Informationsförmedlare
Information och styrning av informationshanteringen 3.5.2024

FÖRESKRIFT OM VÄSENTLIGA KRAV PÅ INFORMATIONSSYSTEM OCH VÄLBEFINNANDEAPPLIKATIONER INOM SOCIAL- OCH HÄLSOVÅRDEN

Bestämmelser om bemyndigande

Lag om behandling av kunduppgifter inom social- och hälsovården (703/2023),10 § 4 moment, 20 § 2 moment, 79 § 4 moment, 82 § 4 moment, 84 § 4 moment, 85 § 3 moment.

Målgrupper

Producenter av informationssystemtjänster och tillverkare av informationssystem för social- och hälsovården
Tillverkare av välbefinnandeapplikationer
Producenter av Kanta-informationsförmedlingsservice
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 5/2021 (föreskrift om väsentliga krav på funktionalitet och informationssäkerhetskrav hos 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 informationsresursen 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

Syftet med denna föreskrift är att precisera de väsentliga krav som ställs på informationssystem som är avsedda för behandling av klient- och patientuppgifter inom social- och hälsovården, så att deras ändamålsenliga funktion, kompabilitet och informationssäkerhet kan säkerställas. Vidare syftar föreskriften till att precisera de väsentliga krav som ställs på välbefinnandeapplikationer.

2 Föreskriftens tillämpningsområde

De termer och definitioner som används i föreskriften följer THL:s föreskrift 4/2024 (kapitel 2).

Denna föreskrift gäller innehållet i de väsentliga kraven på informationssystem och välbefinnandeapplikationer som behandlar klient- eller patientuppgifter inom social- och hälsovården (lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023), nedan lagen om kunduppgifter, kapitel 12 ”Väsentliga krav på informationssystem och välbefinnandeapplikationer”). Institutet för hälsa och välfärd (nedan THL) har med stöd av 84 § 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 som används i olika tjänster. Dessutom har THL med stöd av 85 § i lagen om kunduppgifter 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.

Denna föreskrift gäller

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

Användningsändamålen för de väsentliga kraven i föreskriften:

- Beskriva användningsändamålet för system, delsystem eller välbefinnandeapplikationer som behandlar klient- eller patientuppgifter,
- Sammanställa nationellt fastställda krav samt sammanställa och hänvisa till specifikationer som närmare beskriver kraven.
- Förtydliga de krav som gås igenom vid FPA:s samtestning med Kanta-tjänsterna och dess olika testhelheter av system och välbefinnandeapplikationer i klass A2 och A3 som ska anslutas till Kanta-tjänsterna.
- Gruppera de systemegenskaper som testas av tillverkarna av informationssystem i klass A2 och A3 och av producenterna av informationssystemtjänster, vid FPA:s samtestning samt vid eventuella kundtester.
- Beskriva de informationssäkerhetskrav som ska behandlas i bedömningen av informationssäkerheten för klass A för bedömningar av informationssäkerheten.
- Gruppera och länka till krav och specifikationer som hänför sig till samma funktionella eller innehållsmässiga helheter.
- Sammanställa de nationella specifikationer som gäller vid olika tidpunkter för implementering av en viss funktion eller ett visst datainnehåll.
- Genom profiler uttrycka obligatoriska krav på system och välbefinnandeapplikationer som är avsedda för ett visst ändamål.

- Fastställa och sammanställa tidtabellerna och övergångstiderna för de obligatoriska kraven (till exempel i fråga om de övergångstider som fastställs i lagen om kunduppgifter och de specifikationer och väsentliga krav som gäller ett visst år).
- Stödja beskrivningen och beaktandet av de väsentliga krav som ställs nationellt vid planering och implementering av system samt vid upphandling av system.
- Beskriva egenskaperna hos olika delsystem i systemhelheter och modulära system.
- Förenhetliga de begrepp och krav som används i kraven på tillverkare av system och tillverkare av välbefinnandeapplikationer, producenter av informationssystemtjänster och deras användare och som grundar sig på författningar och nationella specifikationer.

3 Föreskriftens centrala innehåll och avgränsningar

Enligt lagen om kunduppgifter ska ett system och en välbefinnandeapplikation som används vid behandling av klient- eller patientuppgifter uppfylla väsentliga krav på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. Utöver dessa ska välbefinnandeapplikationer uppfylla tillgänglighetskraven. Producenten av en informationssystemtjänst eller tillverkaren av ett informationssystem ansvarar för att systemet uppfyller kraven och tillverkaren av en välbefinnandeapplikation ansvarar för att välbefinnandeapplikationen uppfyller kraven.

I lagen om kunduppgifter föreskrivs också att de system som en tjänstetillhandahållare använder till sitt användningsändamål ska svara mot tjänstetillhandahållarens verksamhet och uppfylla de väsentliga krav som ställs på tjänstetillhandahållarens verksamhet. Denna föreskrift preciserar hur man säkerställer att de väsentliga kraven uppfylls i de system som en tjänstetillhandahållare använder.

Enligt lagen om kunduppgifter ska tillverkaren av ett informationssystem för social- och hälsovården eller producenten av en informationssystemtjänst samt tillverkaren av en välbefinnandeapplikation påvisa att systemet, tjänsten eller välbefinnandeapplikationen överensstämmer med kraven. Till påvisandet hör enligt 80 § och 85 § i lagen om kunduppgifter en utredning om att systemet eller välbefinnandeapplikationen uppfyller de väsentliga krav som motsvarar dess användningsändamål. Utredningen ges i enlighet med föreskrift 4/2024 och denna föreskrift.

Till denna föreskrift bifogas en nationellt enhetlig klassificering av väsentliga krav på system för social- och hälsovården och välbefinnandeapplikationer (bilaga 2). Förteckningen innehåller beskrivningar på övre nivå av väsentliga krav på de system och välbefinnandeapplikationer som används för behandling av klient- och patientuppgifter inom social- och hälsovården. I föreskriften preciseras också vilka väsentliga krav som åtminstone ska implementeras eller uppfyllas för system eller välbefinnandeapplikationer avsedda för olika ändamål (bilaga 3, profiler). I denna föreskrift preciseras dessutom de förfaranden som ska användas vid beskrivning, verifiering och utnyttjande av väsentliga krav.

Föreskriften gäller både system i anslutning Kanta-tjänsterna och andra system som är avsedda för behandling av klient- och patientuppgifter och som hör till klass A eller klass B samt välbefinnandeapplikationer som hör till klass A. Flera av kraven och de specifikationer som ligger till grund för dem gäller system eller välbefinnandeapplikationer som hör till klass A2 eller A3 (se föreskrift 4/2024) och som är anslutna till Kanta-tjänsterna.

Termerna och avgränsningarna som används i föreskriften motsvarar termerna i THL:s föreskrift 4/2024.

Föreskriften och dess bilagor har beretts av experter från Institutet för hälsa och välfärd (THL), Folkpensionsanstalten (FPA), Tillstånds- och tillsynsverket för social- och hälsovården (Valvira), Social- och hälsovårdsministeriet (SHM), Transport- och kommunikationsverket (Traficoms Cybersäkerhetscenter) samt utvecklingsprojekten för tillhandahållare av social- och hälsovårdstjänster. I föreskriften beaktas de utvecklingsbehov som har identifierats vid tillämpningen av tidigare författningar. Kraven på informationssystemen och tjänstetillhandahållarna motsvarar till största delen kraven i de tidigare föreskrifterna.

