Informationsförmedlare
Information och styrning av informationshanteringen

3.5.2024

FÖRESKRIFT 5/2024 BILAGA 1: ANVISNINGAR OM TILLÄMPNINGEN AV VÄSENTLIGA KRAV

Innehåll

1 Mål

Enligt 84 § i lagen om kunduppgifter ska ett informationssystem och en välbefinnandeapplikation som används vid behandling av kunduppgifter uppfylla väsentliga krav på funktionalitet, interoperabilitet samt informationssäkerhet och dataskydd.

Genom THL:s föreskrifter 4/2024 Föreskrift om klassificering och certifiering av informationssystem och välbefinnandeapplikationer inom social- och hälsovården och 5/2024 Föreskrift om väsentliga krav på informationssystem och välbefinnandeapplikationer inom social- och hälsovården, sammanställs förfaranden och nationellt fastställda krav på informationssystem och välbefinnandeapplikationer avsedda för behandling av kunduppgifter inom social- och hälsovården. Närmare syften samt användningsändamål beskrivs i kapitel 2 i föreskrift 5/2024.

Beskrivningen av de väsentliga kraven på informationssystem och välbefinnandeapplikationer är en del av de lagstadgade skyldigheter som gäller informationssystem och välbefinnandeapplikationer inom social- och hälsovården. Skyldigheterna är avsedda att säkerställa att informationssystem och välbefinnandeapplikationer fungerar och att både kundernas och social- och hälsovårdspersonalens rättsskydd tillgodoses. De väsentliga kraven är ett sätt att styra utvecklingen av informationssystem och välbefinnandeapplikationer på nationell nivå och säkerställa deras informationssäkerhet. De väsentliga kraven på funktionalitet utgör också grunden för de väsentliga kraven på interoperabilitet och informationssäkerhet. En enhetlig beskrivning och avgränsning av systemens och välbefinnandeapplikationernas användningsändamål genom väsentliga krav förtydligar kommunikationen om användningsändamål för olika system och välbefinnandeapplikationer och om vilka nationella krav lösningarna uppfyller. För att kunna trygga de grundläggande målen för informationssäkerhet, såsom konfidentialitet, integritet, tillgänglighet och oavvislighet, ställs både allmänna och specificerade krav på systemen och välbefinnandeapplikationerna samt producenterna och tillverkarna av informationssystemtjänster.

Genom de krav som ställs på informationssystem inom social- och hälsovården förenhetligas sådana aspekter som det med stöd av författningarna är nödvändigt att förenhetliga vid behandlingen av kunduppgifter, till exempel genom att kraven fastställer en nationell miniminivå för systemens funktionalitet, datainnehåll och lösningar som gäller informationssäkerhet och dataskydd. Motsvarande mål gäller också välbefinnandeapplikationer. Detta gör att man kan lita på att systemen och applikationerna har tillräckliga och nödvändiga egenskaper, till exempel med tanke på anslutningen till Kanta-tjänsterna och informationssäkerheten, när man anskaffar, utvecklar och tillhandahåller dem för olika tjänster och olika kundgrupper. Konkurrensen mellan system, välbefinnandeapplikationer och produkter kan bland annat handla om användbarhet och egenskaper som tillför användaren ett särskilt mervärde. Genom att sammanställa de väsentliga kraven i en enhetlig förteckning harmoniseras begrepp som används i de krav som grundar sig på författningar och nationella specifikationer och harmoniseras grundläggande krav som rör systemens och välbefinnandeapplikationernas tillverkare och användare.

Utöver de krav som ställs genom författningarna kan informationssystem och välbefinnandeapplikationer utvärderas till exempel med hänsyn till användbarhet, processändringar, kostnader, effektivitet och flera andra aspekter. Dessa andra aspekter ingår vanligtvis i modellerna för utvärdering av medicinsk teknik (health technology assessment, HTA). Utifrån författningarna fastställs och bedöms minimikrav som kan kompletteras genom mer omfattande utvärderingar av medicinsk teknik.

2 Översikt över användningen av väsentliga krav

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ansvarar för beskrivningen av informationssystemets och välbefinnandeapplikationens användningsändamål, klassificeringen av informationssystemet eller välbefinnandeapplikationen, beaktandet av väsentliga krav vid planeringen och genomförandet av lösningen samt certifieringen och registreringen av informationssystemet eller välbefinnandeapplikationen. Producenten av en informationssystemtjänst kan vara systemtillverkaren eller någon annan aktör som utöver att verifiera de nationella kraven kan ansvara för till exempel stödet till användarorganisationerna.

Det är vanligt att tillverkaren av ett informationssystem ansvarar för klassificeringen och certifieringen av systemet samt registreringen av systemet i Valviras register över informationssystem, även om användarorganisationen kommit överens med en tredje part om till exempel integration, underhåll, applikationsstöd, användarstöd, utbildning eller andra åtgärder. Tillverkaren av informationssystemet är som standard producenten av informationssystemtjänsten, om inte någon annan aktör ansvarar för att registrera och certifiera systemet. En tredje part fungerar som producent av informationssystemtjänsten om den ansvarar för registreringen av systemet och uppfyllandet/certifieringen av de väsentliga kraven. Det är viktigt att ansvaret är tydligt definierat i avtal mellan olika parter. Även en befullmäktigad representant, importör eller distributör för ett informationssystem kan fungera som producent av en informationssystemtjänst, om detta har avtalats med tillverkaren av informationssystemet. I undantagsfall kan även tjänstetillhandahållaren ansvara för de skyldigheter som producenten av informationssystemtjänsten eller tillverkaren av informationssystemet har (se föreskrift 5/2024 kap. 9).

En tjänstetillhandahållare som använder ett informationssystem ansvarar för att använda informationssystem som uppfyller de krav som motsvarar social- och hälsovårdstjänsterna som tjänstetillhandahållaren producerar. Systemen ska användas i enlighet med instruktionerna från producenten av informationssystemtjänsten. Tjänstetillhandahållare ska för sin del säkerställa att det informationssystem som används överensstämmer med kraven. Detta sker bland annat genom att man stöder sig på de uppgifter som finns i Valviras register över informationssystem om systemets överensstämmelse med kraven samt genom att man i avtal som gäller upphandling och underhåll av system säkerställer att kraven för de nationella minimikravprofilerna uppfylls. De tjänstetillhandahållare som använder systemen behöver inte känna till alla väsentliga krav eller detaljerna i hur de uppfylls eller verifieras.

Figur 1 visar en översikt över hur föreskriften om väsentliga krav och förteckningen över dem används. Det viktigaste materialet som anknyter till helheten är föreskrifterna, förteckningen över väsentliga krav, systemblanketten och profilerna.

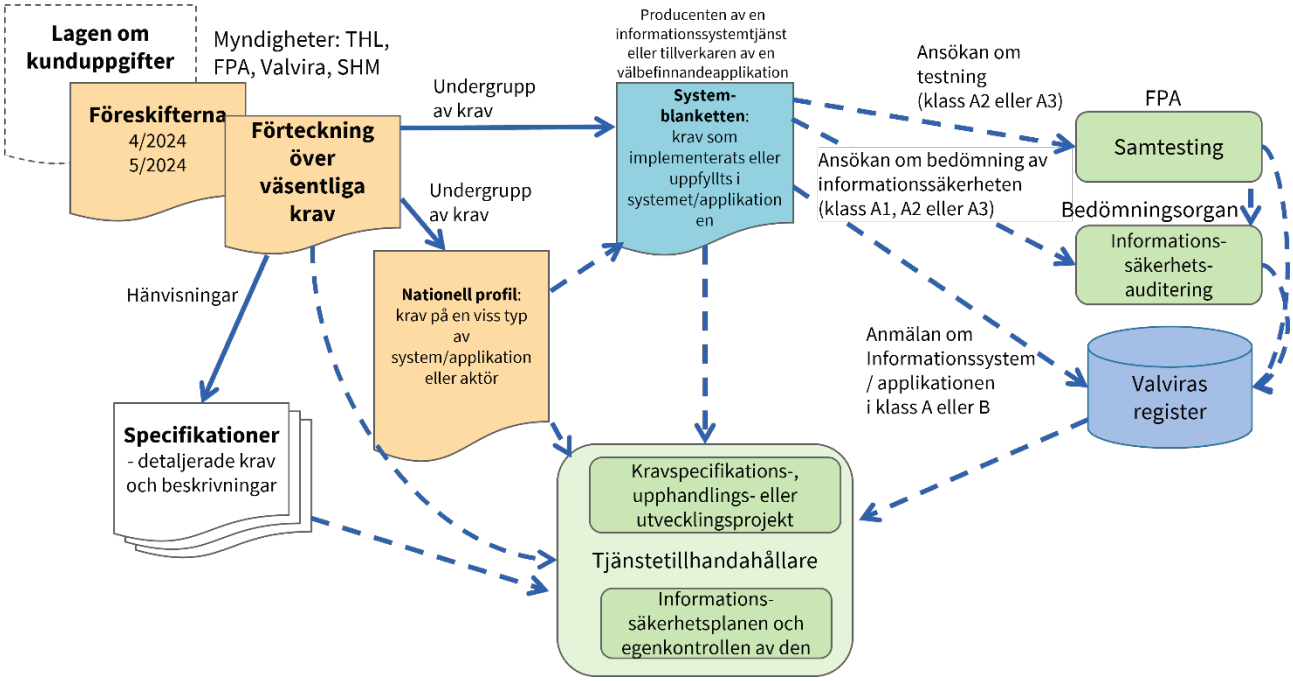

Bild 1. Helheten av väsentliga krav.

2.1 Förteckning över väsentliga krav

Förteckningen över väsentliga krav (föreskrift 5/2024, bilaga 2) är en tabell som sammanställer följande nationella specifikationer för system och välbefinnandeapplikationer som behandlar klient- och patientuppgifter:

- Funktionalitet/funktioner (fliken ”Toiminnot”).
- Datainnehåll (möjligheter att behandla olika datainnehåll) (fliken ”Tietosisällöt”).
- Informationssäkerhetskrav (fliken ”Tietoturvavaatimukset”).

Funktioner i anslutning till välbefinnandeapplikationer, uppgifter om välbefinnande och digitala tjänster som medborgarna använder samt krav som ska beaktas vid bedömningen av informationssäkerheten har dessutom samlats i fliken ”Digitaalisten palvelujen vaatimukset”.

Funktionerna och datainnehållet utgör *väsentliga krav på funktionalitet*.

