behandlar kunduppgifter som lagras i tjänstetillhandahållarens personregister och som är synliga för eller förmedlas till yrkesutbildade personer som är anställda hos tjänstetillhandahållaren.

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

Om producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation är någon annan än den ursprungliga tillverkaren av systemet, delsystemet eller applikationen, 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 informationssystem och välbefinnandeapplikationer som hör till klass A ska man också komma överens om certifieringen och verifieringen av väsentliga krav och om förnyelsen av överensstämmelsen med kraven. En tjänstetillhandahållare kan också själv fungera som tillverkare av en informationssystemtjänst eller i rollen som producent av en informationssystemtjänst (se föreskrift 5/2024 kap. 9).

Ett system eller en välbefinnandeapplikation kan a) självständigt uppfylla alla väsentliga krav enligt dess användningsändamål, b) stödja sig på en annan tillverkares eller producents system eller applikation eller c) stödja sig på en tredje parts plattform eller service för att uppfylla de väsentliga kraven. Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska se till att systemets eller välbefinnandeapplikationens överensstämmelse med kraven kan verifieras och beskrivas även i fall b och c. Då ska antingen verifieringen utföras för varje relevant krav eller så ska det hänvisas till en tidigare certifiering eller registrering enligt de gällande kraven.

6 Beskrivning av användningsändamålet och utredning av hur de väsentliga kraven uppfylls

Producenten av en informationssystemtjänst i ett system som hör till klass A eller B eller tillverkaren av en välbefinnandeapplikation ska beskriva användningsändamålet för systemet eller delsystemet (79 § i lagen om kunduppgifter) samt hur systemet uppfyller de väsentliga kraven (84 § i lagen om kunduppgifter). En utredning av systemets eller delsystemets eller välbefinnandeapplikationens användningsändamål och uppfyllande av de väsentliga kraven ges på en systemblankett enligt bilaga 4 till föreskrift 5/2024.

På systemblanketten ska man

- med en kortfattad fritt formulerad text beskriva informationssystemets eller välbefinnandeapplikationens avsedda ändamål (användningsändamål)
    - av beskrivningen av användningsändamålet bör det framgå i korthet vilken användargrupp (till exempel vilka social- och hälsovårdstjänster eller vilka yrkes- eller kundgrupper) och för vilket syfte (vilka uppgifter som behandlas, vilka tjänster som produceras eller vilken verksamhet som stöds) systemet eller välbefinnandeapplikationen är avsedd
- ange de funktioner och datainnehåll som omfattas av de väsentliga kraven och som hör till systemets eller välbefinnandeapplikationens användningsändamål och som implementeras eller uppfylls via systemet
- ange de väsentliga informationssäkerhetskrav som implementeras eller uppfylls via systemet eller välbefinnandeapplikationen med beaktande av systemets eller välbefinnandeapplikationens användningsändamål

- ange i formulärets uppgifter och tilläggsuppgifter om något väsentligt krav uppfylls endast delvis, om kravet uppfylls under vissa förutsättningar eller inte är tillämpligt eller om det uppfylls via ett annat system eller delsystem eller en annan välbefinnandeapplikation
- ange alla de profiler för väsentliga krav som motsvarar systemets eller välbefinnandeapplikationens användningsändamål
- beskriva hur en välbefinnandeapplikation uppfyller användningsändamålet att främja hälsa och välfärd i enlighet med det lagstadgade kravet (lagen om kunduppgifter 84 §).

Dessa uppgifter utgör den utredning om uppfyllandet av de väsentliga kraven som avses i lagen om kunduppgifter. Ytterligare information och detaljer beskrivs i THL:s föreskrift 5/2024.

Systemblanketten ska

- lämnas in till FPA i samband med ansökan om samtestning av ett system eller välbefinnandeapplikation i klass A2 eller A3
- lämnas in till bedömningsorganet för informationssäkerhet för ett system eller en välbefinnandeapplikation i klass A1, A2 eller A3 som genomgår en bedömning av informationssäkerheten
- lämnas in till Valvira i samband med anmälan till registret över informationssystem för system i klass A och klass B samt välbefinnandeapplikationer i klass A (registrering eller anmälan om ändring av uppgifterna i registret)
- lämnas, som en del av ett anbud på ett system, ett delsystem eller en välbefinnandeapplikation som används i tjänstetillhandahållarens verksamhet, till en tjänstetillhandahållare inom social- och hälsovården, som i anbudsförfrågan eller i ett annat förfarande i upphandlingsprocessen a) kräver att de väsentliga kraven eller de profiler som dessa bildar uppfylls i det system eller delsystem som motsvarar kraven i anbudsförfrågan eller b) kräver att en systemblankett lämnas in.

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

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

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska göra nödvändiga korrigeringar eller preciseringar i de uppgifter som antecknas på blanketten för att säkerställa att blanketten är tydlig eller korrekt, om FPA, bedömningsorganet för informationssäkerhet, THL eller Valvira kräver detta på goda grunder.

7 Certifieringsprocessen

Ett system, ett delsystem eller en välbefinnandeapplikation som hör till klass A ska certifieras. Ansvaret för att inleda och genomföra certifieringen av ett informationssystem ligger hos den aktör som producerar informationssystemtjänsten, som också kan vara systemtillverkaren (lagen om kunduppgifter 85 §). Ansvaret för att inleda och genomföra certifieringen av en välbefinnandeapplikation ligger hos tillverkaren av välbefinnandeapplikationen.

7.1 Skyldigheter i anknytning till certifieringsprocessen

Producenten eller tillverkaren av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska implementera och testa de väsentliga krav på systemet eller välbefinnandeapplikationen som ska certifieras innan

den ansöker om samtestning eller bedömning av informationssäkerheten. De väsentliga kraven som gäller Kanta-tjänsterna ska uppfyllas i enlighet med de mer detaljerade specifikationerna för Kanta-tjänsterna.