Innan denna föreskrift utfärdades ordnade THL en remissrunda för att få synpunkter från intressentgrupperna i fråga. Remissvaren har i tillämpliga delar beaktats i föreskriften och dess bilagor. Mer information om beredningen av föreskriften finns i kapitel 7 i bilaga 1.

4 Förhållande till andra författningar, anvisningar och specifikationer

THL har utfärdat en föreskrift om klassificering och certifiering av informationssystem och välbefinnandeapplikationer inom social- och hälsovården (THL:s föreskrift 4/2024). Denna föreskrift preciserar de krav som ska verifieras med de förfaranden som beskrivs i föreskrift 4/2024 och de förfaranden som ska användas vid anmälan och verifiering av överensstämmelse med kraven.

Förteckningen över väsentliga krav i bilaga 2 till denna föreskrift hänvisar till flera närmare specifikationer och anvisningar som beskriver detaljerade krav på funktionalitet och datainnehåll. Förteckningen är avsedd att förtydliga och stöda utvecklingen, certifieringen, testningen, bedömningen av informationssäkerheten och upphandlingen av system och applikationer samt kommunikationen mellan olika parter. När föreskriften tillämpas fungerar förteckningen också som ett register, genom vilket man kan hitta de viktigaste specifikationerna som beskriver de nationella kraven.

De väsentliga krav som beskrivs i föreskriften och dess bilagor ersätter de väsentliga krav som fastställts med stöd av den tidigare lagen om kunduppgifter samt THL:s föreskrifter 4/2021, 5/2021 och 6/2021. Största delen av de väsentliga kraven är desamma som i tidigare föreskrifter.

Föreskriften 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 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.

THL har utfärdat en separat föreskrift 1/2024 om klienthandlingar inom socialvården och om de uppgifter som ska antecknas i dem.

I THL:s föreskrift 3/2024 beskrivs de utredningar och krav som ska ingå i den informationssäkerhetsplan som förutsätts av tillhandahållare av social- och hälsovårdstjänster, mellanhänder, apotek och FPA. I informationssäkerhetsplanen beskrivs hur objektet för informationssäkerhetsplanen säkerställer att de system som används för produktion av tjänster och de välbefinnandeapplikationer som eventuellt används i verksamheten överensstämmer med kraven som en del av informationssäkerhetsplanen och egenkontrollen som sker via den.

Målområdet för denna föreskrift är inte bestämmelserna om medicintekniska produkter. Bestämmelserna om medicintekniska produkter som beskrivs i kapitel 4 i föreskrift 4/2024 ska beaktas i informationssystem och välbefinnandeapplikationer som uppfyller definitionen av medicintekniska produkter.

5 Väsentliga krav på funktionalitet

De väsentliga kraven på funktionalitet gäller funktioner som implementeras i system och välbefinnandeapplikationer och kapaciteten att behandla olika datainnehåll. Väsentliga krav på funktionalitet är de funktioner och datainnehåll som beskrivs i bilaga 2 till denna föreskrift (Förteckning över väsentliga krav) och som hänvisar till separata, närmare specifikationer. I dessa närmare specifikationer beskrivs också obligatoriska och frivilliga funktioner och uppgifter mer detaljerat. De väsentliga funktionella kraven förtecknas under flikarna ”Toiminnot” (funktioner), ”Tietosisällöt” (datainnehåll) och ”Digitaalisten palvelujen vaatimukset” (krav på digitala tjänster).

Många av de väsentliga kraven på funktionalitet fokuserar i denna föreskrift på de funktioner och uppgifter som är centrala för system och välbefinnandeapplikationer som ansluts direkt eller indirekt till Kanta-tjänsterna.

6 Väsentliga informationssäkerhetskrav

De väsentliga informationssäkerhetskraven gäller egenskaper som implementeras i och via system och välbefinnandeapplikationer för att säkerställa informationssäkerhet och dataskydd. Dessutom inbegriper de

åtgärder som behövs för att planera, implementera eller tillhandahålla ett system, ett delsystem eller en välbefinnandeapplikation samt andra krav som ska omfattas av certifieringen av välbefinnandeapplikationer. Väsentliga informationssäkerhetskrav är de informationssäkerhetskrav som beskrivs i bilaga 2 till denna föreskrift (”Olennaisten vaatimusten luettelo” (förteckning över väsentliga krav), flikarna ”Tietoturvavaatimukset” (informationssäkerhetskrav) och ”Digitaalisten palvelujen vaatimukset” (krav på digitala tjänster)).

I fliken ”Tietoturvavaatimukset” i förteckningen över väsentliga krav beskrivs kravets bindande innehåll under ”Otsikko” (rubrik) och ”Selite” (förklaring). Uppfyllandet av kraven verifieras som en del av bedömningen av informationssäkerheten för system och välbefinnandeapplikationer som hör till klass A. Vid verifieringen används det verifieringssätt som fastställts för varje krav, om kravet är relevant med hänsyn till systemets eller välbefinnandeapplikationens användningsändamål (se kapitel 10.2). Verifieringen som en del av certifieringsprocessen sker i enlighet med föreskrift 4/2024.

En del av kraven på informationssystemets driftsmiljö kan uppfyllas via det system som producenten av en informationssystemtjänst ansvarar för och en del via användarorganisationen. Detaljerna beror på hur systemet implementeras, och detta bör beaktas i avtalen mellan aktörerna samt i användarorganisationernas informationssäkerhetsplaner. Producenten av en informationssystemtjänst måste ta ställning till vilka av de väsentliga informationssäkerhetskraven i systemets driftsmiljö som uppfylls via systemet eller de därtill anslutna tjänsterna som tillhandahålls av producenten av informationssystemtjänsten och vilka av kraven i driftsmiljön som den tjänstetillhandahållare som använder systemet ansvarar för (se kapitel 9). Krav som ingår i ett system eller i en tjänst som tillhandahålls av producenten av en informationssystemtjänst verifieras som en del av bedömningen av informationssäkerheten. Vid verifiering och certifiering förutsätts inte att tjänstetillhandahållarorganisationen deltar i verifieringen av de krav som ställs på driftsmiljön.

En del av informationssäkerhetskraven i bilagorna till denna föreskrift hänvisar till de författningar, separata specifikationer eller standarder som ligger till grund för kraven. Om kravet grundar sig direkt på ett visst källdokument nämns detta separat (direkta källor). En del av källorna stöder tolkningen och tillämpningen av kraven.

7 Minimikravprofiler

Minimikraven för ett system, ett delsystem, en systemhelhet eller en välbefinnandeapplikation avsedd för ett visst användningsändamål kan uttryckas med hjälp av en nationell minimikravprofil (profil). En profil innehåller en delgrupp av de väsentliga krav som beskrivits i förteckningen över väsentliga krav. I bilagorna 3a–3h till föreskriften finns profiler som sammanställer nationella minimikrav för system eller välbefinnandeapplikationer inom social- och hälsovården för flera användningsändamål. Varje bilaga innehåller en eller flera profiler.

De väsentliga kraven enligt en profil ska implementeras eller uppfyllas i ett system eller en välbefinnandeapplikation vars användningsändamål inkluderar det användningsändamål som beskrivs i profilen. Implementeringen av minimikraven enligt en profil är en förutsättning för att ett system, en systemhelhet eller en välbefinnandeapplikation som används för ett visst ändamål ska kunna tas i användning för produktion av tjänster. Profilerna som bifogas denna föreskrift är obligatoriska, med undantag av profilerna 3f1 och 3f2, som är riktgivande och inte gäller välfärdsapplikationer eller informationssystem som används inom social- och hälsovårdstjänsterna.

