Informationstjänster
Social- och hälsovårdsinformation och informationshantering 9.12.2021

ANVISNINGAR OM TILLÄMPNINGEN AV VÄSENTLIGA KRAV

Innehåll

1 Mål

Enligt 34 § i lagen om kunduppgifter ska ett informationssystem som används för behandling av kunduppgifter inom social- och hälsovården uppfylla väsentliga krav på

- funktionalitet
- interoperabilitet
- informationssäkerhet och dataskydd.

Genom THL:s föreskrifter 4/2021 Föreskrift om klassificering och certifiering av informationssystem för social- och hälsovården och 5/2021 Föreskrift om väsentliga krav på funktionalitet och informationssäkerhetskrav hos informationssystem för social- och hälsovården, sammanställs förfaranden och nationellt fastställda krav för informationssystem avsedda för behandling av klientuppgifter inom social- och hälsovården. Mål och användningsområden beskrivs närmare i kapitel 2 i föreskrift 5/2021.

Beskrivningen av de väsentliga kraven på informationssystem är en del av de lagstadgade skyldigheterna som gäller informationssystem för social- och hälsovården. Med hjälp av skyldigheterna försöker man se till att informationssystemen fungerar och att både kundernas och social- och hälsovårdspersonalens rättsskydd tillgodoses. De väsentliga kraven är ett sätt att styra utvecklingen av informationssystemen på nationell nivå och säkerställa deras informationssäkerhet. Kraven på funktionalitet utgör också grunden för de väsentliga kraven på interoperabilitet och informationssäkerhet. En enhetlig beskrivning och avgränsning av systemens användningsändamål genom väsentliga krav förtydligar kommunikationen om de olika systemens användningsändamål och om vilka nationella krav systemen uppfyller. För att säkerställa informationssäkerhetens grundläggande mål, såsom konfidentialitet, integritet, tillgänglighet och oavvislighet, ställs både specificerade och allmänna krav på systemen och producenterna av informationssystemtjänster.

Genom de krav som ställs på informationssystem för social- och hälsovården förenhetligas sådana omständigheter 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. Detta gör att man kan lita på att systemen har tillräckliga och nödvändiga egenskaper till exempel med tanke på anslutningen till Kanta-tjänsterna och informationssäkerheten när man anskaffar dem och utvecklar dem för olika tjänster. Konkurrensen mellan system och produkter kan bland annat gälla användbarhet och egenskaper som tillför användaren ett särskilt mervärde. Sammanställningen av de väsentliga kraven till en enhetlig klassificering förenhetligar begreppen som används i krav som grundar sig på författningar och nationella specifikationer och förenhetligar kraven på systemtillverkare och deras användare.

2 Översikt över användningen av väsentliga krav

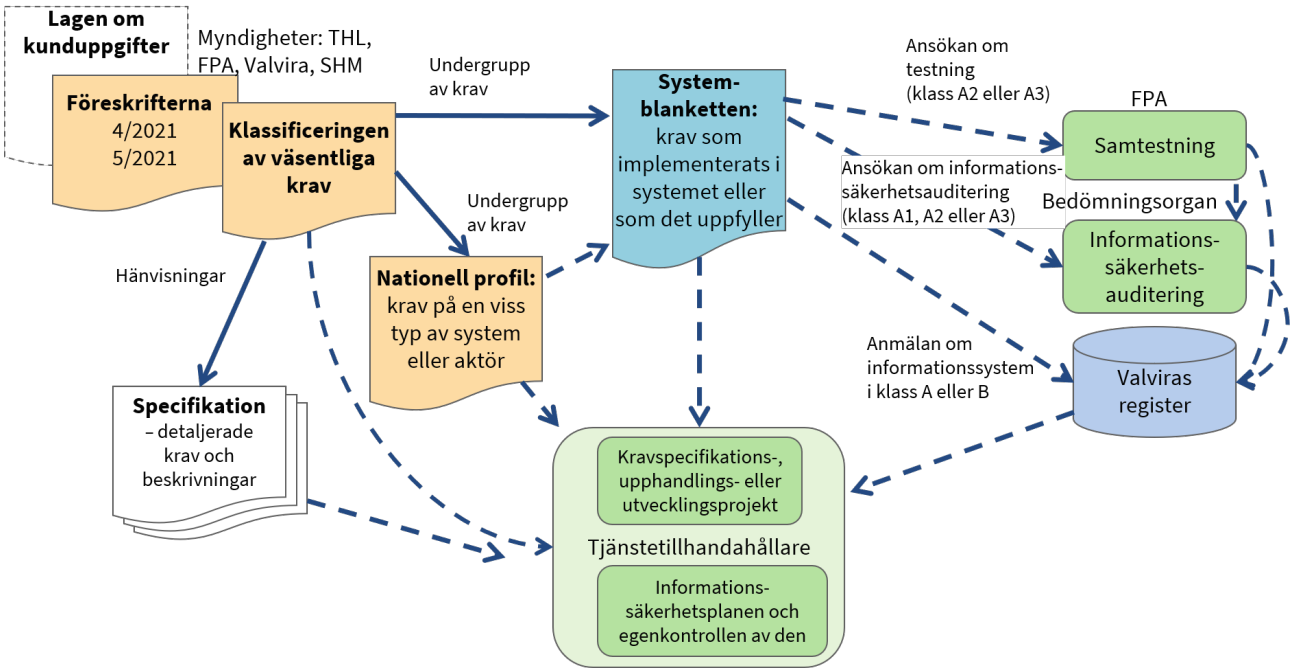
Producenten av en informationssystemtjänst ansvarar för beskrivningen av informationssystemets användningsändamål, klassificeringen av informationssystemet, beaktandet av väsentliga krav i planeringen och genomförandet av informationssystemet samt certifieringen och registreringen av informationssystemet. 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.