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska dokumentera uppfyllandet av de väsentliga kraven så att det inte råder någon oklarhet kring de väsentliga krav som implementerats i systemet eller välbefinnandeapplikationen. Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska sammanställa och presentera den dokumentation som behövs för certifieringen av de krav där verifieringssättet är dokumentation (se kapitel 6 och föreskrift 5/2024 kapitel 10.2).

Certifieringen omfattar (lagen om kunduppgifter 85 §)

- *en utredning om att de väsentliga kraven uppfylls* från producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen, vilken ges på en systemblankett enligt föreskrift 5/2024
- *samtestning* av system, välbefinnandeapplikationer, systemhelheter eller delsystem som hör till klass A2 eller A3, som resulterar i att FPA ger ett positivt samtestningsutlåtande om att interoperabilitetskraven uppfylls med godkänt resultat
- *bedömning av informationssäkerheten*. Bedömningsorganet för informationssäkerhet utfärdar ett informationssäkerhetsintyg för system eller välbefinnandeapplikationer i klass A1, A2 eller A3 som godkänns vid bedömningen.

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska anmäla uppgifter om det certifierade systemet, delsystemet eller välbefinnandeapplikationen till Valvira i enlighet med kapitel 8.

I certifieringsprocessen testas eller bedöms alla väsentliga krav enligt föreskrift 5/2024 som motsvarar systemets och välbefinnandeapplikationens användningsändamål och egenskaper och som ska verifieras genom samtestning eller bedömning av informationssäkerheten.

I samtestningsutlåtandet eller informationssäkerhetsintyget ska det anges om något väsentligt krav på systemet eller den digitala tjänsten uppfylls delvis eller genom kompensation på ett godtagbart sätt[9].

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska underrätta FPA och bedömningsorganet för informationssäkerhet samt Valvira om betydande ändringar i ett system eller en välbefinnandeapplikation som hör till klass A i enlighet med bilaga 2 till denna föreskrift. Betydande ändringar är sådana som förändrar systemets eller applikationens funktion avseende uppfyllandet av de väsentliga kraven i bilaga 2 och 3 till föreskrift 5/2024. Beroende på ändringarna och hur stora effekter de har bedömer FPA eller bedömningsorganet om det behövs en ny samtestning och en ny bedömning av informationssäkerheten eller endast en av dem. Ändringar kräver inte alltid en ny samtestning eller bedömning av informationssäkerheten.

För system och välbefinnandeapplikationer i klass A ska uppfyllandet av kraven verifieras enligt beskrivningen i bilaga 1 kapitel 6 till föreskrift 5/2024 som en del av certifieringen även när kraven uppfylls via andra system, delsystem eller applikationer än det system eller den applikation som ska certifieras.

Lagen kräver inte att en tjänstetillhandahållare som är kund hos en producent av en informationssystemtjänst deltar i certifieringen eller i de verifieringar som hör till den. Tjänstetillhandahållaren och producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation kan dock komma överens om att samarbeta kring certifieringen. FPA:s samtestning eller kundtestning kan också omfatta testning med leverantören av informationssystemet och den tjänstetillhandahållare som är dennes kund, och FPA får enligt 85 § i lagen om kunduppgifter meddela föreskrifter om de förfaranden som ska iakttas vid verifiering av interoperabilitet.

Som en del av certifieringen går man igenom de väsentliga krav på informationssäkerhet som gäller systemets och välbefinnandeapplikationens driftsmiljö och som producenten av en informationssystemtjänst, tillverkaren av informationssystemet eller tillverkaren av en välbefinnandeapplikation ansvarar för när systemet eller applikationen används. Beroende på informationssystemets och den anslutna tjänstens karaktär och avtal kan en del av kraven

[9] ytterligare information: föreskrift 5/2024 kapitel 10.2

som gäller driftsmiljön riktas mot de tjänstetillhandahållare som använder informationssystemet. Det är vanligtvis tjänstetillhandahållarens ansvar att skydda den fysiska driftsmiljön för yrkesutbildade personer som är användare av informationssystemet, men producenten av en informationssystemtjänst kan stödja skyddet genom anvisningar och stödtjänster. De server- eller nätverksmiljöer som hör till driftsmiljön kan beroende på avtal skötas av producenten av en informationssystemtjänst, tillverkaren av en välbefinnandeapplikation, 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 respektive tjänstetillhandahållaren ansvarar för. Detta gäller även de välbefinnandeapplikationer som används i tjänstetillhandahållarens verksamhet. I sådana fall ska det ansvar som hör till producenten av informationssystemtjänsten och tillverkaren av en välbefinnandeapplikation enligt kapitel 5 i denna föreskrift 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 fyllts i av producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation, 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 5/2024. Föreskrift 5/2024 och dess bilaga 1 innehåller ytterligare information och åskådliggörande beskrivningar av tillämpningen av certifieringsprocessen samt av uppfyllandet och verifieringen av de väsentliga kraven.

Producenten av en informationssystemtjänst, den tjänstetillhandahållare som använder ett system och tillverkaren av en välbefinnandeapplikation ansvarar för att ett system eller en välbefinnandeapplikation som kräver certifiering tas i användning för produktion av tjänster i enlighet med villkoren i 81 § lagen om kunduppgifter och i kapitel 9 i denna föreskrift.

Föremålet för samtestning och certifiering kan vara en systemhelhet som innehåller flera olika delsystem och digitala tjänster. Systemhelheten eller alla delsystem och applikationer som hör till den ska ha en producent av en informationssystemtjänst eller en tillverkare av en välbefinnandeapplikation. Detta är också fallet i situationer där systemhelheten har en producent av en informationssystemtjänst som ansvarar för integreringen av delsystemen. Producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen 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[10].