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska anmäla alla de nationella minimikravprofiler vars användningsändamål ingår i systemet eller välbefinnandeapplikationen. Ett undantag är profiler vars beskrivning särskilt anger att profilen i fråga inte behöver anmälas separat om systemet uppfyller kraven för en annan (mer omfattande) profil.[1] Anmälan görs enligt föreskrift 4/2024 (kapitel 6) till FPA, bedömningsorganet för informationssäkerhet och Valvira med hjälp av systemblanketten i bilaga 4 till denna föreskrift.

[1] När föreskrift 5/2024 träder i kraft är profil 3g1 (i bilaga 3g) en sådan profil vars krav man har tagit ställning till i alla profiler enligt bilagorna 3a–3f. I detta fall behöver inte profil 3g1 anges separat på systemblanketten om systemet uppfyller kraven för någon annan profil.

Ett system, ett delsystem, en systemhelhet eller en välbefinnandeapplikation kan uppfylla kraven i flera profiler. I systemet eller välbefinnandeapplikationen ska åtminstone de väsentliga krav som är obligatoriska i de profiler som motsvarar systemets eller välbefinnandeapplikationens användningsändamål ha implementerats och antecknats på systemblanketten.

Kraven i en viss profil kan uppfyllas med ett eller flera system, delsystem eller välbefinnandeapplikationer. Då ska man i anmälningarna och vid certifieringarna beskriva tillsammans med vilka andra system, delsystem eller välbefinnandeapplikationer systemet, systemtjänsten eller välbefinnandeapplikationen uppfyller kraven i profilen, och vilka andra villkor det finns för att kraven ska uppfyllas. För system och välbefinnandeapplikationer i klass A ska uppfyllandet av kraven vid behov verifieras som en del av certifieringen även när kraven uppfylls via andra system, delsystem eller välbefinnandeapplikationer. Mer information om uppfyllandet av kraven i de modulära systemhelheterna finns i kapitel 6.3 i bilaga 1.

Implementering eller uppfyllande av de krav som förutsätts av profilerna som ingår i informationssystemets eller välbefinnandeapplikationens användningsändamål samt verifiering av dem vid samtestning eller bedömning av informationssäkerheten, i den mån kraven kan verifieras vid certifieringen, är en förutsättning för att certifieringen av system och välbefinnandeapplikationer i klass A ska godkännas och för att de ska kunna tas i användning för produktion av tjänster.

I registret över informationssystem som förs av Valvira anges de profiler som ingår i användningsändamålet för varje system, delsystem och välbefinnandeapplikation. Registrering av ett system eller en välbefinnandeapplikation i klass A i Valviras register över informationssystem att kraven på informationssäkerhet i de profiler som gäller systemet eller applikationen har verifierats med godkänt resultat vid bedömningen av informationssäkerheten och att ett informationssäkerhetsintyg har utfärdats systemet eller applikationen har fått ett informationssäkerhetsintyg. För system och applikationer i klass A2 och A3 förutsätts också godkänd samtestning med FPA gällande de väsentliga krav i profilerna som anknyter till Kanta-tjänsterna.

THL kan också utfärda separata föreskrifter om minimikraven för system eller välbefinnandeapplikationer avsedda för ett visst ändamål och att i dessa föreskrifter hänvisa till profiler som specificerats med hjälp av förteckningen över väsentliga krav.

Användningen av profiler och hur de förhåller sig till väsentliga krav beskrivs också i bilaga 1 kapitel 7.

8 Uppfyllandet av väsentliga krav / producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation

För att påvisa att de väsentliga kraven uppfylls använder producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation den systemblankett som finns i bilaga 4. Med blanketten anmäls uppgifter om systemet och välbefinnandeapplikationen vid certifiering och registrering av system i enlighet med föreskrift 4/2024. Med hjälp av systemblanketten lämnas en utredning om att de väsentliga kraven uppfylls enligt 85 § i lagen om kunduppgifter. Alla väsentliga krav som implementerats i systemet, välbefinnandeapplikationen eller delsystemet beskrivs på en systemblankett. Punkterna om system och välbefinnandeapplikationer i detta kapitel kan också tillämpas på delsystem som kan certifieras som en del av en större systemhelhet.

Ett informationssystem i **klass B** uppfyller de väsentliga krav som ställs på systemet när

1. producenten av en informationssystemtjänst har beskrivit systemets användningsändamål, klassificerat systemet och bedömt systemets risknivå i enlighet med föreskrift 4/2024
2. producenten av en informationssystemtjänst har specificerat på systemblanketten de profiler för de väsentliga kraven (de profiler som presenteras i tabellerna i bilaga 3) som ingår i systemets användningsändamål
3. producenten av en informationssystemtjänst har antecknat på systemblanketten de funktioner i de väsentliga kraven som systemet omfattar

4. producenten av en informationssystemtjänst har antecknat på systemblanketten det datainnehåll för de väsentliga kraven som behandlas i systemet och som uttrycker vilka uppgifter systemet producerar eller använder
5. producenten av en informationssystemtjänst har på systemblanketten antecknat de informationssäkerhetskrav som ingår i de väsentliga kraven och som implementeras i systemet eller uppfylls via det
6. de krav som antecknats i enlighet med punkterna 3–5 omfattar åtminstone kraven enligt de profiler som gäller systemet
7. systemblanketten har, när det gäller kraven i punkterna 3–5, i enlighet med anvisningarna försetts med en anteckning om a) de krav som uppfylls i systemet med hjälp av andra system, välbefinnandeapplikationer eller delsystem, b) de krav i anslutning till vilka betydande ändringar har gjorts i systemet, om sådana krav finns och c) de krav som inte är tillämpliga, om det finns anvisningar om detta i beskrivningen av ett visst krav
8. tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst *själv har testat och verifierat* att de väsentliga kraven i punkterna 3–7 fungerar i systemet.

Ett system eller en välbefinnandeapplikation i **klass A1** uppfyller de väsentliga krav som ställs på det när

9. villkoren för klass B (ovan) har uppfyllts[2]
10. de väsentliga informationssäkerhetskraven för systemet eller välbefinnandeapplikationen (punkt 5) har *implementerats, uppfyllts och dokumenterats* så att en bedömning av informationssäkerheten kan göras och ett intyg över godkänd bedömning av informationssäkerheten kan utfärdas.

Förutsättningar för att ta i användning ett system i klass A1, A2 eller A3 för produktion av tjänster är att informationssäkerhetsintyget över de verifierade informationssäkerhetskraven som beskrivs ovan har utfärdats och att uppgifterna som motsvarar intyget finns i Valviras register över informationssystem (se även föreskrift 4/2024, kap. 9).

Ett system eller en välbefinnandeapplikation i **klass A2** eller ett system i **klass A3** uppfyller de väsentliga krav som ställs på systemet när

11. villkoren för klass A1 (ovan) har uppfyllts
12. man i fråga om det datainnehåll som behandlas (punkt 4) har antecknat på systemblanketten vilka uppgifter systemet eller välbefinnandeapplikationen producerar till Kanta-tjänsterna eller utnyttjar via Kanta-tjänsterna
13. de krav på systemets funktionalitet (funktioner och datainnehåll, punkterna 3–8) som gäller specifikationerna i anslutning till Kanta-tjänsterna har *implementerats, uppfyllts, dokumenterats och testats av producenten av informationssystemtjänsten* så att systemet kan genomgå nödvändiga samtestningar med godkänt resultat enligt anvisningarna för FPA:s samtestning med Kanta-tjänsterna.