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 de anvisningarna från producenten av informationssystemtjänsten.

Tjänstetillhandahållare ska för sin del säkerställa att det informationssystemet 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 klassificeringen av dem används. Centrala material som anknyter till helheten är föreskrifterna, klassificeringen av väsentliga krav, systemblanketten och profilerna.

Genom föreskrifterna 4/2021 och 5/2021 utfärdas anvisningar om hur de väsentliga kraven ska beskrivas och verifieras samt hur de lagstadgade redogörelserna och anmälningarna i anslutning till dem ska ges. Föreskrifterna baseras på lagen om kunduppgifter.



Figur 1. Helheten av väsentliga krav.

2.1 Klassificering av väsentliga krav

Klassificering av väsentliga krav (Föreskrift 5/2021, bilaga 2) är en tabell som sammanställer följande nationella specifikationer för system som behandlar klient- och patientuppgifter:

- funktionalitet/funktioner (fliken Funktioner)
- datainnehåll (fliken Datainnehåll)
- informationssäkerhetskrav (fliken Informationssäkerhetskrav).

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 klassificeringen av väsentliga krav. Varje kravrad har en eller flera källhänvisningar och via länkarna på fliken Källhänvisningar kan man granska 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 noggrant på FPA:s och THL:s webbplatser[1] samt i publikationskanalerna för olika datainnehåll, såsom THL:s och FPA:s kodtjänst samt tjänsten Sosmeta. De specifikationsdokument som det hänvisas till innehåller närmare uppgifter om vilka egenskaper eller detaljerade uppgifter som är obligatoriska eller frivilliga i implementeringarna. Huruvida en viss funktion eller ett visst datainnehåll är obligatoriskt beror alltså inte enbart på de uppgifter som beskrivits i profilen och klassificeringen, 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 versioner godkännas.

I samband med de olika funktionerna och datainnehållen i klassificeringen redogörs också för de testpaket som hänför sig till dem och som är avsedda för samtestning av system som ska anslutas till Kantatjänsterna samt för de informationssäkerhetskrav som ska verifieras vid bedömningen av informationssäkerheten (om funktionen anknyter till något av de informationssäkerhetskrav som ska bedömas). De viktigaste specifikationerna som hänför sig till olika funktioner och datainnehåll nämns i samband med respektive funktion och innehåll och de hittas via fliken med hänvisningar till källdokument i klassificeringen. I klassificeringen beskrivs också struktureringsnivån för de specifikationer som finns tillgängliga för olika datainnehåll. Förhållandena mellan funktioner och datainnehåll beskrivs vid behov som en del av klassificeringen, till exempel i en situation där en viss funktion är förenad med krav som hänför sig till ett separat beskrivet datainnehåll eller en annan funktion.

De funktioner, datainnehåll och informationssäkerhetskrav som ingår i de väsentliga kraven har grupperats så att samma kravgrupp innehåller krav inom samma ämnesområde. Grupperingen är avsedd enbart för att sammanställa krav inom samma ämnesområde, och de egentliga systemkraven och profilerna gäller alltid specificerade krav.

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

2.2 Minimikravprofiler

Klassificeringen av väsentliga krav ligger också till grund för *profilerna*. En profil sammanställer de nationella minimikraven för behandling av klient- eller patientuppgifter för informationssystem som är avsedda för ett visst användningsändamål. En profil innehåller alltså en delgrupp av de funktioner, datainnehåll och informationssäkerhetskrav som beskrivs i klassificeringen av väsentliga krav. Profiler publiceras för sådana användningsändamål där det är viktigt att harmonisera minimikraven för ett antal informationssystem.