7.2 Innehållet i och resultaten av samtestningen

Vid samtestningen testas de krav som ingår i profilerna som hör till systemets eller välbefinnandeapplikationens användningsändamål och andra sådana funktioner och datainnehåll som systemet eller välbefinnandeapplikationen tillämpar i anslutning till Kanta-tjänsterna och som utgör testfall för samtestning.

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 intyg enligt 86 § i lagen om kunduppgifter (nedan samtestningsutlåtande) från FPA om godkänd samtestning. FPA kan ge ett system eller en välbefinnandeapplikation flera samtestningsutlåtanden om samtestningen av olika funktioner eller innehåll eller koppla flera testhelheter till samma samtestningsutlåtande. Samtestningen utförs i den omfattning som systemets användningsändamål förutsätter.

Av samtestningsutlåtandet ska framgå åtminstone följande uppgifter om systemet eller välbefinnandeapplikationen:

- Uppgifter om namn och version samt klass (till exempel A2 eller A3).

[10] Mer information om hur kraven ska riktas in i modulära systemhelheter: föreskrift 5/2024 bilaga 1, kapitel 6.3.

- När samtestningsutlåtandet utfärdades (datum för samtestningsutlåtandet).
- Innehållet i de samtestningar som utförts (till exempel samtestningshelheternas rubriker).
    - Om den samtestning som gjorts ersätter en tidigare samtestning, uppgift om vilket eller vilka utlåtanden som ersätts med det nya samtestningsutlåtandet.
- Uppgift om de profiler enligt föreskrift 5/2024 som producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation har anmält som implementerade i systemet eller applikationen.
- Eventuella observationer som ska beaktas vid ibruktagandet av systemet eller välbefinnandeapplikationen eller i verksamhet i produktionsmiljön som följer bestämmelserna.

Till samtestningsutlåtandet bifogas en mer detaljerad samtestningsrapport som även kan innehålla andra uppgifter. FPA ska lämna samtestningsutlåtandet med bilagor till producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen. Samtestningsutlåtandet ska också lämnas till Valvira. Om man också håller på att uföra en bedömning av informationssäkerheten som syftar till certifiering eller förnyande av informationssäkerhetsintyget för systemet eller välbefinnandeapplikationen 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 eller välbefinnandeapplikationens användningsändamål i förhållande till Kanta-tjänsterna eller de nationella specifikationerna.

I systemet eller välbefinnandeapplikationen som ska samtestas ska de väsentliga krav som ska omfattas av samtestningen implementeras utifrån de senast publicerade eller på annat sätt gällande specifikationsversionerna. 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 giltiga för användning för produktion samt för certifiering. I Kanta-tjänsterna är det möjligt att stödja flera versioner av specifikationerna med olika funktioner och datainnehåll. Versionshantering av specifikationer i förhållande till helheterna som testas beskrivs i kapitel 10.3 i föreskrift 5/2024.

Av samtestningsutlåtandet ska det framgå med vilka andra system, delsystem eller applikationer samtestningen eventuellt har utförts, om en del av de väsentliga kraven i det system eller den applikation som samtestningen görs för uppfylls via ett annat system, delsystem eller en annan applikation. Om implementeringen av de krav som gåtts igenom vid samtestningen sker på basis av andra gränssnitt än Kanta-gränssnitten, antecknas i samtestningsutlåtandet vilket eller vilka andra system som implementerar gränssnitt som fungerar tillsammans med det testade systemet. Kraven på system eller delsystem som anslutits till varandra behandlas närmare i kapitel 6.3 i bilaga 1 till föreskrift 5/2024.

7.3 Innehållet i och resultaten av bedömningen av informationssäkerheten

Som kriterier för bedömning av informationssäkerheten enligt denna föreskrift ska informationssäkerhetskraven och kraven på digitala tjänster enligt THL:s föreskrift 5/2024 användas. 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 eller välbefinnandeapplikationens namn och version, klass (A1, A2 eller A3) och vilka profiler som enligt anmälan har implementerats i det system eller den välbefinnandeapplikation som genomgått bedömningen. Intyget ska innehålla eventuella preciserande observationer och förutsättningar som ska beaktas, särskilt i de organisationer som använder systemen eller applikationerna, för att uppfylla kraven vid ibruktagandet av systemet, i verksamhet som följer bestämmelserna eller vid informationssäker användning. För ett system i klass A3 ska det anges i intyget om det är fråga om ett kritiskt system i klass A3 enligt kapitel 5 i denna föreskrift. Intyget ska också innehålla andra uppgifter enligt Transport- och kommunikationsverkets (nedan Traficom) anvisningar för bedömningsorgan.

I bedömningen av informationssäkerheten verifieras alla sådana väsentliga informationssäkerhetskrav som ska verifieras med beaktande av informationssystemets eller välbefinnandeapplikationens användningsändamål, klass, omfattning och kritikalitet samt typen av uppgifter som behandlas. De krav som ska verifieras omfattar informationssäkerhetskraven enligt de profiler som motsvarar systemets eller applikationens användningsändamål och andra krav som har implementerats eller som uppfylls via systemet eller applikationen. Även andra krav på informationssäkerhet än de som gäller användningen och utnyttjandet av Kanta-tjänsterna ska gås igenom och verifieras. Vid verifieringen av kraven används de administrativa och i tillämpliga delar även tekniska verifieringssätt som beskrivs i föreskrift 5/2024 och i Traficoms anvisningar.