Anmälan av ovan nämnda omständigheter med hjälp av systemblanketten beskrivs i kapitel 2.3 i bilaga 1 till föreskrift 5/2024.

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 4/2024, kap. 9).

Överensstämmelsen med kraven för ett system eller en välbefinnandeapplikation som hör till klass A ska påvisas genom certifiering innan det tas i användning för produktion av tjänster. Ett system eller en

[2] Tillverkaren av en välbefinnandeapplikation ansvarar för de olika aspekterna i punkterna 1–8 på motsvarande sätt som producenten av en informationssystemtjänst.

välbefinnandeapplikation i klass A eller B som uppfyller de väsentliga kraven ska registreras i Valviras register över informationssystem. Processen för certifiering och registrering beskrivs i föreskrift 4/2024 (kapitel 7) och i bilaga 1 till denna föreskrift. Numreringen av ovannämnda villkor motsvarar inte direkt skedena i certifierings- och registreringsprocessen.

Om ett system i klass A anmäls till förnyad bedömning av behovet av samtestning eller för bedömning av om systemet behöver en ny bedömning av informationssäkerheten, ska nya funktioner och datainnehåll och sådana som innehåller väsentliga ändringar antecknas tydligt i systemblanketten enligt bilaga 4 (se även kapitel 10 i föreskrift 4/2024).

Systemblanketten enligt denna föreskrift ska fyllas i oberoende av om systemets eller välbefinnandeapplikationens användningsändamål motsvarar någon av de nationella profilerna (ingen, en eller flera). På systemblanketten antecknas också andra väsentliga krav än de som ingår i profilerna som har implementerats eller uppfylls via systemet eller välbefinnandeapplikationen. De väsentliga krav som anges på systemblanketten ska uppfyllas i systemet eller välbefinnandeapplikationen.

Anteckningarna på systemblanketten ska motsvara den systemversion som anmäls till interoperabilitetstestningen, bedömningen av informationssäkerheten eller som ska registreras i Valviras register över informationssystem. På systemblanketten som används vid certifieringen eller registreringen antecknas inte sådana egenskaper som är i planeringsstadiet eller som inte har implementerats i systemet.

Krav som ska uppfyllas via integrationsgränssnitt eller andra system eller delsystem kan antecknas på systemblanketten. Uppfyllandet av de obligatoriska kraven ska vid behov kunna verifieras som en del av certifieringen även i dessa fall.

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska ge akt på ändringar i de väsentliga kraven och justera systemen i enlighet med ändringarna (82 § i lagen om kunduppgifter). Om ändringarna förutsätter en ny samtestning eller en ny bedömning av informationssäkerheten, ska dessa åtgärder vidtas innan den version av systemet eller välbefinnandeapplikationen som innehåller ändringarna tas i användning för produktion av tjänster.

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska vid ansökan om förnyelse av informationssäkerhetsintyget säkerställa att egenskaperna i anslutning till Kanta-tjänsterna har samtestats i systemet eller välbefinnandeapplikationen i enlighet med gällande specifikationer och specifikationsversioner samt kapitel 7.2 i föreskrift 4/2024.

Producenten av en informationssystemtjänst ansvarar för att de väsentliga krav som ingår i systemet eller som certifierats via det uppfylls i systemets olika driftsmiljöer. Användarorganisationen ska vid behov ges anvisningar om hur systemet ska användas så att de väsentliga kraven i systemet uppfylls.

Tjänstetillhandahållaren, FPA, bedömningsorganet, THL eller någon annan instans kan göra en anmälan till Valvira om systemet inte uppfyller de väsentliga krav som ställs när systemet används för produktion av tjänster.

9 Uppfyllandet av väsentliga krav/tjänstetillhandahållare

Enligt 84 § i lagen om kunduppgifter ska de informationssystem som tjänstetillhandahållare och apotek använder till sitt användningsändamål svara mot tjänstetillhandahållarnas och apotekens verksamhet och uppfylla de väsentliga krav som ställs på tjänstetillhandahållarnas och apotekens verksamhet De väsentliga kraven ska uppfyllas i enlighet med bestämmelserna om ikraftträdande och övergångstider i 101 och 102 § i lagen om kunduppgifter. De väsentliga kraven kan uppfyllas genom en helhet som består av ett eller flera system eller delsystem.

Enligt 77 § i lagen om kunduppgifter och THL:s föreskrift 3/2024 ska en tjänstetillhandahållare i sin informationssäkerhetsplan beskriva de system som den använder för behandling av klient- och patientuppgifter.

Tjänstetillhandahållaren ska säkerställa att de system eller delsystem som den använder i sin helhet innehåller de användningsändamål enligt profilerna och uppfyller de krav enligt profilerna som krävs i tjänstetillhandahållarens verksamhet.

En tjänstetillhandahållare ska med iakttagande av tidsfristerna i lagen om kunduppgifter ansluta sig som användare av Kanta-tjänsterna. För att kunna ansluta sig måste tjänstetillhandahållaren ha ett system eller en systemhelhet som uppfyller kraven för anslutning till Kanta-tjänsterna och som gör det möjligt att behandla och lagra de kunduppgifter som behövs i tjänstetillhandahållarens verksamhet. Systemet som används för anslutning kan vara ett system som hör till klass A3 eller en sådan systemhelhet där kraven relaterade till Kanta-tjänsterna uppfylls med hjälp av system eller delsystem som hör till åtminstone klass A2 (se föreskrift 4/2024 kapitel 5 och föreskrift 4/2024 bilaga 1).

En tjänstetillhandahållare ska säkerställa att de system eller välbefinnandeapplikationer i klass A1, A2 eller A3 som denne använder har certifierats med godkänt resultat, att systemens egenskaper som tas i användning för produktion av tjänster via Kanta-tjänsterna har samtestats med godkänt resultat i förhållande till gällande krav och att informationssäkerhetsintyget för dem är giltigt. Tjänstetillhandahållaren ska också i övrigt sträva efter att säkerställa att varje system eller applikation som denne använder uppfyller de väsentliga kraven för sitt användningsändamål. Tjänstetillhandahållaren ska utnyttja Valviras register över informationssystem samt upphandlings- och underhållsavtal med producenter av informationssystemtjänster och tillverkare av välbefinnandeapplikationer för att säkerställa dessa omständigheter. Producenten av en informationssystemtjänst ansvarar i första hand för att de väsentliga kraven som ska uppfyllas och certifieras via systemet uppfylls (se kapitel 8), men systemet ska användas i enlighet med dess användningsändamål och de instruktioner som producenten av informationssystemtjänsten ger.

En tjänstetillhandahållare ska för sin del säkerställa att Valviras register över informationssystem innehåller aktuella uppgifter om de system i klass A1, A2, A3 eller B som används i tjänstetillhandahållarens verksamhet.