Största delen av kraven kommer från specifikationsdokument för olika utvecklingshelheter. Funktioner, datainnehåll och datasäkerhetskrav beskrivs på en allmän nivå så att man kan hitta närmare specifikationer genom förteckningen över väsentliga krav. Varje rad med krav har en eller flera källhänvisningar och via länkarna i fliken ”Lähdeviittaukset” (källhänvisningar) kan man se mer detaljerade specifikationsdokument och bestämmelser som de väsentliga kraven grundar sig på. De mest aktuella gällande specifikationerna särskilt för system som ansluts till Kanta-tjänsterna beskrivs på FPA:s och THL:s webbplatser[1] samt i publikationskanalerna för olika datainnehåll, såsom THL:s och FPA:s kodtjänst samt tjänsterna Sosmeta och Termeta. De specifikationsdokument som det hänvisas till innehåller närmare uppgifter om vilka egenskaper eller detaljerade uppgifter som är frivilliga eller obligatoriska i implementeringarna. Huruvida en viss funktion eller ett visst datainnehåll är obligatoriskt beror alltså inte enbart på de uppgifter som beskrivits i profilen och förteckningen, utan de närmare specifikationerna måste beaktas när kraven implementeras. I de nya implementeringarna ska man använda de senaste gällande versionerna av specifikationerna och för användning i produktion av tjänster kan implementeringar enligt vissa specikationsversioner godkännas.

I anslutning till de olika funktionerna och datainnehållen i förteckningen redogörs också för de testhelheter som hänför sig till dem, vilka är avsedda för samtestning av system och applikationer som ska anslutas till Kanta-tjänsterna, samt för de informationssäkerhetskrav som ska verifieras vid bedömningen av informationssäkerheten (om funktionen anknyter till något av informationssäkerhetskraven). De viktigaste specifikationerna som gäller olika funktioner, datainnehåll och informationssäkerhetskrav nämns i anslutning till respektive väsentligt krav och finns i fliken med hänvisningar till källdokument i förteckningen över väsentliga krav. I förteckningen beskrivs också strukturеringsnivån för de nationella specifikationer som finns tillgängliga för olika datainnehåll. Förhållandena mellan de väsentliga kraven beskrivs som en del av förteckningen, till exempel när en viss funktion är förenad med krav som gäller datainnehåll som beskrivs separat eller någon annan funktion.

De funktioner, datainnehåll och informationssäkerhetskrav som ingår i de väsentliga kraven har grupperats så att samma kravgrupp innehåller krav inom samma ämnesområde. Syftet med grupperingen är enbart att sammanställa krav inom samma ämnesområde – de faktiska systemkraven och profilerna gäller alltid specifika krav och inte kravgrupper.

Systemets eller välbefinnandeapplikationens användningsändamål och de nationellt fastställda kraven styr vilken typ av innehåll och funktioner samt vilka informationssäkerhetsegenskaper som åtminstone ska finnas i systemet. I system eller välbefinnandeapplikationer som ansluts till Kanta-tjänsterna (klass A2 eller A3) implementeras de funktionella kraven enligt de detaljerade specifikationer som det hänvisas till. I andra system (klass B och A1) grundar sig många väsentliga krav på bestämmelser på högre nivå och endast vissa system har detaljerade nationella specifikationsdokument avseende innehåll eller funktioner.

[1] Till exempel finns de nyaste versionerna av Kanta-specifikationerna på Kanta-sidorna (avsnittet Systemutvecklare) och på THL:s sidor (avsnittet om specifikationer).

2.2 Minimikravprofiler

Förteckningen över väsentliga krav ligger också till grund för *profilerna*. En profil sammanställer de nationella minimikraven för system och applikationer avsedda för ett visst användningsändamål. En profil innehåller alltså en delgrupp av de funktioner, datainnehåll och informationssäkerhetskrav som beskrivs i förteckningen över väsentliga krav. Profiler publiceras för sådana användningsändamål där det är viktigt att harmonisera minimikraven för ett antal informationssystem eller välbefinnandeapplikationer.

Profiler kan publiceras separat från uppdateringen av förteckingen över väsentliga krav, och nya minimikravprofiler kan publiceras för informationssystem och välbefinnandeapplikationer avsedda för olika användningsändamål. Profilerna täcker inte alla möjliga användningsändamål för system eller välbefinnandeapplikationer i klass A eller B. Till exempel har specifika profiler inte publicerats för alla system som används inom olika specialiteter inom hälso- och sjukvården eller inom olika socialvårdstjänster.

De väsentliga kraven och profilerna är en central utgångspunkt för planeringen och genomförandet av system eller välbefinnandeapplikationer avsedda för behandling av patientuppgifter inom hälso- och sjukvården eller klientuppgifter inom socialvården. Uppfyllandet av minimikraven enligt profilen i bilagan till föreskriften är en förutsättning för att ett informationssystem, en informationssystemhelhet eller en välbefinnandeapplikation som används för profilens användningsändamål ska kunna tas i användning för produktion av tjänster. I ett informationssystem eller en informationssystemhelhet vars användningsändamål motsvarar en profil ska åtminstone de egenskaper som angetts som obligatoriska i profilen implementeras eller uppfyllas i enlighet med de specifikationer som det hänvisas till. Motsvarande krav gäller välbefinnandeapplikationer.

Profilerna finns i bilaga 3 till föreskrift 5/2024. I bilagan finns flera tabeller och varje tabell innehåller en eller flera profiler. Till exempel innehåller bilaga 3a två profiler: patientdatasystem som behandlar recept samt apotekssystem.

Varje profil innehåller sådana funktioner, datainnehåll och informationssäkerhetskrav som enligt specifikationerna ska implementeras i ett informationssystem eller en välbefinnandeapplikation som används för det användningsändamål som profilen avser. Till exempel innehåller profilen för apotekssystem (föreskrift 5/2024 bilaga 3a, profil 3a2) minst de funktioner och uppgifter som krävs av de informationssystem som apoteken använder för att behandla recept och läkemedelsexpedieringar. Profilen innehåller bland annat de funktioner och uppgifter som behövs för att söka receptuppgifter och expediera läkemedel samt sådana informationssäkerhetskrav som åtminstone är nödvändiga för apoteksverksamheten i det informationssystem som används för att behandla recept och läkemedelsexpedieringar (se även kapitel 6.6).

Profilerna har sammanställts i synnerhet för informationssystem som ansluts till olika Kanta-tjänster, såsom Patientdataarkivet, Klientdataarkivet för socialvården, datalagret för egna uppgifter och receptcentret. En del av profilerna, såsom profilen i bilaga 3g till föreskrift 5/2024, består dock av en mer omfattande sammanställning av de krav som ställs i olika författningar på alla system i klass B eller A. I system och välbefinnandeapplikationer som hör till klass A (även A1) går man igenom informationssäkerhetskraven vid bedömningen av informationssäkerheten, men flera informationssäkerhetskrav gäller även informationssystem som hör till klass B.

Ett system eller en välbefinnandeapplikation kan uppfylla kraven för flera olika profiler. Till exempel kan ett omfattande klient- och patientdatasystem uppfylla alla profiler i bilaga 3b, de grundläggande kraven för ett journalsystem (bilaga 3c), profilerna för Klientdataarkivet för socialvården (bilaga 3d), profilen för ett patientdatasystem som behandlar recept (bilaga 3a), profilen för en tjänst som producerar intyg eller utlåtanden i Kanta-arkivet (bilaga 3f) samt profilen för ett system som hämtar uppgifter om välbefinnande åt professionella (bilaga 3h). I samma system kan det också finnas en del för medborgarärenden (bilaga 3h) eller ett delsystem för medborgaranvändning enligt definitionen av en välbefinnandeapplikation (bilaga 3h), se kapitel 6.5. Utöver profilkraven implementeras alltid även andra krav i systemen. Dessa kan både vara sådana för vilka det finns ett eget väsentligt krav (utanför profilen) och eller krav som är specifika för projektet eller användarorganisationen.

Profilerna beskriver också vid vilken tidpunkt de olika kraven ska uppfyllas. Profilerna och de krav som hör till profilerna har ikraftträdandetider som återspeglar till exempel de tidsfrister som författningarna kräver för att en viss

typ av uppgifter ska arkiveras i Kanta-tjänsterna eller för att en viss specifikationsversion ska stödas i system som används för produktion av tjänster och som ansluts till Kanta-tjänsterna. Profilernas giltighetstider och övergångstider baserar sig på nationella författningar och föreskrifter, såsom övergångsbestämmelserna i lagen om kunduppgifter. Om datumet då profilen träder i kraft och datumet som angetts för ett krav har passerat, i kraft (”voimassa”), eller införs i samband med anslutningen (”liittymisen yhteydessä” innebär det att kravet redan gäller. Då ska det system (och dess nya versioner) som ska tas i användning enligt profilen, redan används eller som ska anslutas till Kanta-tjänsterna uppfylla kravet.

Systemets klass avgörs inte direkt utifrån vilka profiler eller funktioner som implementeras i systemet. Till exempel kan ett system av klass A1 vara ett system där gränssnitt och krav relaterade till Kanta-tjänsterna uppfylls och verifieras via ett informationssystem eller delsystem som hör till klass A3.

2.3 Systemblanketten som används av producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation beskriver användningsändamålet för det egna systemet eller välbefinnandeapplikationen, de väsentliga krav som implementerats i systemet eller välbefinnandeapplikationen samt de minimikravprofiler som systemet eller välbefinnandeapplikationen följer på en systemblankett. Systemblanketten grundar sig på förteckningen över väsentliga krav. På blanketten beskrivs funktionerna, datainnehållet och informationssäkerhetskraven i ett enskilt informationssystem, en välbefinnandeapplikation, ett delsystem eller en informationssystemhelhet. Systemblanketten innehåller inte alla tilläggsuppgifter som ingår i förteckningen över väsentliga krav. Mer information om kraven på systemblanketten finns i förteckningen och de källdokument som den hänvisar till.

Den ifyllda systemblanketten fungerar som en redogörelse enligt lagen om kunduppgifter om att de väsentliga kraven uppfylls i systemet eller välbefinnandeapplikationen. Systemblanketten ska fyllas i och en redogörelse lämnas för alla informationssystem (klass A eller B) eller välbefinnandeapplikationer enligt definitionen i lagen om kunduppgifter. Systemblanketten dokumenterar hur de väsentliga kraven på systemet eller välbefinnandeapplikationen har beaktats i planeringen, genomförandet och dokumentationen av systemet eller välbefinnandeapplikationen samt i planeringen av och anvisningarna om användningen. Det är viktigt att beakta systemets eller välbefinnandeapplikationens användningsändamål, klassificering, risknivå, väsentliga krav och profiler redan vid planeringen av systemet eller välbefinnandeapplikationen eller dess uppdateringar.