Verifieringen görs enligt THL:s föreskrift 5/2024 på det sätt som varje krav förutsätter med beaktande av systemets eller välbefinnandeapplikationens klass, risknivå och kritikalitet samt typen av uppgifter som behandlas. Verifieringen av informationssäkerhetskraven ska utföras med hjälp av verifieringssätt som motsvarar systemets eller applikationens användningsändamål, risknivå och omfattning av behandlingen av kunduppgifter. Om kraven uppfylls via andra certifierade system eller applikationer som är anslutna till systemet eller applikationen, görs verifieringen endast i den utsträckning som krävs för att fastställa att kraven uppfylls även i det system eller den applikation som är föremål för certifieringen.

Enligt 84 § i lagen om kunduppgifter ska välbefinnandeapplikationer uppfylla tillgänglighetskraven. I samband med bedömningen av informationssäkerhet för välbefinnandeapplikationer går man igenom rapporten om resultaten i tillgänglighetstestningen. Välbefinnandeapplikationens tillgänglighet ska testas med hjälp av en tillgänglighetsbedömning som görs av tillverkaren själv eller av en utomstående aktör. De väsentliga kraven på tillgänglighet ska i tillämpliga delar också användas för att säkerställa tillgänglighet för de digitala tjänster som omfattas av tillämpningsområdet för lagen om tillhandahållande av digitala tjänster (306/2019) inom social- och hälsovårdstjänsterna, om de digitala tjänsterna uppfyller definitionen av ett informationssystem eller en välbefinnandeapplikation.

Om systemet eller välbefinnandeapplikationen används för produktion av tjänster ska det genomgå en bedömning av informationssäkerheten och ett förnyat informationssäkerhetsintyg ska skrivas innan det tidigare intygets giltighetstid löper ut i enlighet med kapitel 10 i denna föreskrift (Förnyande av överensstämmelse med kraven).

Ett nytt intyg över bedömning av informationssäkerhet ska utfärdas eller interoperabilitetstestningen göras om, om betydande ändringar görs i ett system eller i en välbefinnandeapplikation eller om de väsentliga kraven har ändrats på ett sätt som kräver en ny certifiering (82 § i lagen om kunduppgifter). Anmälan om ändringar i informationssystemet eller välbefinnandeapplikationen ska göras i de situationer som anges i bilaga 2 till denna föreskrift. Om en anmälan om betydande ändringar i ett system eller en applikation leder till en bedömning av informationssäkerheten, ska man i denna bedömning gå igenom de krav som påverkas av ändringarna. Om de övriga kraven enligt producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation uppfylls på samma nivå som tidigare, kan det befintliga informationssäkerhetsintyget uppdateras så att giltighetstiden för det tidigare intyget inte ändras. Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation 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 i denna föreskrift igenom alla informationssäkerhetskrav som implementerats eller uppfyllts via systemet och skriver ett nytt intyg med en ny giltighetstid.

Lagen om kunduppgifter förutsätter inga regelbundna uppföljande auditeringar av informationssäkerheten, men producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation kan komma överens med bedömningsorganet om uppföljande auditeringar. Eventuella uppföljande auditeringar av informationssäkerheten som systemet eller välbefinnandeapplikationen 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. Uppföljande auditeringar dokumenteras inte i Valviras register över informationssystem. Om det vid den uppföljande auditeringen upptäcks ändringar på basis av vilka informationssäkerhetsintyget måste förnyas eller

uppdateras, inleds en bedömning av informationssäkerheten som syftar till att förnya eller uppdatera intyget, på basis av vilken även uppgifterna i Valviras register över informationssystem uppdateras.

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

Det nya eller uppdaterade intyget över bedömning av informationssäkerheten ersätter det intyg som tidigare utfärdats för samma system eller välbefinnandeapplikation.

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 eller välbefinnandeapplikationen har godkänts vid åtminstone en samtestning.

Om ett system i klass A2 eller A3 eller en välbefinnandeapplikation för första gången ska certifieras så att den genomgår både samtestning och bedömning av informationssäkerheten, bör man sträva efter att informationssäkerhetsintyget och samtestningsutlåtandet gäller samma version av systemet. Det är möjligt att inleda bedömningen av informationssäkerheten innan samtestningsutlåtandet är klart. I dessa situationer ska producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen se till att samma version av systemet eller applikationen används både vid samtestningen och bedömningen av informationssäkerhet eller att man använder en sådan version där eventuella systemändringar i anslutning till de väsentliga krav som ska samtestas inte påverkar de informationssäkerhetskrav som ska bedömas. Då kontrollerar bedömningsorganet för informationssäkerhet, innan informationssäkerhetsintyget beviljas, med producenten av informationssystemtjänsten eller tillverkaren av en välbefinnandeapplikationen att det inte kommer att ske några ändringar i det system eller den applikation som är föremål för samtestningen som skulle kunna påverka uppfyllandet av informationssäkerhetskraven. Bedömningsorganet ska också kontrollera saken med FPA. Vid senare certifieringar och förnyande av överensstämmelse med kraven som görs för samma system ska man agera så som anges i kapitel 10 ”Förnyande av överensstämmelse med kraven”.

Resultaten av samtestningen antecknas inte i informationssäkerhetsintyget.

Förfarandena för bedömning av informationssäkerheten beskrivs närmare i kapitel 5 och 6 i bilaga 1 till föreskrift 5/2024.

8 Registrering av och tillsyn över informationssystem och välbefinnandeapplikationer

Producenten av en informationssystemtjänst ska göra en anmälan om system och tillverkaren av en välbefinnandeapplikation ska göra en registeranmälan om välbefinnandeapplikationer till Valvira innan systemen eller välbefinnandeapplikationerna tas i användning för produktion av tjänster. I 80 § i lagen om kunduppgifter beskrivs vilka uppgifter anmälan ska innehålla.