Profiler kan publiceras separat från uppdateringen av klassificeringen av väsentliga krav, och nya minimikravprofiler kan publiceras för informationssystem avsedda för olika användningsändamål. Profilerna täcker

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

inte alla möjliga användningsändamål för system i klass A eller B. Till exempel har inga specifika profiler publicerats för alla system inom olika specialiteter.

De väsentliga kraven och profilerna fungerar som en central utgångspunkt för planeringen och genomförandet av system avsedda för behandling av patientuppgifter inom hälso- och sjukvården eller klientuppgifter inom socialvården. Uppfyllandet av minimikraven enligt profilen i bilagan till en föreskrift är en förutsättning för att ett informationssystem eller en informationssystemhelhet 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.

Profilerna finns i bilaga 3 till föreskrift 5/2021. I bilagan finns flera tabeller och varje tabell innehåller en eller flera profiler. Till exempel innehåller bilaga 3a två profiler: Patientdatasystem som behandlar recept och Apotekssystem.

Profilen innehåller sådana funktioner, datainnehåll och informationssäkerhetskrav som enligt specifikationerna ska implementeras i ett informationssystem som används för profilens användningsändamål. Till exempel innehåller profilen Apotekssystem (föreskrift 5/2021, bilaga 3a, profil 3a2) de funktioner och uppgifter som åtminstone förutsätts av de informationssystem som apoteken använder, bland annat för att söka information om recept och expediera läkemedel, samt sådana informationssäkerhetskrav som åtminstone måste uppfyllas i apoteksverksamheten.

Profilerna har sammanställts i synnerhet för informationssystem som ansluts till olika Kanta-tjänster, såsom Patientdataarkivet, Klientdataarkivet för socialvården och receptcentret. En del av profilerna, såsom profilen i bilaga 3g till föreskrift 5/2021, 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 som hör till klass A (även A1) går man igenom informationssäkerhetskraven vid bedömningen av informationssäkerheten, men kraven gäller även informationssystem som hör till klass B.

Ett system 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), flera profiler för Klientdataarkivet för socialvården (bilaga 3d), profilen för ett patientdatasystem som behandlar recept (bilaga 3a) samt profilen för en tjänst som producerar intyg eller utlåtanden i Kanta-arkivet (bilaga 3f). I systemen implementeras förutom profiler alltid även andra krav, varav en del kan ingå i de väsentliga kraven.

Profilerna beskriver också när 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 eller ”införs i samband med anslutningen” innebär det att kravet redan gäller. Då ska det system som tas i bruk enligt profilen, redan används eller som ansluts till Kanta-tjänsterna (och nya versioner av det) uppfylla kravet.

Det är inte meningen att systemets klass ska avgöras utifrån vilka profiler eller funktioner som implementeras i systemet. Till exempel kan klass A1 innehålla 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 verktyg för producenten av en informationssystemtjänst

På systemblanketten beskriver producenten av en informationssystemtjänst användningsändamålet för sitt system, de väsentliga krav som har uppfyllts i systemet samt de minimikravprofiler som systemet iakttar. Systemblanketten grundar sig på klassificeringen av väsentliga krav. På blanketten beskrivs funktionerna, datainnehållet och informationssäkerhetskraven i ett enskilt informationssystem, ett delsystem eller en informationssystemhelhet. Systemblanketten innehåller inte alla tilläggsuppgifter som ingår i klassificeringen. Mer information om kraven på systemblanketten finns i klassificeringen 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. Detta gäller för informationssystem som hör till klass B och klass A. Systemblanketten dokumenterar hur de väsentliga kraven på systemet har beaktats i planeringen, genomförandet och dokumentationen av systemet samt i planeringen av och anvisningarna om användningen av systemet. Det är viktigt att beakta systemets användningsändamål, klassificering, risknivå, väsentliga krav och profiler redan när systemet eller dess uppdateringar planeras.

Systemblanketten används när producenten av en informationssystemtjänst ansöker om FPA:s samtestning för testning av ett informationssystem 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. En del av de väsentliga kraven har länkats till testpaketen för FPA:s samtestning, där man utifrån de specifikationer som hänvisas till i de olika kraven testar interoperabiliteten mellan system som ska anslutas till Kanta-tjänsterna och Kanta-tjänsterna samt andra system som är anslutna till Kanta-tjänsterna.

Systemblanketten används också när bedömningen av informationssäkerhet av ett informationssystem 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 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. Valvira för ett offentligt register över de informationssystem för social- och hälsovården som anmälts till Valvira och kan göra uppgifterna i anmälningarna tillgängliga till exempel via sina egna webbsidor. Valviras register över informationssystem innehåller uppgifter om den anmälan som producenten av en informationssystemtjänst lämnat samt uppgifter om de samtestningar och den bedömning av informationssäkerheten som systemet genomgått.