Systemblanketten används när producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ansöker om FPA:s samtestning för testning av ett informationssystem eller en välbefinnandeapplikation i klass A2 eller A3 som ska anslutas till Kanta-tjänsterna. Många av de väsentliga kraven gäller datainnehåll och funktioner som testas som en del av samtestningen. Sådana väsentliga krav har länkats till FPA:s samtestningshelheter, där man utifrån de specifikationer som hänvisas till i de olika kraven testar interoperabiliteten mellan system eller välbefinnandeapplikationer som ska anslutas till Kanta-tjänsterna och andra system eller applikationer som är anslutna till Kanta-tjänsterna.

Systemblanketten används också när bedömningen av informationssäkerhet av ett informationssystem eller en välbefinnandeapplikation i klass A1, A2 eller A3 inleds. De väsentliga informationssäkerhetskraven används som kriterier för bedömning av informationssäkerheten och som grund för informationssäkerhetsintyget som utfärdas för system eller välbefinnandeapplikationer i klass A.

Blanketten finns också som bilaga till anmälan som enligt lag ska göras till Valvira för varje informationssystem i klass B, A1, A2 eller A3 som behandlar klient- eller patientuppgifter och som tas i bruk inom social- och hälsovården. Anmälan ska också göras för välbefinnandeapplikationer, med blanketten som bilaga. Valvira för ett offentligt register över de informationssystem och välbefinnandeapplikationer inom social- och hälsovården som anmälts till Valvira. Valviras register över informationssystem innehåller uppgifter om den anmälan som producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation har lämnat, uppgifter om de samtestningar och den bedömning av informationssäkerheten som systemet eller applikationen genomgått samt till

exempel uppgifter som uppkommit i samband med Valviras tillsynsprocess. Uppgifterna i registret kan granskas via Valviras webbplats.

Den lagstadgade anmälan som ska göras till Valvira gäller alla informationssystem inom social- och hälsovården som hör till klasserna A och B och vars användningssyfte är behandling av klient- eller patientuppgifter, även om systemet inte är anslutet till Kanta-tjänsterna. Den lagstadgade anmälan till Valvira gäller alla välbefinnandeapplikationer i klass A vars användningsändamål måste vara att främja välfärd och hälsa. Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ansvarar också för att de uppgifter som anmälts till registret är aktuella.

Med systemblanketten uppfyller alltså producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ett antal lagstadgade skyldigheter. På blanketten anger man basuppgifter om systemet eller välbefinnandeapplikationen, beskriver systemets eller välbefinnandeapplikationens användningsändamål, tar ställning till vilka nationella profiler och krav som har implementerats och beskriver vid behov egenskaper som har ändrats jämfört med tidigare versioner eller förhållandet till andra system eller applikationer.

Endast de krav som implementerats i systemet eller välbefinnandeapplikationen eller som uppfylls via systemet ska anges på systemblanketten. Uppfyllandet av kraven ska vid behov kunna verifieras som en del av certifieringen eller på begäran av tillsynsmyndigheten.

Systemblanketten fylls i enligt följande steg när producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation använder blanketten i certifieringsprocessen eller i anmälan till Valvira:

1. Fyll i basuppgifter om systemet eller välbefinnandeapplikationen: systemets eller välbefinnandeapplikationens namn, producenten av informationssystemtjänsten, tillverkaren (kan också vara samma som producenten av informationssystemtjänsten) eller tillverkaren av välbefinnandeapplikationen, version[2].
2. Beskriv kort systemets eller välbefinnandeapplikationens användningsändamål: för vilket ändamål, till vilka tjänster och med vilka begränsningar systemet eller välbefinnandeapplikationen ska användas. Ange dessa uppgifter vid punkterna för beskrivning av användningsändamålet och användningskontext på blanketten (välj till exempel offentliga eller privata social- eller hälsovårdstjänster, digitala tjänster för medborgare).
3. Beskriv systemets risknivå utifrån riskbedömningen av systemet och hur omfattande användning av kunduppgifter och uppgifter om välbefinnande systemet är avsett för på de grunder som beskrivs i föreskrift 4/2024 och dess bilaga 1. Utnyttja vid behov stödmaterial såsom THL:s verktyg för riskbedömning.
4. Ange under punkten *Systemets/välbefinnandeapplikationens klass* till vilken klass systemet hör (A3, A2, A1 eller B) i enlighet med föreskrift 4/2024 och dess bilaga 1.
5. I punkten för profiler (Profiilit) i systemblanketten ska du ange de profiler i bilaga 3 till föreskrift 5/2024 vars användningsändamål är en del av systemets eller välbefinnandeapplikationens användningsändamål. Varje profils namn och beskrivning samt tilläggsuppgifter innehåller information om hur profilen tillämpas. De profiler vars användningsändamål systemet eller välbefinnandeapplikationen är avsett för ska implementeras i systemet eller välbefinnandeapplikationen och anges i blanketten. Det räcker med att ange profilernas koder (till exempel ”3a1, 3c1”) på systemblanketten, du behöver inte skriva profilens hela namn. I synnerhet för certifierade system som hör till klass A2 eller A3 är det viktigt att identifiera och ange

[2] Även om versionsnumret kan ändras ofta är det viktigt att skilja mellan nyare och äldre versioner av systemet eller välbefinnandeapplikationen i certifieringen, så att implementeringen av de verifierade kraven kan spåras, certifieringsresultaten kan jämföras med system som används i produktion i olika driftsmiljöer och samtestningen och bedömingen av informationssäkerheten kan göras med rätt systemversioner. Se även kapitel 7.3 i föreskrift 4/2024 och kapitel 2.2 i denna bilaga.

de profiler som motsvarar systemets användningsändamål och de krav som skapas via dem på rätt sätt redan när man söker sig till samtestning.

6. I fliken för funktioner (Toiminnot) i blanketten anger du de funktioner som motsvarar väsentliga krav och som har implementerats i systemet eller välbefinnandeapplikationen.
7. I fliken för datainnehåll (Tietosisällöt) i blanketten anger du det datainnehåll som motsvarar väsentliga krav och som har implementerats i systemet eller välbefinnandeapplikationen.
8. I fliken för informationssäkerhetskrav (Tietoturvavaatimukset) anger du de informationssäkerhetskrav som har implementerats i systemet eller som uppfylls via systemet eller välbefinnandeapplikationen.
9. Om det är fråga om en välbefinnandeapplikation, ett system som använder uppgifter om välbefinnande eller en digital ärendetjänst för medborgare (eller om dessa egenskaper finns i systemet), ange i fliken för krav på digitala tjänster (Digit. palvelujen vaatimukset) de väsentliga krav som gäller dessa egenskaper, så som vid punkterna 6–8.
10. Kontrollera att funktionerna, innehållet och informationssäkerhetskraven som du fyllt i på systemblanketten motsvarar de krav som anges som obligatoriska i de profiler du valt under punkt 3. Profilerna kan också användas som underlag för att fylla i punkterna 6–9 så att kraven på alla profiler som gäller systemet eller applikationen fylls i först och sedan kompletteras blanketten med de andra väsentliga krav som är relevanta för systemet eller applikationen.
11. Säkerställ att implementeringen är förenlig med kraven, testa och dokumentera de väsentliga krav som implementerats i systemet eller välbefinnandeapplikationen innan systemet eller välbefinnandeapplikationen certifieras eller registreras, både de väsentliga krav som ingår i profilerna och andra väsentliga krav som implementerats i systemet eller välbefinnandeapplikationen.
12. Kontrollera uppgifterna på blanketten och använd blanketten i situationer enligt figur 1 vid certifiering och registrering av systemet eller välbefinnandeapplikationen.
13. Uppdatera blanketten när ändringar görs i systemet eller välbefinnandeapplikationen – de krav som har ändrats jämfört med den tidigare versionen av blanketten ska anges som ändrade i de nya versionerna av blanketten.
14. Följ med ändringar i de väsentliga kraven och de specifikationer som de hänvisar till samt versionsuppdateringarna och beakta dessa i de funktioner som implementerats i systemet, vid ändringsanmälningar och vid förnyande av överensstämmelsen med kraven.

Betydelsen av att använda blanketten vid anmälan och precisering av de väsentliga krav som uppfylls, till exempel anmälan av implementerade profiler, beskrivs i kapitel 8 i föreskrift 5/2024. Under de olika punkterna av systemblanketten och på sidan med allmänna uppgifter och anvisningar om hur blanketten ska fyllas i finns närmare anvisningar för de olika punkterna. Närmare information om varje kravrad i systemblanketten hittas vid behov i bilaga 2 till föreskrift 5/2024 innehållande förteckningen över väsentliga krav. Närmare uppgifter är bland annat förhållandena mellan olika krav, närmare specifikationer och författningar i anslutning till respektive krav samt kravens överensstämmelse med kraven i tidigare föreskrifter.

I punkterna 6–9 på blanketten anges både de egenskaper som implementerats i systemet eller välbefinnandeapplikationen utifrån profiler som motsvarar systemets eller välbefinnandeapplikationens användningsändamål och systemets eller välbefinnandeapplikationens övriga egenskaper. Om systemet till exempel uppfyller kraven enligt profilen för de grundläggande kraven i ett journalsystem (profil 3c1) men dessutom har egenskaper för dokumentation och hantering av näringsuppgifter (datainnehållskrav TPOT25, som inte är obligatoriskt i profilen), ska också implementeringen av näringsuppgifterna anges på systemblanketten.

Krav som när systemet används uppfylls via andra informationssystem eller separat beskrivna delsystem som ansluts till systemet ska också anges i punkterna 6–9 på blanketten. Samma systemhelhet eller kundmiljö kan innehålla system eller delsystem som tillverkats av olika aktörer eller som olika producenter av informationssystemtjänster

ansvarar för. I fråga om informationssystemhelheter som består av olika system och i modulära informationssystem används blanketten för enskilda delsystem om de olika delsystemen certifieras eller registreras separat. Blanketten kan också användas för att beskriva en systemhelhet som består av flera delsystem, till exempel om samtestningen gäller en helhet som ska uppfyllas via flera olika delsystem i en informationssystemhelhet för bilddiagnostik. Vid certifiering och registrering av system ska man dock se till att blanketten är ifylld för varje delsystem som ska omfattas av ett separat samtestningsutlåtande eller informationssäkerhetsintyg eller separat registrering. Mer information finns i kapitel 6.3 i denna bilaga.

Systemblanketten ska på begäran också sändas till tjänstetillhandahållare inom social- och hälsovården eller apotek som begär anbud på ett system avsett för behandling av patientuppgifter eller klientuppgifter inom socialvården.