Valvira för ett offentligt register över de system och välbefinnandeapplikationer inom social- och hälsovården som anmälts till Valvira och som uppfyller kraven.

Anmälan och registret innehåller de uppgifter som avses i 80 § i lagen om kunduppgifter. För anmälan av uppgifter används de förfaranden som preciseras i denna föreskrift och föreskrift 5/2024. Systemblanketten enligt föreskrift 5/2024 innehåller många uppgifter som ska anmälas till registret. Den systemblankett som ska skickas in med registeranmälan är en redogörelse enligt 80 och 85 § i lagen om kunduppgifter för de väsentliga krav som har uppfyllts i systemet.

De uppgifter om informationssystemet eller välbefinnandeapplikationen som ska publiceras i registret grundar sig på

a) de uppgifter som krävs av Valvira i samband med registeranmälan

b) de uppgifter som angetts på systemblanketten enligt föreskrift 5/2024: basuppgifter om informationssystemet, beskrivningen av användningsändamålet, profilerna i systemet, risknivån och de väsentliga krav som uppgetts på systemblanketten (klass A och B)

c) samtestningsutlåtanden och/eller samtestningsrapporter (klass A2 och A3)

d) det senaste gällande informationssäkerhetsintyget (klass A)

e) information från tillsynsprocessen om hur länge ett system och en applikation som hör till klass A har uppvisat en betydande avvikelse

f) andra utredningar och myndighetsbeslut som Valvira anser nödvändiga.

I samband med registreringen ska en systemblankett enligt föreskrift 5/2024 lämnas in. Systemblanketten innehåller de viktigaste uppgifterna om beskrivningen av användningsändamålet, certifieringen, registreringen och uppfyllandet av de väsentliga kraven. Producenten av informationssystemtjänsten och tillverkaren av välbefinnandeapplikationen ansvarar för att de uppgifter som lämnas på systemblanketten är korrekta, aktuella och exakta och motsvarar de väsentliga krav som har implementerats i systemet eller som har uppfyllts genom systemet.

Registrering i Valviras register över informationssystem förutsätter att informationssystemet eller den digitala tjänsten har certifierats om den hör till klass A. Enligt lagen hör välbefinnandeapplikationer till klass A och måste certifieras innan de registreras i Valviras register över informationssystem.

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation som ansvarar för ett informationssystem, en välbefinnandeapplikation eller ett delsystem som hör till klass A2 eller A3 ska i samband med registeranmälan till Valvira visa upp FPA:s samtestningsutlåtanden som gäller de samtestningshelheter som implementerats och testats i systemet eller välbefinnandeapplikationen. Åtminstone det senaste samtestningsutlåtandet för varje samtestningshelhet som testats i systemet eller välbefinnandeapplikationen ska lämnas in. De egenskaper som samtestats ska tillsammans bilda en helhetsbild (se även kapitel 7.2).

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation som ansvarar för ett informationssystem i klass A ska i samband med anmälningar till Valvira visa upp det giltiga informationssäkerhetsintyget. Endast det senaste och gällande informationssäkerhetsintyget över en godkänd bedömning av informationssäkerheten ska anmälas.

Registeranmälan och systemblanketten i anslutning till certifieringen ska lämnas till Valvira senast när certifieringen av informationssystemet eller välbefinnandeapplikationen har slutförts med godkänt resultat. Valvira kan ge anvisningar om hur anmälan och blanketten ska lämnas in också innan bedömningsorganet för informationssäkerhet har beviljat ett informationssäkerhetsintyg.

Valvira får i enlighet med 80 § i lagen om kunduppgifter meddela föreskrifter om innehållet i anmälan, förnyande av anmälan och vilka uppgifter som ska antecknas i registret. Valvira uppdaterar uppgifterna i registret genom registreringsprocessen, tillsynsprocessen och begäran om uppgifter enligt 91 § i lagen om kunduppgifter samt andra begäranden om uppgifter.

9 Förutsättningar för ibruktagandet av informationssystem eller välbefinnandeapplikationer

Förutsättningarna för att ta ett informationssystem eller en välbefinnandeapplikation i användning för produktion av tjänster beskrivs i 81 § i lagen om kunduppgifter. I detta kapitel preciseras dessa förutsättningar i förhållande till de omständigheter som rör väsentliga krav och certifiering som anges i föreskrifterna 4/2024 och 5/2024.

Ett informationssystem som hör till klass B ska uppfylla följande krav innan systemet får tas i användning för produktion av tjänster:

- Systemet uppfyller de väsentliga krav som ställs enligt dess användningsändamål (se kapitel 6).
- Producenten av informationssystemtjänsten har lämnat en skriftlig utredning i enlighet med föreskrift 5/2024 om att de väsentliga kraven uppfylls i samband med registreringen till Valvira.
- Uppdaterade uppgifter om systemet finns i Valviras register över informationssystem.
- Systemet är, enligt uppgifterna i Valviras register över informationssystem (se föreskrift 5/2024 kap. 10.4), inte förenat med en betydande avvikelse som förhindrar att systemet tas i bruk för produktion av tjänster.