Tjänstetillhandahållaren ska beakta väsentliga krav i sin egen verksamhet när system tas i bruk och används för produktion av tjänster samt i verksamheten enligt informationssäkerhetsplanen. Detta gäller de omständigheter och de observationer och förutsättningar som framkommit i certifieringen och som påverkar uppfyllandet av de väsentliga kraven i de system som tjänstetillhandahållaren använder[3]. Särskild uppmärksamhet ska fästas vid de observationer som publiceras via Valviras register över informationssystem för att genomföra systemens överensstämmelse med kraven.

En tjänstetillhandahållare ska enligt 77 § i lagen om kunduppgifter som en del av sin informationssäkerhetsplan säkerställa att informationssystemets driftsmiljö är lämplig för en sådan ändamålsenlig användning av systemen som säkerställer informationssäkerheten och dataskyddet. En del av kraven på driftsmiljön kan uppfyllas via det system som producenten av en informationssystemtjänst ansvarar för (se kapitel 6). Varje system ska uppfylla de väsentliga krav på driftsmiljön som producenten av en informationssystemtjänst ansvarar för. En tjänstetillhandahållare ska säkerställa att man har avtalat med producenterna av informationssystemtjänster och eventuella andra parter om vilka krav på driftsmiljön som ska uppfyllas via respektive part

En tjänstetillhandahållare kan i sin verksamhet också erbjuda sina kunder välbefinnandeapplikationer eller så kan sådana ingå i de informationssystem som tjänstetillhandahållaren använder. Dessutom kan tjänstetillhandahållaren i enlighet med lagen om kunduppgifter utnyttja de uppgifter om välbefinnande som finns i datalagret för egna uppgifter. Det är inte obligatoriskt för tjänstetillhandahållaren att tillhandahålla välbefinnandeapplikationer eller

[3] Det kan till exempel vara fråga om ett informationssäkerhetskrav som för att bli uppfyllt förutsätter åtgärder i driftsmiljön för tjänstetillhandahållaren som använder systemet eller ett krav på funktionalitet som uppfylls via gränssnitten för systemintegration.

utnyttja uppgifter om välbefinnande. Även de informationssystem som tjänstetillhandahållaren använder kan ha egenskaper och användargränssnitt för medborgarna, t.ex. i samband med digitala ärendetjänster[4].

Om en tjänstetillhandahållare själv har rollen som tillverkare av ett informationssystem, producent av en informationssystemtjänst eller tillverkare av en välbefinnandeapplikation, ska tjänstetillhandahållaren i fråga om det system eller den applikation som tjänstetillhandahållaren ansvarar för uppfylla de skyldigheter som författningarna ålägger tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst. Dessa är klassificering av systemet eller applikationen, uppfyllande av de väsentliga kraven, certifiering och registrering. Detta gäller även eventuella situationer där en tjänstetillhandahållare håller på att ta i bruk ett system som inte har en sådan utsedd ansvarig part som ansvarar för överensstämmelsen med kraven enligt lagen om kunduppgifter. En tjänstetillhandahållare som använder systemet eller applikationen ansvarar för dessa åtgärder, om den inte har kommit överens om ansvaret i anslutning till dem med någon producent av informationssystemtjänster.

10 Preciseringar av verifieringen av väsentliga krav

10.1 Bedömning av uppfyllandet av krav i system som inte ansluts till Kanta-tjänsterna

För system i klass B utförs ingen sådan samtestning eller bedömning av informationssäkerheten som hör till certifieringen. För system i klass A1 utförs ingen samtestning, men för dem görs en bedömning av informationssäkerheten (se föreskrift 4/2024 kap. 5 och 7).

I förteckningen över väsentliga krav (bilaga 2) specificeras krav som härrör direkt från de viktigaste bestämmelserna som styr behandlingen av kunduppgifter. Kraven i anslutning till behandling av klient- och patientuppgifter som härrör direkt från bestämmelserna gäller informationssystem och välbefinnandeapplikationer av samtliga klasser. *Specifikationerna och hänvisningarna i dessa krav avseende system som ansluts direkt till Kanta-tjänsterna* gäller dock inte system i klass B eller A1, om inte annat uttryckligen anges i specifikationsdokumentet eller hänvisningen. För system i klass B och A1 härrör innehållet i dessa krav direkt från de bestämmelser som hänvisas till i de olika kraven.

De krav som allmänt gäller behandlingen av klient- och patientuppgifter och som även gäller system i klass B och A1 har sammanställts i profilbilagan 3g till denna föreskrift, ”Minimikrav för system avsedda för behandling av klient- eller patientuppgifter”. Dessa lagstadgade krav gäller alla system avsedda för behandling av klient- eller patientuppgifter, om det inte särskilt anges i den mer detaljerade profilen att kravet inte gäller system enligt profilen i fråga. Om ett system i klass B eller A1 indirekt använder uppgifter i Kanta-tjänsterna eller producerar uppgifter som förmedlas till Kanta-tjänsterna, kan systemet också omfattas av kraven i profilbilaga 3b: 3b2 – applikation som använder uppgifter som hämtas från Kanta-informationsresursen för kunduppgifter eller 3b4 – applikation som producerar uppgifter som förmedlas till Kanta-informationsresursen för kunduppgifter.

Producenten av en informationssystemtjänst antecknar i enlighet med kapitel 8 på systemblanketten både krav enligt profilerna och andra väsentliga krav på systemet än sådana som hör till profilerna och enligt vilka funktioner, datainnehåll eller informationssäkerhetskrav har implementerats i informationssystemet.

10.2 Bedömning av uppfyllandet av kraven och verifieringssätten vid certifiering

I certifieringen av system och välbefinnandeapplikationer i klass A (samtestning och bedömning av informationssäkerheten) bedöms genomförandet av varje krav som har implementerats i systemet eller applikationen och som omfattas av samtestning eller bedömning av informationssäkerheten. Bedömaren vid samtestning är FPA och vid bedömning av informationssäkerheten ett godkänt bedömningsorgan för informationssäkerhet.

[4] Mer information i bilaga 1 kap. 6.5 Krav på välbefinnandeapplikationer och ärendetjänster samt deras förhållande till informationssystemen

I fråga om ett enskilt krav kan den som bedömer kravet ta ställning till huruvida kravet uppfylls enligt följande:

- Huruvida kravet är relevant i systemet:
    - Relevanta krav är åtminstone alla gällande obligatoriska och rekommenderade väsentliga krav som uttrycks i de profiler som motsvarar systemets eller applikationens användningsändamål.
    - Relevanta är de väsentliga krav som producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation har angett som implementerade i den systemblankett som levererats, inklusive både de tidigarenämnda krav som hör till profilerna och de övriga krav som antecknats som uppfyllda via systemet;
    - Om kravet endast delvis är relevant i fråga om det informationssystem, det delsystem eller den välbefinnandeapplikation som ska bedömas eller om det är nödvändigt att särskilt uppge att kravet inte är relevant i systemet eller applikationen (till exempel med beaktande av systemets användningsändamål och begränsningar av användningsändamålet), kan bedömaren göra en anteckning om detta i den rapport, det utlåtande eller det intyg som bedömningen ger upphov till, om saken behöver motiveras[5].
- Avseende relevanta krav:
    - Kravet uppfylls helt (normal situation).
    - Kravet uppfylls inte eller uppfylls endast delvis. Den del som inte uppfylls kompenseras på ett godtagbart sätt så att målet som eftersträvas med kravet uppnås, varvid kompensationssättet måste beskrivas.
    - Kravet uppfylls inte.
    - Vid behov en anteckning om verifieringssättet och hur uppfyllandet av kravet har verifierats, till exempel hänvisning till dokumentation, en testrapport eller programvara.