3 Betydelsen och utnyttjandet av Valviras informationssystemregister

Valviras register över informationssystem inom social- och hälsovården sammanställer uppgifter om anmälda informationssystem och välbefinnandeapplikationer samt resultaten av samtestningen och bedömningen av informationssäkerheten avseende informationssystem och välbefinnandeapplikationer. Valvira publicerar de centrala uppgifterna om informationssystemen och välbefinnandeapplikationerna som finns i registret.

Via registret över informationssystem finns offentligt tillgängliga uppgifter om informationssystem och välbefinnandeapplikationer avsedda för behandling av kunduppgifter inom social- och hälsovården. De offentliga uppgifterna i registret är en viktig grund för bland annat tillsynen över informationssystemen och välbefinnandeapplikationerna och deras överensstämmelse med kraven. Tjänstetillhandahållare inom social- och hälsovården kan utnyttja uppgifterna i Valvira register över informationssystem till exempel som stöd för upphandlingar. Genom att anmäla informationssystem och välbefinnandeapplikationer till registret med hjälp av väsentliga krav och profiler kan man till exempel göra uppgifter om godkända och certifierade system och välbefinnandeapplikationer som uppfyller olika profiler synliga eller sökbara på ett jämförbart sätt. Uppgifterna i registret över informationssystem och mer information om registret finns på Valviras webbplats.

Genom anmälan till Valvira och tillhörande beskrivningar försäkrar producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation att systemet eller välbefinnandeapplikationen uppfyller de väsentliga kraven i 84 § i lagen om kunduppgifter när det installeras och drivs på behörigt sätt och används i enlighet med användningsändamålet. Anmälaren ansvarar för att de anmälda funktionerna och datainnehållen är implementerade i systemet eller välbefinnandeapplikationen. I informationssystem och välbefinnandeapplikationer som hör till klass A ska uppgifterna på blanketten också motsvara resultaten av bedömningen av informationssäkerheten och eventuell samtestning.

I anmälningar till Valviras register över informationssystem ska man följa eventuella anvisningar och föreskrifter från Valvira. Det är inte nödvändigt att anmäla alla nya versioner av ett informationssystem eller en välbefinnandeapplikation till Valviras register över informationssystem. Oberoende av anmälan ansvarar producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation för att den nya versionen uppfyller de väsentliga kraven på minst samma nivå som den tidigare versionen.

Tillsynsmyndigheterna, såsom Valvira, Dataombudsmannens byrå och regionförvaltningsverken, övervakar med hjälp av registret att kraven enligt lagen om kunduppgifter uppfylls. Uppgifterna som skickas in till registret ska vara korrekta och aktuella.

4 Utnyttjandet av väsentliga krav och profiler i organisationer inom social- och hälsovården

Enligt 84 § i lagen om kunduppgifter ska de informationssystem som en tjänstetillhandahållare använder till sitt användningsändamål svara mot tjänstetillhandahållarens verksamhet och uppfylla de väsentliga krav som ställs på tjänstetillhandahållarens verksamhet. Föreskrift 5/2024 (särskilt kapitel 9) preciserar hur dessa omständigheter

säkerställs. Väsentliga krav i anslutning till tjänstetillhandahållarens verksamhet kan uppfyllas med en helhet som består av ett eller flera informationssystem.

Anordnaren eller producenten av social- och hälsovårdstjänster ska säkerställa att

1. användningsändamålet för de informationssystem eller delsystem som den använder som helhet motsvarar organisationens verksamhet
2. uppgifter om de informationssystem i klass A och klass B som den använder finns i Valviras register
3. de system i klass A1, A2 och A3 som den använder har ett giltigt informationssäkerhetsintyg
4. de system i klass A2 eller A3 som den använder och som ska anslutas till Kanta-tjänsterna har samtestats i förhållande till funktioner och datainnehåll som innehåller krav relaterade till Kanta-tjänsterna, vilka ska verifieras vid samtestning
5. de informationssystem eller delsystem som den använder i sin helhet uppfyller kraven för de nationella minimikravprofilerna i den mån verksamheten kräver användning av informationssystem för de användningsändamål som beskrivs i profilerna
6. man vid användningen av informationssystemen beaktar sådana observationer och förutsättningar avseende de väsentliga kraven som framkommit i certifieringen och som påverkar uppfyllandet av de väsentliga kraven i de system som används
7. om det i verksamheten också används välbefinnandeapplikationer eller om det finns sådana delsystem i systemen som uppfyller definitionen av en välbefinnandeapplikation, uppfylls punkterna 2, 3, 4 och 6 också i fråga om de välbefinnandeapplikationer som används.

Som ett praktiskt verktyg för att säkerställa dessa aspekter ska en informationssäkerhetsplan enligt föreskrift 3/2024 användas, där man ska beskriva de informationssystem som tjänstetillhandahållaren använder för behandling av patientuppgifter eller socialvårdens klientuppgifter. Uppgifterna om de informationssystem som används och deras överensstämmelse med kraven uppdateras vid behov som en del av den regelbundna uppdateringen och egenkontrollen av informationssäkerhetsplanen med hjälp av till exempel Valviras register över informationssystem och uppgifter från producenter av informationssystemtjänster. Planen ska också inbegripa de informationssystem som tjänstetillhandahållaren använder och där digitala tjänster som behandlar kunduppgifter tillhandahålls medborgarna och bör även inkludera eventuella välbefinnandeapplikationer som ska användas eller tillhandahållas kunderna i verksamheten.

En tjänstetillhandahållare inom social- och hälsovården kan utnyttja och tillämpa förteckningen över väsentliga krav och kravprofilerna, Valviras register samt systemblanketten i informationssystemens kravspecifikationer, upphandlingar och utvecklingsarbete. När man gör riskbedömningar för olika informationssystem kan man utnyttja riskbedömningsverktyget som används för klassificering och certifiering av informationssystem, även om verktyget i första hand är avsett att hjälpa producenter av informationssystemtjänster och tillverkare av välbefinnandeapplikationer att fastställa risknivån.

I samband med upphandlingar av informationssystem måste man säkerställa att systemen som upphandlas uppfyller de nationella minimikraven. Om föremålet för upphandlingen är ett system som behandlar klient- eller patientuppgifter, bör en del av kraven i upphandlingen fastställas via väsentliga krav eller profiler som sammanställer sådana. I Valviras register över informationssystem kan man kontrollera vilka system som hör till olika klasser och som uppfyller olika profiler. Registret innehåller också de viktigaste uppgifterna om system som ansluts till Kanta-tjänsterna och som har godkänts vid samtestning med FPA samt uppgifter om bedömningen av informationssäkerheten och informationssäkerhetsintygets giltighet för system som är certifierade i klass A. Motsvarande uppgifter om välbefinnandeapplikationer finns också i registret.

Anordnaren eller producenten av social- och hälsovårdstjänster kan också i anbudsförfrågningar som gäller upphandlingar begära en systemblankett av producenten av informationssystemtjänster och jämföra uppgifterna i blanketten med de krav som fastställts i upphandlingen och med de uppgifter som finns i Valviras register över informationssystem. På så sätt kan man säkerställa att det system som ska upphandlas uppfyller de nationella krav som fastställts med stöd av lagen om kunduppgifter.

Systemblanketten kan också tillämpas på annat sätt i tjänstetillhandahållarens verksamhet. På blanketten kan man till exempel ange olika system genom vilka tjänstetillhandahållaren uppfyller eller kan uppfylla de olika kraven i sin egen verksamhet.

5 Tillämpningen av certifieringsprocessen

Certifieringen gäller informationssystem i klass A1, A2 eller A3 samt alla välbefinnandeapplikationer som avses i lagen om kunduppgifter. Klassificeringen av ett informationssystem görs i enlighet med föreskrift 4/2024 och dess bilaga 1. Godkänd certifiering är en förutsättning för registrering och ibruktagande av informationssystem eller välbefinnandeapplikationer i klass A. Ett delsystem som är avsett att användas tillsammans med andra informationssystem eller delsystem kan också certifieras.

Åtgärder som föregår certifieringsprocessen enligt föreskrift 4/2024 och som utförs av tillverkaren av ett informationssystem i klass A eller producenten av en informationssystemtjänst är bland annat

- fastställande av användningsändamålet för systemet eller välbefinnandeapplikationen
    - inklusive klassificering samt ställningstagande till vilka av profilerna för väsentliga krav och vilka andra väsentliga krav som ingår i systemets användningsändamål
- planering och implementering av systemet eller välbefinnandeapplikationen
- egen testning som utförs av producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen
- nödvändig dokumentation

    inklusive systemblanketten och dokumentationen av uppfyllandet av väsentliga krav som verifieras genom dokumentation.

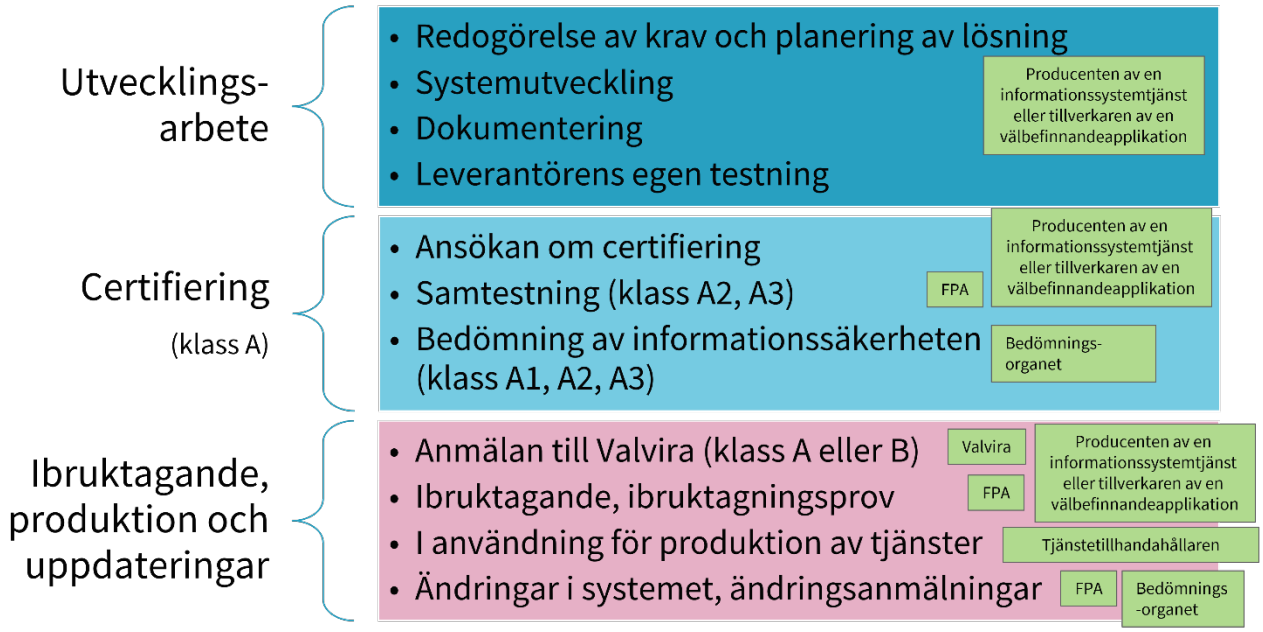

Bild 2. Certifieringsprocessen samt föregående och efterföljande åtgärder.