Ett informationssystem eller en välbefinnandeapplikation som hör till klass A ska uppfylla följande krav innan systemet får tas i användning för produktion av tjänster:

- Systemet eller välbefinnandeapplikationen uppfyller de väsentliga krav som ställs enligt dess användningsändamål (se kapitel 6).
- Systemet eller välbefinnandeapplikationen har certifierats med godkänt resultat (se kapitel 7).
    - System eller välbefinnandeapplikationer som hör till klass A2 eller A3 har godkända samtestningsutlåtanden om de egenskaper som ska samtestas i anslutning till Kanta-tjänsterna utifrån gällande specifikationer.
    - System som hör till klass A1, A2 eller A3 har ett informationssäkerhetsintyg som inte får vara föråldrat.
- Välbefinnandeapplikationen främjar medborgarnas hälsa och välfärd som en förutsättning för att kraven på funktionalitet ska vara uppfyllda i enlighet med 84 § i lagen om kunduppgifter.
- Producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen har lämnat en skriftlig utredning enligt föreskrift 5/2024 om att de väsentliga kraven uppfylls i samband med registreringen till Valvira
- Uppdaterade uppgifter om systemet eller välbefinnandeapplikationen finns i Valviras register över informationssystem.
- Systemet är, enligt uppgifterna i Valviras register över informationssystem (se föreskrift 5/2024 kap. 10.4), inte förenat med en betydande avvikelse som förhindrar att systemet tas i bruk för produktion av tjänster.

Ett system eller en välbefinnandeapplikation 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. Ett sådant system eller en sådan välbefinnandeapplikation kan tas i användning för produktion av tjänster för de användningsändamål enligt profilerna i bilaga 3 till föreskrift 5/2024 vars obligatoriska krav som motsvarar de väsentliga krav som hör till samtestningarna har samtestats med godkänt resultat.

Tjänstetillhandahållare inom social- och hälsovården och apotek ska säkerställa att uppgifterna om det system som är avsett för behandling av klient- eller patientuppgifter och som tas i användning för produktion av tjänster i deras verksamhet finns i det register som förs av Valvira. Dessutom ska tjänstetillhandahållaren eller apoteket säkerställa att de system som används i sin helhet motsvarar tjänstetillhandahållarens eller apotekets verksamhet och att man med dem kan uppfylla de allmänna och eventuella tjänstespecifika minimikraven enligt 67 § och 84 § i lagen om kunduppgifter och föreskrift 5/2024 i tjänstetillhandahållarens eller apotekets verksamhet[11].

10 Förnyande av överensstämmelse med kraven

Förnyandet av överensstämmelsen med kraven för ett informationssystem i klass B som används för produktion av tjänster sker så att producenten av en informationssystemtjänst i enlighet med kapitel 6 och 8 säkerställer att

1. informationssystemet uppfyller gällande väsentliga krav som motsvarar dess användningsändamål och implementerade egenskaper
2. korrekta och uppdaterade uppgifter om systemet finns i Valviras register över informationssystem.

Resten av detta kapitel gäller förnyandet av överensstämmelsen med kraven för ett informationssystem eller en välbefinnandeapplikation som hör till klass A.

Vid förnyande av ett informationssystem eller en välbefinnandeapplikation som hör till klass A och som används för produktion av tjänster ska

1. informationssäkerhetsintyget förnyas innan informationssäkerhetsintyget för det informationssystem eller den välbefinnandeapplikation som används för produktion föråldras
2. det säkerställas att det informationssystem eller den välbefinnandeapplikation som ansluts till Kanta-tjänsterna har godkända samtestningsutlåtanden för de väsentliga krav som hör till användningsändamålet och som ska samtestas på basis av de krav och specifikationsversioner som krävs för användning för produktion av tjänster.

Överensstämmelsen med kraven ska förnyas innan det tidigare gällande informationssäkerhetsintyget upphör att gälla.

Upprätthållandet av överensstämmelsen med kraven kan också kräva implementering och certifiering av nya krav på systemet i enlighet med de tidsfrister som anges i bestämmelserna eller att åtgärder vidtas på grund av systemändringar (se kapitel 7.1 och bilaga 2).

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska kontakta bedömningsorganet för informationssäkerhet för att förnya informationssäkerhetsintyget när giltighetstiden för ett informationssäkerhetsintyg för ett system, ett delsystem eller en välbefinnandeapplikation i klass A håller på att gå ut. Bedömningsorganet för informationssäkerhet och vid behov FPA ska kontaktas senast sex månader innan det tidigare intyget löper ut.

Bedömningsorganet för informationssäkerhet förnyar informationssäkerhetsintyget genom att verifiera alla väsentliga informationssäkerhetskrav som är relevanta för systemet eller välbefinnandeapplikationen. Dessa är de krav i förteckningen över väsentliga krav (föreskrift 5/2024, bilaga 2) som verifieras genom bedömning av informationssäkerheten och som är tillämpliga på det systemet eller den välbefinnandeapplikation som är föremål för bedömningen. Vid verifieringen av varje krav kan man stödja sig på samma förfaranden och dokumentation som i det tidigare beviljade informationssäkerhetsintyget, om

- kravet eller den specifikation som ligger till grund för kravet inte har ändrats och fortfarande gäller vid certifieringen, och

[11] ytterligare information föreskrift 5/2024 kapitel 9

- sätten att implementera eller uppfylla kravet inte har förändrats i systemet eller välbefinnandeapplikationen, och
- det inte har skett några förändringar i deras driftsmiljöer som påverkar uppfyllandet av kraven, och
- inga nya sårbarheter eller utnyttjanden har upptäckts över tid i de förfaranden eller de programvaror som använts.

Bedömningsorganet för informationssäkerhet utfärdar ett informationssäkerhetsintyg över godkänd bedömning av informationssäkerheten i enlighet med kapitel 7.3 i den här föreskriften. Ett informationssäkerhetsintyg kan utfärdas oberoende av om informationssystemet eller välbefinnandeapplikationen har pågående samtestningar eller inte.

Om det är fråga om ett informationssystem eller en välbefinnandeapplikation som hör till klass A2 eller A3 ska producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen också kontakta FPA för en ny bedömning av behovet av samtestning när förnyandet av informationssäkerhetsintyget inleds. Om det i bedömningen konstateras att en ny samtestning ska utföras, ska testningen utföras enligt gällande specifikationer eller de specifikationer som samtestningen kräver. FPA ger ett positivt utlåtande om godkänd samtestning.