Ovannämnda uppgifter kan ingå i en detaljerad rapport om samtestning eller bedömning av informationssäkerheten.

De obligatoriska väsentliga kraven på systemets eller välbefinnandeapplikationens användningsändamål måste uppfyllas i de system och applikationer som tas i användning för produktion av tjänster.

Om ett obligatoriskt väsentligt krav inte uppfylls kan bedömaren avbryta bedömningen eller fastställa en tidsfrist för uppfyllandet av kravet innan samtestningen eller bedömningen av informationssäkerheten godkänns som en del av den pågående certifieringsprocessen. Om bedömningen avbrutits eller inte slutförts ska producenten av informationssystemtjänsten inte uppdatera uppgifterna om systemet i Valviras register över informationssystem.

Om ett relevant krav inte uppfylls eller uppfylls endast delvis, men dess mål kan uppnås med godtagbar kompensation, kan bedömaren fatta beslut om godkännande så att den godtagbara kompensationen anges i samtestningsutlåtandet eller informationssäkerhetsintyget. För att bedöma om kompensationen är godtagbar kan bedömaren kräva en riskbedömning och en beskrivning av kompensationen av producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation. Kompensation är en åtgärd som vidtas i undantagsfall och det måste finnas en vägande grund för att godkänna åtgärden till exempel med tanke på klient- eller patientsäkerheten eller social- och hälsovårdstjänsternas funktion. Kompensationen får inte medföra olägenheter eller oskäliga krav eller kostnader för andra aktörer, i synnerhet inte för användarna. Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska underrätta de tjänstetillhandahållare som använder systemet eller applikationen om kompensationer som godkänts.

Om ett obligatoriskt krav i anslutning till den minimikravprofil som systemet eller applikationen förutsätter inte uppfylls och kravet inte kan kompenseras på ett godtagbart sätt, uppfyller systemet eller applikationen inte profilens krav. Samtestningen eller bedömningen av informationssäkerheten kan inte slutföras om inte de obligatoriska

[5] För vissa väsentliga krav uppmanas också producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen att göra en separat anteckning och ge en motivering om kravet i fråga inte är relevant i systemet eller applikationen.

kraven uppfylls eller kompenseras på ett godtagbart sätt. I anmälan till Valviras register över informationssystem ska man inte uppge en profil vars krav på funktionalitet eller interoperabilitet systemet eller applikationen inte uppfyller. Då får systemet eller applikationen inte tas i användning för produktion av tjänster för användningsändamålet i fråga. Informationssystemet kan dock användas för de ändamål för vilka kraven har certifierats med godkänt resultat och anmälts. Då ska producenten av informationssystemtjänsten för sin del säkerställa att systemet inte tas i användning för ett användningsändamål för vilket det inte uppfyller kraven.

Kompensationer och mindre avvikelser från de obligatoriska krav som angetts för systemet och obligatoriska krav enligt de profiler som motsvarar systemets användningsändamål ska antecknas i informationssäkerhetsintyget, om de hänför sig till informationssäkerhetskraven. Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska underrätta de tjänstetillhandahållare som använder systemet eller applikationen om eventuella kompensationer. Mindre avvikelser som upptäckts vid bedömningen av informationssäkerheten och som inte utgör betydande avvikelser som hindrar att systemet tas i användning ska justeras inom skälig tid, dock senast före följande förnyelse av informationssäkerhetsintyget.

Om det vid certifieringen framgår att ett informationssystem eller en välbefinnandeapplikation som *redan är i användning för produktion av tjänster* och som ska certifieras inte uppfyller de obligatoriska relevanta kraven, ska informationssystemet eller applikationen justeras eller kravet kompenseras på ett godtagbart sätt innan samtestningen eller bedömningen av informationssäkerheten i anslutning till kravet godkänns. Betydande avvikelser vid användning i produktion ska anmälas enligt 82 § i lagen om kunduppgifter.

Valvira kan meddela ett föreläggande om att skyldigheten ska fullgöras inom utsatt tid (93 § i lagen om kunduppgifter). Tidsfristen kan också gälla en skyldighet i anslutning till certifieringen för producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation, såsom justering eller kompensation. Tidsfristen kan gälla alla driftsmiljöer för ett system eller en applikation som används för produktion av tjänster (se även kapitel 10.4, punkt 6 i denna föreskrift).

Till Valviras register över informationssystem anmäls i enlighet med 80 § i lagen om kunduppgifter uppgifter om betydande avvikelser hos ett informationssystem eller en välbefinnandeapplikation som hör till klass A och som används i produktion av tjänster, resultat av samtestningen och giltighetstiden för informationssäkerhetsintyget (se föreskrift 4/2024 kap. 8). Valvira kan också besluta om andra uppgifter som ska antecknas i registret över informationssystem, såsom kompensationer som ska beaktas vid användning av systemet eller applikationen eller andra observationer som framkommit i samband med certifieringen.

Om bedömningen av uppfyllandet av ett krav förutsätter en mer precis tolkning av specifikationsdokumentet som ligger till grund för kravet, ska bedömaren vid behov försöka bekräfta tolkningen hos den part som ansvarar för specifikationsdokumentet, till exempel FPA eller THL. Den ansvariga parten ska publicera den preciserade tolkningen, i första hand i samband med det ursprungliga specifikationsdokumentet.

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska förbereda sig för samtestning eller bedömning av informationssäkerheten så att de relevanta kraven har identifierats och så att man kan presentera det material som behövs om uppfyllandet av de relevanta kraven eller vidta nödvändiga verifieringsåtgärder. Till förberedelserna hör också att anteckna separat uttryckta icke-relevanta eller ej tillämpliga krav i enlighet med kapitel 8 och, i förekommande fall, samla in de uppgifter som behövs för verifieringen, om verifieringen kräver uppgifter från tredje part.

Vid verifieringen av informationssäkerhetskraven används följande verifieringssätt:

V: validering eller teknisk inspektion, till exempel genomgång av en logg, meddelandeinstans eller en rapport från systemet eller applikationen.

Testning där

TT: kontroll av huruvida en egenskap finns och är ändamålsenlig genom att systemet eller applikationen används (funktionell testning), som en del av bedömningen av informationssäkerheten

HT: teknisk informationssäkerhets- och sårbarhetstestning och bedömning av säkerhetsnivån genomförs som en del av bedömningen av informationssäkerheten

D: genomgång av systemets eller applikationens dokumentation eller andra systemrelaterade dokument

(kompletterande): H: intervju som en del av bedömningen av informationssäkerheten, som kan fördjupa och komplettera bedömningen; en intervju är inte godtagbar som primär metod för verifiering av krav för system eller välbefinnandeapplikationer i klass A.

Vid verifiering av krav ska man använda ett verifieringssätt som är tillräckligt för att verifiera varje krav eller kravpunkt. Vilket verifieringssätt och vilken verifieringsnivå som är tillräcklig beror på kravet, systemets eller välbefinnandeapplikationens detaljerade klassificering, omfattning och användningsändamål (bland annat med beaktande av innehållets omfattning och den risknivå som avgörs av typen av uppgifter som behandlas). Verifieringssättet och verifieringsnivån för olika krav beskrivs också i bilagorna 1, 2 och 3 till denna föreskrift. För varje informationssäkerhetskrav anges i bilaga 2, och vid behov i profilerna, de verifieringsnivåer som ska användas för system och välbefinnandeapplikationer som hör till olika klasser eller risknivåer eller som är avsedda för olika ändamål.