I figur 2 finns en översikt över certifieringsprocessen, de föregående och efterföljande faserna samt aktörerna som deltar i processen. Även i anmälningar om ändringar iakttas samma förfaranden, som följer anvisningarna i bilaga 2 till föreskrift 4/2024.

Om systemet hör till klass A2 eller A3 inleder producenten av informationssystemtjänsten certifieringsprocessen genom att kontakta FPA:s samtestning och komma överens om samtestningen. FPA ger närmare anvisningar om hur

man ansöker om samtestning och i vilket skede av certifieringsprocessen man kan inleda en bedömning av informationssäkerheten, om systemet ska genomgå både samtestning och bedömning av informationssäkerheten. En systemblankett enligt föreskrift 5/2024 ska lämnas in till FPA i samband med ansökan om samtestning. Efter godkänd samtestning ger FPA ett samtestningsutlåtande.

Om systemet hör till klass A1 inleder producenten av informationssystemtjänsten certifieringsprocessen genom att kontakta bedömningsorganet för informationssäkerhet och komma överens om hur bedömningen av informationssäkerheten ska genomföras. Även för system i klass A2 och A3 görs en bedömning av informationssäkerheten.

Motsvarande förfaranden gäller även välbefinnandeapplikationer i anslutning till Kanta-tjänsterna.

Bedömningar av informationssäkerheten kan göras av sådana bedömningsorgan för informationssäkerhet som har fått Traficoms godkännande att utföra bedömningar av informationssäkerheten som grundar sig på lagen om kunduppgifter. Godkända bedömningsorgan offentliggörs på Traficoms webbplats. En systemblankett enligt föreskrift 5/2024 ska lämnas in till bedömningsorganet i samband med ansökan om bedömning av informationssäkerhet.

Om informationssystemet eller välbefinnandeapplikationen ska genomgå både samtestning och bedömning av informationssäkerheten, bör man sträva efter att informationssäkerhetsintyget utfärdas för samma systemversion som samtestningsutlåtandet. Ett informationssystem, ett delsystem eller en välbefinnandeapplikation som hör till klass A och som godkänts vid bedömningen av informationssäkerhet får ett informationssäkerhetsintyg. En pågående samtestning är inte ett hinder för att utfärda ett informationssäkerhetsintyg, men endast sådana krav och profiler vars krav har samtestats med godkänt resultat ska anmälas till Valviras register över informationssystem.

Lagen om kunduppgifter förutsätter inga regelbundna uppföljande auditeringar av informationssäkerheten, men producenten av en informationssystemtjänst och bedömningsorganet kan avtala om uppföljande auditeringar. THL rekommenderar uppföljande auditeringar av system i klass A3 och system med hög risknivå. Under dessa går man årligen igenom viktiga ändringar och risker i informationssystemet och dess tekniska driftsmiljö (inklusive plattformstjänster och operativsystem) som eventuellt påverkar uppfyllandet av informationssäkerhetskraven, eventuella ändringar och uppdateringar av väsentliga krav samt det eventuella behovet av en ändringsanmälan. Eventuella uppföljande auditeringar som en del av certifieringen krävs inte enligt lagen om kunduppgifter eller denna föreskrift. Vid eventuella uppföljande auditeringar ska man dock beakta avgränsningarna enligt föreskrift 4/2024 och praxis för ändringsanmälningar enligt bilaga 2. I Valviras register över informationssystem görs inga anteckningar om uppföljande auditeringar. Om en uppföljande auditering emellertid leder till en bedömning som ger upphov till ett nytt informationssäkerhetsintyg, ska uppgifterna också uppdateras i Valviras register över informationssystem.

Det krävs ingen extern testning, verifiering eller bedömning av informationssäkerheten för andra krav än de nationellt specificerade kraven enligt THL:s föreskrifter. Om man till exempel vid en bedömning av informationssäkerheten också verifierar andra krav än informationssäkerhetskraven enligt föreskrift 5/2024, ska resultaten av dessa verifieringar tydligt särskiljas från resultaten av bedömningen som genomförs enligt föreskriften.

En godkänd certifiering följs alltid av att systemet anmäls eller att uppgifterna om systemet uppdateras i Valviras register över informationssystem.

De organisationer som tar i bruk ett informationssystem och ansluter sig till Kanta-tjänsterna ingår nödvändiga avtal för att använda Kanta-tjänsterna, utför ett ibruktagningsprov och vidtar andra åtgärder som behövs för att ta systemet i bruk i samarbete med producenten av informationssystemtjänsten. Ibruktagandet är inte en del av certifieringen, men certifiering är en förutsättning för ibruktagande.

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska i enlighet med 80 § i lagen om kunduppgifter göra en anmälan till Valvira om versionsstödet för ett system som är avsett att användas för produktion av tjänster upphör. Detta gäller även situationer där systemet eller applikationen tas ur bruk för produktion av tjänster. Dessa åtgärder är inte en del av certifieringen.

6 Preciseringar av tillämpningen och ikraftträdandet av väsentliga krav

6.1 Tidpunkter att beakta avseende ikraftträdandet av kraven

Avseende ikraftträdandet och verifieringen av kraven i föreskrifterna är följande datum viktiga:

1. *Datumet då föreskriften träder i kraft*. Från och med detta datum tillämpas föreskriften och dess bilagor.
2. *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 överensstämmelse med kraven eller förfarandena för certifieringsprocesser som pågår när föreskriften träder i kraft.
3. *Datumet då profilen träder i kraft vid certifiering och anmälningar*, som anges i bilagan till föreskriften. Datumet styr bland annat de krav som verifieras vid olika tidpunkter i certifieringen – se föreskrift 5/2024, kapitel 12.
4. *Datumet som visas för ett enskilt krav i profilen* och som gäller tidpunkten då ett krav enligt bestämmelserna träder i kraft i system som används för produktion av tjänster – se föreskrift 5/2024, kapitel 12.

Ovannämnda datum har beröringspunkter med tidpunkterna då olika bestämmelser och specifikationsdokument träder i kraft. De datum som anges i övergångsbestämmelserna för lagen om kunduppgifter styr exempelvis tidsfristerna för olika krav på datainnehåll och funktioner i fråga om när de olika kraven måste uppfyllas i informationssystem som används för produktion av tjänster. Dessa tidsfrister motsvarar de kravspecifika ikraftträdandetiderna för väsentliga krav (punkt 4 ovan).

Tiden när ett visst krav träder i kraft kan skilja sig åt mellan olika profiler, på grund av att de nationella kraven på system avsedda för olika användningsändamål delvis kan ändras oberoende av kraven på system avsedda för andra användningsändamål. Till exempel kan de tidigare kraven på ”bassystem” senare krävas även av mer specialiserade system eller så kan krav på bilddiagnostik vid en senare tidpunkt krävas av system som uppfyller kraven för specialitetsspecifika profiler. Krav som anges vara giltiga ingår i bedömningen av informationssäkerheten eller i samtestningen av ett system i enlighet med profilen.

6.2 Riskbaserad inriktning av krav och verifieringssätt

Det viktigt att beakta vilken typ av risker som riktas mot systemet och riskernas omfattning, i synnerhet när det gäller informationssäkerhetskraven och dataskyddskraven. Både producenten av en informationssystemtjänst och den organisation som använder informationssystemet ska identifiera de mest centrala riskerna i samband med användningen av systemen och försöka förbereda sig på dem. Detsamma gäller tillverkare av välbefinnandeapplikationer, oberoende av om applikationen ska tillhandahållas medborgarna direkt eller om den ska användas inom ramen för tjänstetillhandahållarnas verksamhet.

Ett systems eller en applikations *risknivå* påverkar klassificeringen av systemet, kraven på systemet och verifieringen av kraven. Systemets användningsändamål är den viktigaste faktorn som avgör risknivån. Kraven genomförs och bedöms i förhållande till de uppgifter som behandlas via systemet och de funktioner som systemet erbjuder. Risknivån påverkas dessutom av hur systemet implementeras, i vilken omfattning systemet används eller avses att användas, hur omfattande behandlingen av klientuppgifter är, hur sensitiva och innehållsmässigt omfattande uppgifterna som behandlas är samt vilka beroenden relaterade till arkitekturen och avtalen som finns mellan olika delsystem eller mellan systemet och de plattformar som systemet använder.

Som en del av föreskrifterna 4/2024 och 5/2024 och som grund för klassificeringen och verifieringen av system föreslås enhetliga grunder för fastställandet av systemens och applikationernas klasser (A1, A2, A3, B) och av den risknivå som ska användas vid riktandet av kraven och verifieringen. Grunderna för klassificeringen beskrivs i föreskrift 4/2024 och dess bilaga 1. När risknivån fastställs är det *inte* fråga om en detaljerad riskbedömning som görs

situationsspecifikt i tjänstetillhandahållarnas egen verksamhet. En sådan riskbedömning beror förutom på systemet alltid också på verksamheten i den organisation som använder systemet och de omständigheter som ska beaktas i driftsmiljön samt på hur sannolikt det är att olika risker inträffar vid tidpunkten för bedömningen.

De mest centrala systemen som används i kritiska social- och hälsovårdstjänster (*kritiska system i klass A3*) omfattas av särskilda beredskapskrav för undantagstillstånd.

System som hör till klass A3 och en del av systemen i klass A2 eller A1 hör till system med *hög risknivå*. De omfattas av fler krav och mer detaljerade verifieringsmetoder än system på *basnivå*. Risknivån (hög/basnivå) kan bedömas utifrån de ovan beskrivna faktorerna som påverkar risken. Särskilt klasserna A1 och A2 kan beroende på systemets risknivå innehålla olika krav eller kravverifiering på olika nivåer. Om systemet inte ska anslutas till Kanta-tjänsterna kan omfattningen av användningen av kunduppgifter som sker via systemet och systemets risknivå vara avgörande för huruvida systemet hör till klass B eller klass A1.