För den ovan beskrivna bedömningen av behovet samtestning ska producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation 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, ifall

- implementeringen grundar sig på en föråldrad specifikation och tidsfristen, som fastställts i samband med den nya ersättande specifikationen eller i författningar, för när den nya specifikationsversionen ska tas i bruk har löpt ut
- implementeringen inte motsvarar den publicerade specifikationsversionen[12] som krävs för samtestning med Kanta-tjänsterna, även om implementeringar enligt den äldre versionen som försvinner fortfarande skulle stödjas i Kanta-tjänsternas produktionsmiljö.

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska anmäla de uppdaterade uppgifterna om förnyande av överensstämmelse med kraven till Valviras register över informationssystem senast en månad efter att det förnyade informationssäkerhetsintyget har beviljats. I anmälan till Valviras register ska inte uppges sådana väsentliga krav eller sådana profiler enligt föreskrift 5/2024 för vilka de tillhörande kraven som ska certifieras inte har certifierats med godkänt resultat i enlighet med gällande krav och specifikationer[13].

De centrala uppgifterna i det nya gällande informationssäkerhetsintyget och eventuella nya samtestningsutlåtanden ska göras tillgängliga i Valviras register över informationssystem på det sätt som beskrivs i kapitel 8 i denna föreskrift.

En version av applikationen eller systemet som fått ett förnyat informationssäkerhetsintyg kan uppdateras i de produktionsmiljöer som används, oberoende av samtestningar, förutsatt att aktuella uppgifter om versionen finns i Valviras register. Då måste dock följande beaktas:

- Egenskaper som kräver godkänd samtestning med Kanta-tjänsterna får tas i användning för produktion av tjänster först när ett samtestningsutlåtande om genomförandet av dem har getts.

---

[12] FPA och THL anger giltigheten för de specifikationsversioner som används för certifiering med frasen "voimassa sertifioinnissa" (giltig för certifiering) och giltigheten för de specifikationsversioner som används för produktion med frasen "voimassa tuotannossa" (giltig för produktion).

[13] Valvira har möjlighet att jämföra de uppgifter som tidigare lämnats om systemet eller välbefinnandeapplikationen med de uppgifter som lämnats i samband med förnyandet av överensstämmelsen med kraven och med samtestningsutlåtanden om olika testhelheter.

- Till Valviras register över informationssystem ska man inte anmäla sådana väsentliga krav eller profiler som implementerade i systemet eller applikationen, vars krav systemet eller applikationen inte uppfyller; när det gäller krav som ska certifieras kräver anmälan av profiler och krav enligt användningsändamålet till Valviras register över informationssystem att samtestningarna i anslutning till dessa har utförts och att informationssäkerhetsintyget är i kraft.

Hur de väsentliga kraven förhåller sig till de specifikationer och specifikationsversioner på basis av vilka överensstämmelsen med kraven förnyas beskrivs också i kapitel 10.3 i THL:s föreskrift 5/2024.

Kraven som gäller stöd för olika versioner av strukturer och uppgifter i klienthandlingarna inom socialvården beskrivs i THL:s föreskrift 1/2024. Vid förnyandet av överensstämmelsen med kraven ska man i enlighet med föreskrift 1/2024 ta hänsyn till handlingsstrukturernas status.

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

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ansvarar för att systemet eller applikationen uppfyller de väsentliga kraven genom hela användningen för produktion av tjänster i enlighet med 94 § i lagen om kunduppgifter.

11 Handledning och rådgivning

Mer information om tillämpningen av denna föreskrift och certifieringsprocessen i förhållande till de väsentliga krav som ställs på informationssystem och välbefinnandeapplikationer finns i föreskrift 5/2024 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 10. maj 2024 och gäller tills vidare.

Enligt föreskriften krävs inte att det gällande överensstämmelseintyget för ett informationssystem eller en välbefinnandeapplikation i klass A omedelbart förnyas, såvida inte de övriga kraven för förnyelse uppfylls. Senast sex månader innan giltighetstiden för informationssäkerhetsintyget enligt den tidigare lagen om kunduppgifter (784/2021) går ut ska en systemblankett för systemet eller applikationen enligt föreskrift 5/2024 lämnas in till FPA för bedömning av behovet av förnyad samtestning och till bedömningsorganet för informationssäkerhet för bedömning av behovet av förnyad bedömning av informationssäkerheten.

Ett informationssystem som med stöd av den tidigare lagen om kunduppgifter (784/2021) samt THL:s föreskrifter 4/2021 och 5/2021 eller 1/2022 har certifierats med godkänt resultat kan tas i användning för produktion av tjänster av nya tjänstetillhandahållare i enlighet med de tidigare godkända kraven, om det har ett giltigt informationssäkerhetsintyg och de krav som verifierats vid samtestningen av det motsvarar de aktuella kraven för produktionsanvändning.

En systemblankett enligt föreskrift 5/2024 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 eller en välbefinnandeapplikation i klass A.

De klassificerings- och certifieringsförfaranden som beskrivs i föreskriften tillämpas på alla system och välbefinnandeapplikationer som ska certifieras *senast från och med den 1 november 2024*. Vid certifieringen tillämpas de väsentliga kraven enligt de profil- och kravspecifika giltighetstider som beskrivs i föreskrift 5/2024. Om

samtestningen eller bedömningen av informationssäkerheten har inletts innan föreskriften träder i kraft, kan certifieringsprocessen slutföras *senast den 31 december 2024* i enlighet med de krav, bestämmelser och förfaranden som gällde när processen inleddes. Informationssäkerhetsintyget eller samtestningsutlåtandet ska då innehålla en tydlig anteckning om att bedömningen har utförts i enlighet med kraven i lagen om kunduppgifter 784/2021 och THL:s föreskrifter 4/2021 och 5/2021. På begäran av producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation kan man dock även i dessa fall tillämpa förfaranden och krav enligt THL:s föreskrifter 4/2024 och 5/2024.