Om det som ska bedömas är ett väsentligt informationssäkerhetskrav som har verifierats i informationssystemet eller välbefinnandeapplikationen med stöd av andra gällande författningar än lagen om kunduppgifter av en tredje part som godkänns i dessa författningar, ska kravet inte verifieras på nytt. Detta förutsätter att den verifiering som utförts av en tredje part är i kraft och att producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen lägger fram den dokumentation som behövs för verifieringen och godkännandet. Av dokumentationen ska framgå åtminstone tillräckligt specificerade uppgifter om föremålet för det verifierade kravet, den författning eller bestämmelse som verifieringen grundar sig på, det verifierade kravet jämte källhänvisningar och hur kravet motsvarar det väsentliga kravet i fråga, en anteckning om att kravet verifierats med godkänt resultat, uppgifter om den tredje part som verifierat kravet samt verifieringens giltighet. Exempel på krav som verifierats med stöd av andra författningar är externa auditeringar av kvalitetssystemet för tillverkare av medicintekniska produkter och godkända bedömningar av överensstämmelse med de standarder som använts som direkta källor för informationssäkerhetskraven. På systemblanketten i bilaga 4 anmäls sådana andra bedömningar för vilka producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen uppger att en redan utförd verifiering är tillräcklig. Dessa ska anges på sidan med basuppgifter i systemblanketten samt i anslutning till varje väsentligt krav som verifierats på detta sätt.

Vid informationssäkerhetstestning och verifiering av informationssäkerhetskrav rekommenderas att ett lämpligt allmänt ramverk för informationssäkerhetstestning, såsom OWASP ASVS eller MASVS, tillämpas, förutsatt att kraven motsvarar eller är förenliga med informationssäkerhetskraven i bilaga 2.

10.3 Versionshantering av krav och specifikationer

De väsentliga kraven ska uppfyllas vid användning för produktion av tjänster och certifieras enligt gällande specifikationer. Om den specifikation som det hänvisas till i det väsentliga kravet innehåller krav som motsvarar systemets eller applikationens klass och användningsändamål, ska dessa krav uppfyllas i systemet eller applikationen utifrån den gällande versionen av det mer detaljerade specifikationsdokumentet.

THL eller FPA publicerar uppgifter om gällande specifikationer och specifikationsversioner, och med stöd av vilka versioner överensstämmelsen med kraven ska verifieras. FPA publicerar aktuella uppgifter om vilka specifikationer och specifikationsversioner som krävs i Kanta-tjänsternas produktionsmiljö och i samtestning med Kanta-gränssnitt. I ett informationssystem eller en välbefinnandeapplikation som hör till klass A2 eller A3 ska systemimplementeringen, samtestningen och ett positivt utlåtande grunda sig på sådana väsentliga krav, specifikationer och specifikationsversioner som vid respektive tidpunkt förutsätts av ett system eller en applikation som ansluts till Kanta-tjänsterna. I Kanta-tjänsterna är det möjligt att stödja flera versioner av specifikationerna med olika funktioner och datainnehåll. Vid samtestning är det möjligt att stödja eller kräva nya specifikationsversioner innan de börjar stödjas eller krävas i användning för produktion av tjänster.

Om det i samband med att en ny specifikation eller specifikationsversion från THL eller FPA träder i kraft krävs att en tidigare implementering ändras på ett sätt som kräver ny certifiering, anger THL eller FPA detta i samband med att specifikationen publiceras. Om en ny certifiering eller en ny bedömning av certifieringsbehovet krävs, ska dessa åtgärder genomföras inom den tidsfrist som anges i föreskriften eller i anslutning till specifikationen. Implementeringar enligt tidigare specifikationsversioner är också godtagbara vid certifiering och användning för produktion av tjänster om det inte har angetts i specifikationen eller i det material som hänvisar till den att deras giltighet vid användning för produktion av tjänster och certifiering har upphör.

FPA eller THL publicerar information om vilka specifikationsversioner som ska tas bort eller ersättas och fram till vilken tidpunkt man kan godkänna implementeringar enligt en specifikationsversion som ska tas bort eller ersättas vid certifieringen av system i klass A och i produktionsmiljön för Kanta-tjänsterna. Kraven som gäller stöd för olika versioner av strukturer och uppgifter i klienthandlingarna inom socialvården beskrivs i THL:s föreskrift 1/2024.

Anmälningar om systemändringar i förhållande till certifiering av system i klass A behandlas i bilaga 2 till föreskrift 4/2024.

Mer information om användningen av specifikationer och hur de förhåller sig till väsentliga krav finns i bilaga 1 till denna föreskrift.

10.4 Betydande avvikelser från de väsentliga kraven

Betydande avvikelser i system eller välbefinnandeapplikationer som används för produktion av tjänster är:

1. En avvikelse som medför risker för patient- eller klientsäkerheten.
2. En avvikelse som medför betydande risker för dataskyddet, informationssäkerheten eller verksamheten inom social- och hälsovårdstjänsterna.
3. En sådan avvikelse från väsentliga krav i ett informationssystem eller en välbefinnandeapplikation som används för produktion av tjänster som medför betydande eller långvariga återverkningar eller ytterligare avvikelser för flera tjänstetillhandahållare eller flera andra informationssystem.
4. En avvikelse som orsakar omfattande störningar i uppgifternas riktighet, integritet eller interoperabilitet (särskilt via Kanta-tjänsterna).
5. Ett föråldrat informationssäkerhetsintyg (eller överensstämmelseintyg enligt tidigare författningar) för ett system eller en applikation som används för produktion av tjänster, särskilt om förnyandet av intyget drar ut på tiden av orsaker som beror på tillverkaren av ett informationssystem, producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation.
6. I informationssystemet eller välbefinnandeapplikationen har man inte uppfyllt ett obligatoriskt väsentligt krav som hör till dess användningsändamål, dvs. ett krav som anges som obligatoriskt i den profil som motsvarar systemets användningsändamål.
7. Ett informationssystem eller en välbefinnandeapplikation som hör till klass A har inte certifierats med godkänt resultat avseende ett sådant väsentligt krav enligt punkt 6 som är föremål för verifiering genom samtestning eller bedömning av informationssäkerheten.

8. En obligatorisk egenskap i ett system eller en applikation som används för produktion av tjänster grundar sig på en föråldrad specifikationsversion, vars giltighet i produktionen eller stöd i Kanta-tjänsterna har upphört så att systemet inte har kunnat eller inte kan övergå till implementering enligt gällande krav inom den tidsfrist som fastställts i bestämmelserna eller av tillsynsmyndigheten.
9. De tidsfrister för justeringar i systemet eller applikationen som fastställts i författningar eller av myndigheter har inte iakttagits, särskilt om försummelsen upprepas.

Betydande avvikelser ska anmälas i enlighet med 82 § och 90 § i lagen om kunduppgifter. De tillverkare av informationssystem, producenter av informationssystemtjänster, mellanhänder, tjänstetillhandahållare eller tillverkare av välbefinnandeapplikationer som berörs av en betydande avvikelse ska vidta åtgärder för att rätta till avvikelsen. Valvira publicerar information om avvikelser som rör informationssystem och välbefinnandeapplikationer i registret över informationssystem. Valvira styr och främjar överensstämmelsen med kraven i enlighet med lagen om kunduppgifter. Valvira kan bland annat utföra inspektioner (89 §), meddela ett föreläggande att fullgöra en skyldighet eller avhjälpa brister (93 och 94 §), meddela användningsförbud (94 §) samt förena ett föreläggande som det meddelat med vite (96 §).