Som stöd för att fastställa systemets risknivå och i vilken omfattning systemet används finns utöver materialet i föreskrift 4 även stödmaterial, till exempel verktyget för riskbedömning, som producenten av en informationssystemtjänst eller en expert som bedömer informationssystemet kan använda för att bedöma omfattningen av behandlingen av uppgifter och risknivån.

Anvisningarna och verktyget för riskbedömningar har baserats på bland annat Dataombudsmannens byrås anvisningar om riskbedömningar av dataskyddet, modellerna för riskbedömning enligt ISO-standarderna, de tidigare VAHTI-anvisningarna och VAHTI-verktygen samt kommentarer och utvecklingsförslag till utkasten till föreskrifterna.

6.3 Inriktning av krav samt certifieringsskyldigheter i modulära systemhelheter

Eftersom produktionen av olika tjänster är förenad med olika behov, måste de väsentliga kraven inriktas på ett ändamålsenligt sätt med tanke på informationssystemens användningsändamål. Man måste också kunna utnyttja olika sätt att skaffa och utveckla informationssystem. Det är möjligt att uppfylla kraven via informationssystemhelheter som sammanställts på olika sätt. Exempelvis i modulära systemhelheter ställs det olika krav på helhetens olika delar. Ett funktions- och profilbaserat tillvägagångssätt stöder inriktningen av kraven så att kraven kan anpassas till olika tjänster och deras olika produktionssätt. Dessutom stöder ett sådant tillvägagångssätt inriktningen av kraven på systemhelheter som sammanställs på olika sätt och på deras delsystem.

Certifieringsåtgärder kan inriktas mot system som består av flera delsystem eller mot systemhelheter. Vid ansökan om samtestning och bedömning av informationssäkerheten ska man i dessa fall lämna in en tydlig beskrivning av de delsystem som ingår i helheten och parterna som ansvarar för dem. Dessutom ska användningsändamålet och de väsentliga krav som uppfylls beskrivas för varje delsystem som registreras separat. För att beskriva dessa omständigheter för varje delsystem används en systemblankett i enlighet med föreskrift 5/2024, där man enligt föreskriften också anger vilka väsentliga krav som uppfylls via andra delsystem.

Det är möjligt att integrera systemen på olika sätt, till exempel genom att överföra information via gränssnitt mellan systemen eller genom att starta ett annat system. Informationssystem eller informationssystemtjänster som är kopplade till varandra kan höra till olika klasser och risknivåer. Varje informationssystem ska klassificeras och vid behov certifieras med beaktande av systemets uttryckliga användningsändamål. Om ett system används för att starta ett annat system, är egenskaperna hos det system som ska startas som utgångspunkt inte det startande systemets ansvar. Klassificeringen och certifieringen av system och delsystem som är kopplade till varandra behandlas också närmare i kapitel 7.1 i föreskrift 4/2024 och i bilaga 1 till föreskrift 4/2024.

I tilläggsuppgifterna och profilerna för de väsentliga kraven i föreskrift 5/2024 nämns separat för flera krav om kravet är sådant att det är nödvändigt att implementera i *något system* i tjänstetillhandahållarens verksamhet, men det är inte nödvändigt att implementera det till exempel i alla system som används av en viss tjänstetillhandahållare.

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska i samband med ansökan om samtestning av en större systemhelhet underrätta FPA om det för dess delsystem produceras ett separat

utlåtande om de delar av samtestningen som verifieras via delsystemet i fråga. På motsvarande sätt ska bedömningsorganet underrättas i samband med ansökan om bedömning av informationssäkerheten, om det för delsystemet produceras ett separat informationssäkerhetsintyg över de informationssäkerhetskrav som verifieras via delsystemet i fråga. I samtestningsutlåtandet eller samtestningsrapporten och i informationssäkerhetsintyget eller den tillhörande rapporten ska det specificeras med vilka andra system, delsystem eller applikationer kraven har verifierats. Om flera producenter av informationssystemtjänster, tillverkare av välbefinnandeapplikationer eller andra parter deltar i certifieringen av en systemhelhet, ansvarar var och en i regel i egenskap av producent av en informationssystemtjänst för certifieringen av sitt eget delsystem. Det är dock möjligt att avtala om de praktiska verifieringsförfarandena, deltagandet i certifieringen och ansvaret för delsystemen mellan producenterna av de informationssystemtjänster som ingår i systemhelheten.

Om ett system, ett delsystem eller en välbefinnandeapplikation som har certifierats som en del av en systemhelhet har fått ett separat godkänt utlåtande om de delar av samtestningen eller ett separat intyg över de informationssäkerhetskrav som har verifierats via delsystemet i fråga, kan systemet användas i motsvarande omfattning även tillsammans med andra system, delsystem eller applikationer än de som har certifierats i samma systemhelhet.

I certifieringen av delsystemet kan man stödja sig på krav som ska uppfyllas via andra tidigare certifierade system, delsystem eller välbefinnandeapplikationer. På detta sätt får inte andra tidigare certifierade systemen, delsystemen eller välbefinnandeapplikationerna ett nytt samtestningsutlåtande eller informationssäkerhetsintyg i samband med certifieringen av delsystemet.

Om godkännandet av en systemhelhet i något avseende är beroende av ett delsystem som godkänts i ett annat sammanhang, kan systemhelheten godkännas endast om godkännandet av delsystemet i fråga är giltigt, om egenskapen i fråga inte verifieras som en del av certifieringen av systemhelheten.

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

Definitionen av ett informationssystem utesluter inte att ett delsystem är avsett för behandling av kunduppgifter även om dessa uppgifter inte produceras eller behandlas av en yrkesutbildad person. Även i dessa situationer ansvarar producenten av informationssystemtjänsten för klassificeringen av systemet och de väsentliga kraven. Den tjänstetillhandahållare som använder systemet ansvarar också för att sådana system fungerar och för hanteringen av kunduppgifter i sin egen verksamhet.

Det är också möjligt att inkludera välbefinnandeapplikationer i systemhelheten eller så kan välbefinnandeapplikationen vara ett delsystem som ingår i ett större system. Det är också möjligt att integrera välbefinnandeapplikationer med varandra och stödja sig på krav som uppfylls via en annan applikation. Ett informationssystem kan ha egenskaper som också uppfyller definitionen av en välbefinnandeapplikation, dvs. ett informationssystem kan också vara en välbefinnandeapplikation på basis av definitionerna i lagen om kunduppgifter.

6.4 Dataskydds- och beredskapskrav på tredjepartstjänster

Både tjänstetillhandahållare och producenter av informationssystemtjänster måste beakta dataskydds- och informationssäkerhetsrisker samt beredskapsbehov i sin verksamhet. Producenten av en informationssystemtjänst ansvarar för de väsentliga kraven i anslutning till informationssystemet också i den mån som informationssystemet stöder sig på verktyg eller plattformar som produceras av en tredje part eller på ICT-tjänster som tillhandahåller delade resurser, om inte annat avtalats med den tjänstetillhandahållare som är kund hos producenten. Samma grundkrav tillämpas också i situationer där man använder kapacitetstjänster som produceras av tredje part, såsom serveruthyrning, serverhantering, backuptjänster, serverhallstjänster och molntjänster. Sådana lösningar kan även användas i välbefinnandeapplikationer.

Plattformstjänster, inklusive molntjänster som tillhandahåller delade resurser, kan produceras av andra parter än tjänstetillhandahållaren eller producenten av en informationssystemtjänst. Enligt den offentliga förvaltningens riktlinjer för molntjänster kan icke-offentlig information behandlas i en offentlig molntjänst när

informationssäkerheten och dataskyddet har implementerats och verifierats på behörigt sätt. Även det egentliga informationssystemet eller delsystemet kan genomföras till exempel som en molnbaserad SaaS-tjänst, om de väsentliga kraven kan uppfyllas och verifieras, och om risk- och beredskapsaspekterna har beaktats på en tillräcklig nivå. Producenten av en informationssystemtjänst eller tjänstetillhandahållaren kan använda molnbaserade PaaS- eller IaaS-lösningar för att genomföra systemet på ett skalbart sätt utöver eller som ett alternativ till att systemets tekniska prestationsmiljö i sin helhet administreras av producenten av informationssystemtjänsten eller tjänstetillhandahållaren. I delade miljöer kan det också vara möjligt att förbereda sig och reagera snabbt på nya hotfulla situationer och risker. I dessa lösningar ska man dock särskilt se till riskhanteringen i samband med tillgången till webbtjänster och att man genom tekniska, organisatoriska och avtalsmässiga skyddsåtgärder med beaktande av uppgifternas känslighet säkerställer att obehöriga inte kommer åt de kunduppgifter som överförs eller förvaras. Dessa aspekter ska också beaktas i fråga om välbefinnandeapplikationer som förlitar sig på externa plattformstjänster.

Många av de tekniska skyddsåtgärderna genomförs via de krav på identifiering, autentisering och åtkomsthantering som ställs på informationssystemen eller välbefinnandeapplikationerna. Tekniska skyddsåtgärder för plattformstjänster från tredje part är bland annat kryptering av datakommunikation och informationslagring eller användning av slutna nätverk. Kunduppgifter som förvaras i externa tjänster ska med beaktande av uppgifternas känslighet krypteras tillräckligt starkt så att endast tjänstetillhandahållaren eller producenten av en informationssystemtjänst har de nycklar som behövs för att dekrypterade uppgifterna.

Till de organisatoriska skyddsåtgärderna hör förutom certifieringsförfaranden även bland annat informationssäkerhetsplaner för tjänstetillhandahållare och mellanhänder samt användarutbildning i dataskydds- och informationssäkerhetsfrågor. Avtalsmässigt ska man se till att alla aktörer som deltar i behandlingen av uppgifter och produktionen av systemtjänster agerar tillräckligt enhetligt för att skydda kunduppgifter.