Informationssäkerhetsintyget för system eller applikationer som certifierats med stöd av den tidigare lagen om kunduppgifter 784/2021 samt THL:s föreskrifter 4/2021 och 5/2021 eller 6/2021 eller 1/2022 ska förnyas innan giltighetstiden för informationssäkerhetsintyget enligt den tidigare lagen löper ut. I samband med förnyandet ska producenten av en informationssystemtjänst i enlighet med kapitel 10 säkerställa att alla väsentliga krav som motsvarar systemets användningsändamål, och som är föremål för verifiering genom samtestning eller bedömning av informationssäkerheten, har implementerats och certifierats i systemet.

Om uppgifterna om ett system i klass B i Valviras register över informationssystem grundar sig på föråldrade bestämmelser, ska överensstämmelsen med kraven förnyas och uppgifterna i informationssystemregistret uppdateras i enlighet med kapitel 10 och Valviras anvisningar eller föreskrifter.

Om ett system övergår från klass B till klass A1 enligt de kriterier som beskrivs i denna föreskrift och dess bilagor, ska systemet certifieras i enlighet med gällande väsentliga krav eller den certifiering som inleddes innan föreskriften trädde i kraft slutföras *senast den 1 november 2024*[14].

Om kraven enligt THL:s föreskrift 4/2024 eller 5/2024 förutsätter att uppgifterna i ett informationssystem i klass B eller A uppdateras[15] i Valviras register över informationssystem, men inte kräver en ny certifiering, ska en uppdaterad anmälan om informationssystemet lämnas till Valviras register senast *den 1 november 2024*, om inte Valvira bestämmer något annat.

Om ett system eller en välbefinnandeapplikation som inte tidigare anslutits till Kanta-tjänsterna ansluts till Kanta-tjänsterna direkt eller med stöd av ett annat system, en annan applikation eller informationsförmedlingsservice för kunduppgifter, ska systemet eller välbefinnandeapplikationen klassificeras och certifieras enligt kraven för klass A2 eller A3 före anslutningen.

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

För ett system som fått ett överensstämmelseintyg enligt lagen om kunduppgifter 159/2007 och föreskrift 1/2015 som gällde före 2021, ska en verifiering av de väsentliga kraven och en bedömning av informationssäkerheten i enlighet med denna föreskrift eller dess övergångsbestämmelser utföras senast den 1 november 2024[16]. I samband med detta ska producenten av informationssystemtjänsten säkerställa att alla väsentliga krav som motsvarar dess användningsändamål har implementerats och certifierats i systemet.

---

[14] Kriterierna för att höra till klasserna B och A och kraven för klass A1 i föreskrift 4/2024 motsvarar i huvudsak dem i föreskrift 4/2021 enligt den tidigare lagen om kunduppgifter (784/2021), så tidsfristen är densamma som i föreskrift 4/2021.

[15] Uppdateringsbehovet kan gälla till exempel klassificeringen av systemet, profiler som implementerats i systemet eller sådana väsentliga krav enligt föreskrift 5/2024 som implementerats i ett system av klass B och som inte har ingått i den tidigare registreringen eller anmälan som lämnats till Valvira. Enligt 81 § i lagen om kunduppgifter får Valvira meddela mer detaljerade föreskrifter om förnyande av anmälan.

[16] Tidsfristen är densamma som i föreskrift 4/2021: inom tre år från det att den tidigare lagen om kunduppgifter 784/2021 trädde i kraft. I lag 784/2021 föreskrevs att intyget är giltigt i högst tre år. Enligt den upphävda lagen 159/2007 var det möjligt att före 2021 utfärda ett intyg som var giltigt i högst fem år.

Mer information om när profilerna för väsentliga krav och de krav som uttrycks i profilerna träder i kraft och hur de påverkar bland annat socialvårdens klientdatasystem finns i föreskrift 5/2024.

Sirpa Soini

Direktör

Jarmo Kärki

Enhetschef

Bilagor

Bilaga 1. Exempel på klassificeringen av system och välbefinnandeapplikationer

Bilaga 2. Anmälan om ändringar i informationssystem och välbefinnandeapplikationer som hör till klass A

För kännedom

tillverkare av klient- och patientdatasystem och apotekssystem samt producenter av informationssystemtjänster för social- och hälsovården
offentliga och privata tjänstetillhandahållare inom social- och hälsovården
apotek
mellanhänder
tillverkare av välbefinnandeapplikationer
producenter av informationsförvaltningstjänster och ICT-tjänster för social- och hälsovården
Folkpensionsanstalten
Tillstånds- och tillsynsverket för social- och hälsovården Valvira
kompetenscentrum inom det sociala området
bedömningsorgan för informationssäkerhet
Cybersäkerhetscentret
Dataombudsmannens byrå
social- och hälsovårdsministeriet
finansministeriet
kommunikationsministeriet
Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea
regionförvaltningsverken
Myndigheten för digitalisering och befolkningsdata
Försörjningsberedskapscentralen
Finlands Kommunförbund rf

Denna föreskrift publiceras i myndigheternas föreskriftssamlingar

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

och finns att tillgå:

- på registratorskontoret vid Institutet för hälsa och välfärd samt på
- webbadressen https://thl.fi/sv/teman/informationshantering-inom-social-och-halsovarden/foreskrifter-och-specifikationer/foreskrifter