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 kompenserats 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 justering innan samtestningen eller bedömningen av informationssäkerheten godkänns eller innan bedömningen avbryts, enligt beskrivningen i avsnitt 10.2.

Om ett informationssystem eller en välbefinnandeapplikation som används för produktion av tjänster inte uppfyller de gällande, obligatoriska väsentliga kraven som är tillämpliga på det eller om dess överensstämmelse med kraven har föråldrats, ska producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen underrätta Valvira och de tjänstetillhandahållare som använder informationssystemet om saken. För system eller välbefinnandeapplikationer i klass A2 eller A3 krävs dessutom en anmälan till FPA. Valvira och de tjänstetillhandahållare som använder systemet ska i enlighet med 82 § underrättas om betydande avvikelser. För välbefinnandeapplikationer ska anmälan också göras till applikationens användare. Om en betydande avvikelse beror på tillverkarens verksamhet eller på själva systemet eller välbefinnandeapplikationen, ska producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen bedöma den risk som avvikelsen medför och planera nödvändiga justeringar eller fortsatta åtgärder utifrån en riskbedömning. Om det är fråga om ett krav som har verifierats vid certifiering och som inte uppfylls på grund av ändringar i systemet, ska nödvändiga ändringsanmälningar göras efter justeringen enligt bilaga 2 till föreskrift 4/2024. Dessa åtgärder ska vidtas utöver vad som annars föreskrivs i 82 och 90 § i lagen om kunduppgifter om uppföljning efter ibruktagandet av informationssystem och välbefinnandeapplikationer och om underrättelse om avvikelser.

Ett system, ett delsystem eller en välbefinnandeapplikation ska fungera korrekt i fråga om de väsentliga krav som implementerats i det. En avvikelse från de väsentliga kraven kan konstateras om det är uppenbart att ett system eller en applikation inte fungerar korrekt, till exempel om uppgifter regelbundet kopplas till fel person. Detta förutsätter inte att kravet på korrekthet särskilt omnämns i de väsentliga kraven eller i de specifikationer som de hänvisar till.

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 bilaga 1. Mer information om de väsentliga kraven och certifieringsprocessen samt stöd- och utbildningsmaterial finns på THL:s webbplats och på webbplatsen Kanta.fi.

Institutet för hälsa och välfärd ger på begäran råd och handledning om tillämpningen av denna föreskrift.

12 Ikraftträdande och övergångsbestämmelser

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

I kapitel 12 i föreskrift 4/2024 beskrivs övergångsbestämmelserna med tanke på verifieringen av överensstämmelsen med kraven i tidigare certifierade system och systemens giltighet.

När det gäller ikraftträdandet av kraven i föreskrifterna ska följande beaktas:

- *Datumet då denna föreskrift 5/2024 träder i kraft*, från och med vilket föreskriften och dess bilagor ska tillämpas med de preciseringar som anges i detta kapitel.

- *Datumen som anges i övergångsbestämmelserna för föreskrift 4/2024*. Genom dessa uttrycks giltighetstiden och kontinuiteten för åtgärder och krav som vidtagits innan föreskrifterna trädde i kraft, till exempel giltighetstiden för de tidigare certifierade systemens och välbefinnandeapplikationernas överensstämmelse med kraven eller förfarandena för certifieringsprocesser som pågår när föreskriften träder i kraft.

I fråga om genomförandet av profiler och krav, certifieringen och anmälningarna till Valviras register över informationssystem ska dessutom följande tidpunkter för ikraftträdandet av kraven beaktas:

1. *Datumet då profilen träder i kraft vid certifieringar och i anmälningar*, såsom anges i bilaga 3 till föreskrift 5/2024. Från och med detta datum ska kraven i profilen senast tillämpas vid certifieringen av system och välbefinnandeapplikationer (samtestning och bedömning av informationssäkerheten) och i anmälningar till Valviras register över informationssystem, om systemets användningsändamål överensstämmer med profilen.

2. *Datumet som visas för ett enskilt krav i profilen*. Datumet beskriver tidpunkten då kravet har trätt i kraft eller träder i kraft i de system eller applikationer som används för produktion av tjänster enligt profilen. I ett system eller en applikation som används för produktion enligt profilen ska kravet implementeras eller uppfyllas senast vid denna tidpunkt. Om det står ”rekommenderas” (suositeltava) vid kravet är det en rekommendation att kravet implementeras i ett system eller en applikation som överensstämmer med profilen, men det är inte en förutsättning för att systemet eller applikationen ska kunna tas i användning för produktion av tjänster. Om det står ”giltigt” (voimassa) eller ett passerat datum vid kravet, baseras kravet på tidigare gällande bestämmelser och det ska vara implementerat i alla system och applikationer som används för produktion av tjänster och som omfattas av kravet. Kravens giltighetstid kan också preciseras enligt krav- eller systemklass. Eventuella preciseringar anges vid varje krav i respektive profil. Vid certifieringen iakttas tidsfristerna i punkt 1 så att de krav som gäller åtgärder för samtestning eller bedömning av informationssäkerheten har verifierats och en motsvarande anmälan har sänts till Valviras register över informationssystem innan systemet, systemversionen, välbefinnandeapplikationen eller applikationsversionen tas i användning för produktion av tjänster. Vid certifieringen ska kraven beaktas i testningen och produktionsanvändningen enligt gällande och kommande specifikationer, såsom beskrivs i avsnitt 10.3.

Om ett system eller en välbefinnandeapplikation uppfyller kraven för flera olika profiler och ett krav har olika ikraftträdandedatum i olika profiler, ska kravet i fråga implementeras i systemet eller applikationen enligt det datum som infaller först.

Föreskrifter som utfärdas senare kan ersätta eller komplettera denna föreskrift. Separata föreskrifter kan utfärdas om de väsentliga krav eller profiler som särskilt förutsätts för olika social- och hälsovårdstjänster. Förteckningen över väsentliga krav kan kompletteras utan att föreskriften ändras vid tidpunkter som meddelas separat. Profiler som baseras på föreskriften och förteckningen kan publiceras för nya ändamål, och de kan göras bindande genom nya föreskrifter.

Sirpa Soini

Direktör

Jarmo Kärki

Enhetschef

Bilagor

Bilaga 1. Anvisningar om tillämpningen av väsentliga krav

Bilaga 2. Förteckning över väsentliga krav

Bilaga 3a. Profiler för e-recept

Bilaga 3b. Profiler för system som ansluts till Kanta-informationsresursen för kunduppgifter

Bilaga 3c. Profiler för Patientdataarkivet

Bilaga 3d. Profiler för Klientdataarkivet för socialvården

Bilaga 3e. Profiler för bilddiagnostik

Bilaga 3f. Profiler för intyg (publiceras senare)

Bilaga 3g. Minimikrav på system avsedda för behandling av klient- eller patientuppgifter (inkl. klass B eller A1)

Bilaga 3h. Profiler för medborgarnas digitala tjänster och uppgifter om välbefinnande

Bilaga 4: Systemblankett för väsentliga krav

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