Medborgarnas möjligheter att få information om sin hälsa eller hälsotjänster även utomlands och aktörernas möjlighet till gränsöverskridande samarbete är exempel på gränsöverskridande behandling av uppgifter. Principen om det fria flödet av uppgifter i EU och EES tillåter att uppgifter som hör till särskilda kategorier av personuppgifter enligt EU:s allmänna dataskyddsförordning behandlas med skyddsåtgärder på samma nivå såväl i Finland som i övriga EU- och EES-länder. Överföring av uppgifter till tredjeländer och behandling av uppgifter i tredjeländer är möjlig om behandlingen av personuppgifter är tillåten i dessa situationer och om man kan iaktta överföringsgrunderna på EU-nivå, en tillräckligt noggrann fall- och landspecifik bedömning av dataskyddsnivån samt nödvändiga kompletterande skyddsåtgärder. Till exempel kan standardiserade bestämmelser som godkänts av EU-kommissionen och godkända uppförandekoder utgöra en överföringsgrund. Med beaktande av omständigheterna i enskilda fall, lagstiftningen i tredjeland och den överföringsgrund som används kan kompletterande tekniska, organisatoriska och avtalsbaserade skyddsåtgärder krävas. Om uppgifter överförs till ett tredjeland på överföringsgrunden att kommissionen har fattat beslut om att skyddsnivån i det aktuella landet är adekvat (kommissionens likvärdighetsbeslut), kan uppgifterna i stället överföras som till landet i fråga utan ytterligare krav eller tillstånd. Minimering av de uppgifter som behandlas samt anonymisering eller pseudonymisering av uppgifterna i delsystem som utför beräkningar och slutledningar minskar också dataskyddsriskerna.

En del av de väsentliga kraven är också kopplade till beredskapsbehoven vid omfattande kris- eller störningssituationer, till exempel väsentliga krav på beredskap inför att viktiga datakommunikationsförbindelser bryts i särskilt kritiska system. Beredskap för andra typer av risker kan också skapas genom en geografisk decentralisering av systemen genom molnlösningar. Social- och hälsovårdsaktörerna och producenterna av informationssystemtjänster kan utnyttja samma eller motsvarande beredskaps- och informationssäkerhetslösningar även i andra system än de nationellt mest kritiska systemen.

6.5 Krav på välbefinnandeapplikationer och ärendetjänster samt deras förhållande till informationssystemen

Enligt lagen om kunduppgifter är ett informationssystem ett system avsett för elektronisk behandling av kunduppgifter eller för registrering och uppdatering av kundhandlingar. Om systemet har planerats för behandling

av kunduppgifter som omfattas av registerföringen hos en tjänstetillhandahållare inom social- och hälsovården samt för behandling av uppgifter i kundhandlingar, uppfyller systemet definitionen av ett informationssystem. Det är exempelvis inte avgörande om informationssystemet tillhandahåller användargränssnitt både för yrkesutbildade personer och för allmänheten. I många informationssystem finns funktioner som kunderna kan använda för att få uppgifter om sig själva eller lämna uppgifter till tjänstetillhandahållarens personal, serviceprocesser och handlingar eller som grund för dem. En elektronisk ärendetjänst som en tjänstetillhandahållare tillhandahåller sina personkunder och som behandlar klientuppgifter som omfattas av tjänstetillhandahållarens registerföring och som överförs till eller härrör från klient- eller journalhandlingar är ett informationssystem enligt definitionen i lagen om kunduppgifter.

Enligt lagen om kunduppgifter är en välbefinnandeapplikation en applikation i anslutning till datalagret för egna uppgifter som behandlar uppgifter om välbefinnande eller en applikation till vilken en medborgare kan få sina kunduppgifter från informationsresursen för kunduppgifter, receptcentret och informationshanteringstjänsten inom Kanta-tjänsterna. Välfärdsapplikationer kan produceras och användas både i samband med och självständigt från de tjänster som tillhandahålls av tjänstetillhandahållare inom social- och hälsovården. Uppgifter som sparats i datalagret för egna uppgifter med välbefinnandeapplikationer får användas i tjänstetillhandahållarens verksamhet i enlighet med övergångsbestämmelserna i lagen om kunduppgifter. I en välbefinnandeapplikation (eller i ett informationssystem där välbefinnandeapplikationen ingår som ett delsystem) är det möjligt att även föra register över personuppgifter på annat sätt än via Kanta-tjänsterna. Tillverkaren av välbefinnandeapplikationen eller dennes kundorganisation, såsom en tjänstetillhandahållare inom social- och hälsovården, kan ansvara för registerföringen av dessa uppgifter. Samtidigt är det möjligt att skapa mycket begränsade välbefinnandeapplikationer som nästan helt förlitar sig på till exempel datalagret för egna uppgifter.

En digital tjänst som en tjänstetillhandahållare tillhandahåller sina kunder kan alltså enligt definitionerna i lagen om kunduppgifter vara ett informationssystem, en välbefinnandeapplikation eller både och. I föreskrifterna 4/2024 och 5/2024 används termen digital tjänst med hänvisning till de välbefinnandeapplikationer som medborgare använder och de informationssystem som både yrkesutbildade personer och medborgare använder.

Certifieringskraven för välbefinnandeapplikationer skiljer sig delvis från dem för informationssystem. Orsaken till detta är att den rättsliga grunden, användargruppen, typen av uppgifter som behandlas och uppgifternas innehåll, riskerna, Kanta-anslutningslösningarna samt ansvaret för egenkontroll och tillsynen för välbefinnandeapplikationer kan vara mycket olika jämfört med för informationssystem. De väsentliga krav och förfaranden för informationssystem och välbefinnandeapplikationer som tidigare fastställts i separata föreskrifter har slagits samman i föreskrifterna 4/2024 och 5/2024. Orsaken till detta är att a) många av kraven och förfarandena är desamma både för informationssystemen och välfärdsapplikationerna, b) i praktiska digitala tjänstelösningar i anslutning till Kanta-tjänsterna och tjänster som riktar sig till medborgarna på annat sätt är det viktigt att uppfylla samma grundläggande krav, c) det är inte ändamålsenligt med dubbel verifiering av samma eller nästan identiska krav i fråga om informationssystemlösningar vars delsystem även kan uppfylla definitionen av en välbefinnandeapplikation, d) i informationssystem, ärendetjänster och välbefinnandeapplikationer som används både av yrkesutbildade personer och av medborgare används allt oftare samma uppgifter, e) medborgarna eller de apparater och applikationer de använder kan i större utsträckning än tidigare producera information som även kan utnyttjas av yrkesutbildade personer och av tjänstetillhandahållare, f) hanteringen av dataskydds- och informationssäkerhetsrisker måste planeras på ett helhetsmässigt sätt, med hänsyn till både yrkesutbildade personer och medborgare samt till nya användningssätt såsom mobilapplikationer och onlinetjänster.

Förfarandena och kraven för välbefinnandeapplikationer i anslutning till datalagret för egna uppgifter, som tidigare fastställdes i den separata föreskriften 6/2021, har integrerats med kraven och förfarandena för informationssystem i föreskrifterna 4/2024 och 5/2024. Samtestningen och bedömningen av informationssäkerheten utförs för både informationssystem och välbefinnandeapplikationer i enlighet med dessa föreskrifter. Specifikationer för informationssystem som används av tjänstetillhandahållare och yrkesutbildade personer i fråga om användning av uppgifter om välbefinnande som producerats via välbefinnandeapplikationer är under beredning och väsentliga krav i anslutning till detta ingår i föreskrifterna.

När man planerar, genomför och bedömer lösningar för ärendetjänster och välbefinnandeapplikationer måste man ta hänsyn till att lösningen används av medborgare och individer snarare än av yrkesutbildade personer. Skillnaden är betydande till exempel i planeringen av användargränssnitt, identifieringslösningar och krav som gäller produktionen av kunduppgifter. Flera av de krav som fastställts för system som används av yrkesutbildade personer kan inte direkt tillämpas på ärendetjänster eller välbefinnandeapplikationer som innehåller användargränssnitt för medborgarna. Utöver kraven på välbefinnandeapplikationer har man fastställt nationella krav på tjänstetillhandahållares ärendetjänster som riktar sig till kunder. Kraven på välbefinnandeapplikationer och andra digitala tjänster samt krav som gäller användningen av uppgifter om välbefinnande i datalagret för egna uppgifter har sammanfattats i de väsentliga kraven i föreskrift 5/2024 i avsnittet ”Digit. Palvelujen vaatimukset” (krav på digitala tjänster). Avsnittet innehåller funktionella krav, krav som ska gås igenom vid samtestning samt krav som ska gås igenom vid bedömningen av informationssäkerhet. Datainnehållet i datalagret för egna uppgifter ingår också i kraven på datainnehåll i föreskrift 5/2024.

Många av kraven som särskilt gäller välbefinnandeapplikationer gås igenom vid certifieringen av välbefinnandeapplikationer. Kraven på de ärendetjänster som ingår i informationssystem är en del av certifieringen av informationssystemet i fråga, eftersom ärendetjänsterna också medför nya typer av informationssäkerhets- och dataskyddsrisker i anslutning till hanteringen av kunduppgifter.

I informationssystemprofilerna i bilaga 3h till föreskrift 5/2024 har man samlat många krav för användning av uppgifter om välbefinnande och krav på digitala tjänster (både ärendetjänster och välbefinnandeapplikationer). Profilerna innehåller krav för följande användningsändamål (se även bild 3):

- En tjänstetillhandahållares ärendetjänst (informationssystem som även innehåller gränssnitt/kanaler avsedda för kunder) (3h1) förutsatt att det inte är en välbefinnandeapplikation.
- En välbefinnandeapplikation som producerar uppgifter i datalagret för egna uppgifter (3h2).
- En välbefinnandeapplikation som använder uppgifter i datalagret för egna uppgifter (3h3).
- En välbefinnandeapplikation med vilken kunden kan få sina kunduppgifter från datalagret för egna uppgifter, receptcentret eller informationshanteringstjänsten inom Kanta-tjänsterna (3h4).
- Ett informationssystem med vars hjälp tjänstetillhandahållare och yrkesutbildade personer kan använda uppgifter om välbefinnande som finns i datalagret för egna uppgifter (3h5).

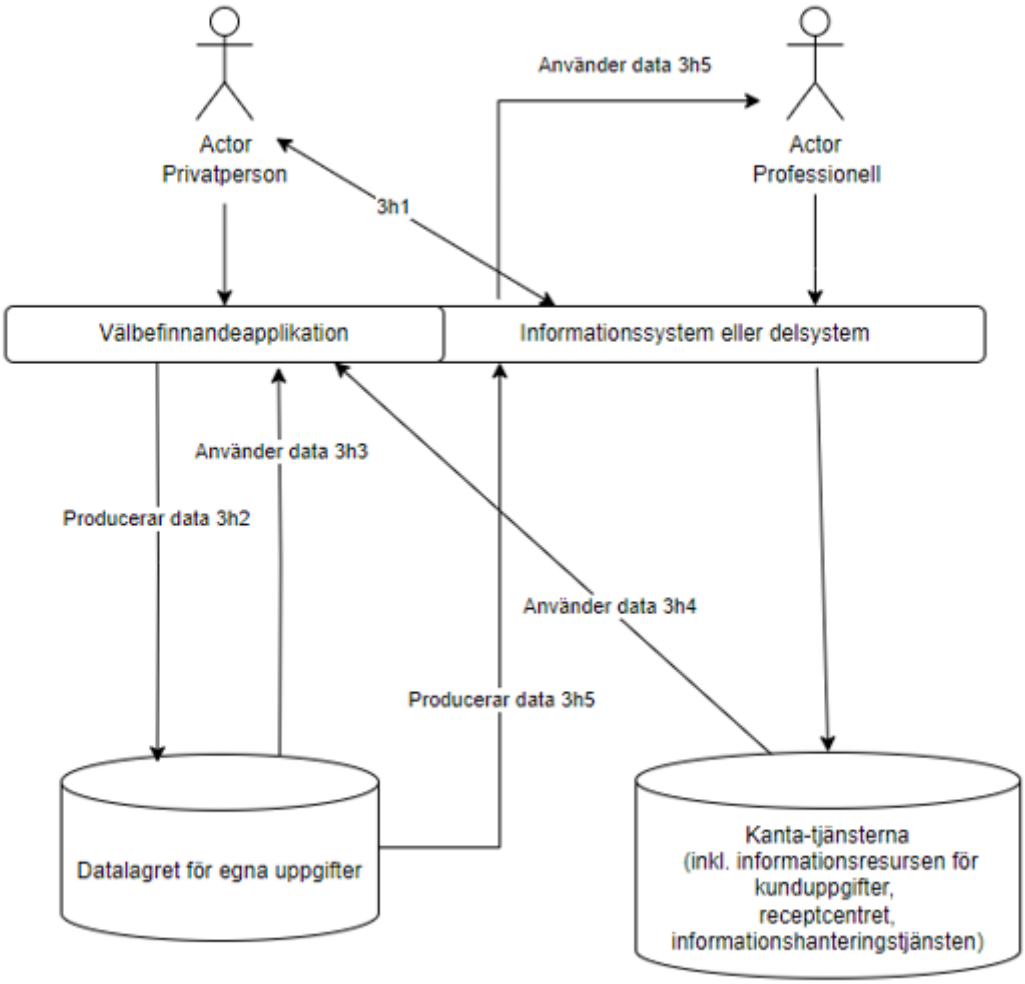

Bild 3. Förhållandet mellan profilerna i bilaga 3h till föreskrift 5/2024 och användare, datasystem, välbefinnandeapplikationer och Kanta-datalager.

Ett informationssystem eller en välbefinnandeapplikation kan uppfylla kraven i flera profiler, även när det gäller de krav som beskrivs i bilaga 3h. Till exempel kan ett omfattande klient- och patientdatasystem (som uppfyller till exempel profilerna 3a1 för receptförskrivning, 3c1 för behandling av patientjournaluppgifter och 3d1 för behandling av klientuppgifter inom socialvården) också innehålla ärendetjänster (3h1) och uppgifter om välbefinnande som är sökbara för yrkesutbildade personer (3h5), eller så kan till exempel en välbefinnandeapplikation enligt profilerna 3h2 och 3h3 vara integrerad i systemet som ett delsystem, som en del av en portal för kunder eller som mindre mobilapplikationer.

6.6 Hantering av recept samt apotekens informationssystem och webbtjänster

Handlingar som upprättats för expediering av läkemedel, dvs. recept, är kundhandlingar enligt lagen om kunduppgifter 703/2023. Bestämmelserna i lagen om kunduppgifter om informationssystem, organisationers databehandlingsprinciper och informationssäkerhetsplanen har gällt apoteken och deras informationssystem redan under den tid då den tidigare lagen om kunduppgiften var i kraft. Apotekssystem har redan enligt tidigare föreskrifter varit informationssystem i klass A3 som ska certifieras. Ändringen av definitionen av ett recept till en journalhandling

har inte väsentligt förändrat hur eller i vilken utsträckning apoteken redan hanterar recept. Apotekens rätt att hantera recept och kraven på apotekssystem är oförändrade i lag 703/2023.

I regeringens proposition i anslutning till lagen om kunduppgifter 703/2023 fastställs att de informationssystem som används vid expedieringen av recept omfattas av definitionen av informationssystem, men inte de övriga informationssystem som apoteken använder. De krav som gäller apotekssystem för expediering av recept på apotek har sammanställts i profil 3a2 i bilaga 3 till föreskrift 5/2024. Föreskrifterna 4/2024 och 5/2024 gäller apotek och producenter av informationssystemtjänster som erbjuder apotekssystem endast i fråga om dessa informationssystem.

Apotekens webbtjänster regleras av läkemedelslagen (395/1987), läkemedelsförordningen (693/1987) och Fimeas föreskrift 2/2011 om apotekens webbtjänster. Bestämmelserna om välbefinnandeapplikationer i lagen om kunduppgifter innehåller till exempel inga andra bestämmelser som apotekens webbtjänster förutsätter. Den nuvarande lagstiftningen möjliggör inte att uppgifter om recept och läkemedelsersättningar överförs och sammanställs så att de är tillgängliga för kunden i apotekets webbtjänst. I regeringens proposition i anslutning till lagen om kunduppgifter (RP 246/2022 rd) konstateras att nätapotek inte kan inrättas enbart med stöd av lagen om kunduppgifter. I apotekens webbtjänster behandlas uppgifter som hör till apotekets person- och kundregister. Behandlingen av dessa uppgifter utgör inte behandling av kunduppgifter inom social- och hälsovården. Apotekens webbtjänster är således inte sådana informationssystem eller välbefinnandeapplikationer som avses i lagen om kunduppgifter. Skyldigheterna i lagen om kunduppgifter och föreskrifterna 4/2024 och 5/2024 om klassificering, certifiering, väsentliga krav och registrering i anslutning till informationssystem och välbefinnandeapplikationer gäller inte apotekens webbtjänster. Det rekommenderas dock att man i utvecklingen av apotekens webbtjänster där så är tillämpligt beaktar de krav som ställs på digitala tjänster som används inom social- och hälsovårdstjänsterna (till exempel kraven enligt profil 3h1 i föreskrift 5/2024).

Receptuppgifterna hör till det gemensamma registret för Folkpensionsanstalten och apoteken samt för tjänstetillhandahållare och självständiga läkemedelsförskrivare (18 § i lagen om elektroniska recept). Användningen av uppgifter mellan de personuppgiftsansvariga för det gemensamma registret mellan dessa aktörer utgör inte utlämnande av kunduppgifter, så receptuppgifterna gäller inte till exempel bestämmelser om kunduppgifter i anslutning till anmälningar om utlämnande av uppgifter.

7 Mer information om beredningen av föreskrifterna 4/2024 och 5/2024

Innehållet i föreskrifterna 4/2024 och 5/2024 grundar sig i huvudsak på tidigare föreskrifter som utfärdades 2015, 2016 och 2021. Utifrån dessa har man i Valviras register över informationssystem registrerat över 60 certifierade system eller välbefinnandeapplikationer som hör till klass A och över 320 system som hör till klass B. Största delen av kraven är desamma som i tidigare föreskrifter. Tidpunkten för ikraftträdandet av de nya kraven (till exempel i profilerna i föreskrift 5/2024) har fastställts med hänsyn till de tidsfrister som föreskrivs i lagstiftningen, utvecklings- och certifieringscyklerna för systemen samt synpunkterna från remissbehandlingen av föreskrifterna.

Vid beredningen av föreskrifterna 4/2024 och 5/2024 jämte bilagor har man utöver de ändrings- och kompletteringsbehov som lagen medför även beaktat erfarenheterna från de föreskrifter som utfärdats med stöd av lagen om kunduppgifter, som trädde i kraft 2021, och behoven av att precisera dem. Dessutom har man beaktat ett antal behov som tjänstetillhandahållare inom social- och hälsovården, producenter av informationssystemtjänster samt nationella myndigheter har haft i anknytning till de nationella specifikationerna och Kanta-tjänsterna I samband med beredningen av föreskriften, förteckningen och profilerna ordnade man en omfattande remissrunda och presenterade ämnet i flera olika samarbetsgrupper och vid olika evenemang. Utifrån de över 300 kommentarer som inkom under remissrundan har preciseringar, kompletteringar och korrigeringar gjorts i föreskrifterna 4/2024 och 5/2024 jämte bilagor samt i de krav som de innehåller.

I de första versionerna av föreskrifterna om väsentliga krav från 2015–2016 betonades i synnerhet de krav som uppstår via Kanta-tjänsterna. I lagen om kunduppgifter 784/2021 och föreskrifterna som följer den utvidgades kraven bland annat utifrån riksdagens och de styrande myndigheternas ställningstaganden till att i större utsträckning än

tidigare gälla även informationssystem som hör till klass B samt andra informationssystem än sådana som ska anslutas till Kanta-tjänsterna, och de förfaranden och verifieringssätt som används för att verifiera kraven skärptes.

De viktigaste ändringarna och kompletteringarna i 2024 års föreskrifter är följande:

- Den separata föreskriften om välbefinnandeapplikationer har integrerats i en större helhet som omfattar väsentliga krav och certifiering.
- Kraven på digitala tjänster och ärendetjänster riktade till medborgare har tagits med tydligare som en separat del av helheten av väsentliga krav.
- Kopplingarna mellan FPA:s samtestningshelheter och de väsentliga kraven har preciserats.
- Verkställandet av de nationella kraven och tidsfristerna för harmonisering av logguppgifter och hanteringen av användningsloggar har inkluderats i de väsentliga kraven (ingen separat föreskrift).
- Föreskrifternas förhållande till apotekens informationssystem och webbtjänster har förtydligats.
- Direkta källor som stöder implementeringen av informationssäkerhetskraven finns med i förteckningen över väsentliga krav,
- Förhållandet mellan resultaten av informationssäkerhetsbedömningen och samtestningen samt registreringen av informationssystemen har preciserats.
- Informationssäkerhets- och dataskyddskravens källor och länkar till internationella standarder har förtydligats.

I 2024 års bestämmelser har innehållet i flera, tidigare separata anvisningar sammanställts och komprimerats, föråldrade källor i anslutning till kraven har tagits bort och uppdaterade källor har lagts till (författningar, specifikationer, standarder och källor som ger bakgrund till de olika kraven).

THL uppdaterar innehållet i föreskrifterna 4/2024 och 5/2024 samt de väsentliga kraven och profilerna vid behov via de nya föreskrifterna, baserat på nya specifikationsdokument, erfarenheter från certifieringsprocessen och utvecklingsförslag från olika intressentgrupper.