Den lagstadgade anmälan som ska göras till Valvira gäller alla informationssystem för 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.

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

Endast de krav som har implementerats i systemet antecknas 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 använder blanketten i certifieringsprocessen eller i anmälan till Valvira:

1. Fyll i basuppgifter om systemet: systemets namn, producenten av informationssystemtjänsten, tillverkaren (kan också vara samma som producenten av informationssystemtjänsten), version.

2. Beskriv kort systemets användningsändamål: för vilket ändamål, till vilka tjänster och med vilka begränsningar systemet ska användas. Ange dessa uppgifter vid punkterna för beskrivning av användningsändamålet och användningskontext på blanketten (välj till exempel offentliga eller privata social- eller hälsovårdstjänster).

3. Beskriv systemets risknivå utifrån riskbedömningen av systemet och hur omfattande användning av kunduppgifter systemet är avsett för på de grunder som beskrivs i föreskrift 4/2021 och dess bilaga 1. Utnyttja vid behov stödmaterial såsom THL:s verktyg för riskbedömning.

4. Ange under punkten *Systemets klass* till vilken klass systemet hör (A3, A2, A1 eller B) i enlighet med föreskrift 4/2021 och dess bilaga 1.

5. Under Profiler på systemblanketten ska du ange de profiler i bilaga 3 till föreskrift 5/2021 vars användningsändamål är en del av systemets användningsändamål. Varje profils namn och beskrivning samt tilläggsuppgifter innehåller information om hur profilen tillämpas. De profiler vars användningsändamål systemet stöder ska implementeras i systemet och anges på blanketten. Det räcker med att ange profilernas koder (till exempel ”3a1, 3c1”) på systemblanketten, du behöver inte skriva profilens hela namn.

6. På fliken Funktioner i blanketten anger du de funktioner som motsvarar väsentliga krav och som har implementerats i systemet.

7. På fliken Datainnehåll i blanketten anger du det datainnehåll som motsvarar väsentliga krav och som har implementerats i systemet.

8. Ange de informationssäkerhetskrav som har implementerats i systemet eller som uppfylls via systemet.

9. 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.

10. Kontrollera själv, testa och dokumentera de väsentliga kraven som implementerats i systemet innan systemet certifieras eller registreras, både för de väsentliga krav som ingår i profilerna och för andra väsentliga krav som systemet uppfyller.

11. Kontrollera uppgifterna på blanketten och använd blanketten i situationer enligt figur 1 vid certifiering och registrering av systemet.

12. Uppdatera blanketten när ändringar görs i systemet – de krav som har ändrats jämfört med den tidigare versionen av blanketten ska anges som ändrade i de nya versionerna av blanketten.

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 5/2021. 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 finns vid behov i bilaga 2 Klassificering av väsentliga krav i föreskrift 5/2021. Närmare uppgifter är bland annat förhållandena

mellan olika krav, närmare specifikationer av kraven och informationssäkerhetskravens motsvarigheter till kraven i tidigare föreskrifter.

I punkterna 6–8 på blanketten anges både de egenskaper som implementerats i systemet utifrån profiler som motsvarar systemets användningsändamål och systemets 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 antecknas i punkterna 6–8 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 olika delsystem i en informationssystemhelhet för bilddiagnostik.

Om betydande ändringar görs i ett certifierat system ska de anmälas i enlighet med föreskrift 4/2021 och dess bilaga 2, eftersom ändringar i system som hör till klass A kan kräva en bedömning av behovet av en ny testning, en bedömning av behovet av att förnya informationssäkerhetsintyget och en uppdatering av uppgifterna om systemet i Valviras register över informationssystem. I anmälningar som gäller ändringar i systemet ska man på systemblanketten, i enlighet med blankettens anvisningar, ange de krav vars implementering eller uppfyllande har ändrats jämfört med den tidigare systemversionen och blanketten.

Systemblanketten ska på begäran också sändas till en tillhandahållare av social- och hälsovårdstjänster 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 informationssystemen inom social- och hälsovården sammanställer uppgifter om anmälda informationssystem i klass A och B samt resultaten av samtestningen och bedömningen av informationssäkerheten avseende informationssystem i klass A. Valvira publicerar de centrala uppgifterna om informationssystemen som finns i registret.

Via registret över informationssystem finns offentligt tillgängliga uppgifter om informationssystem som är avsedda för behandling av kunduppgifter inom social- och hälsovården. De offentliga uppgifterna i registret utgör en central grund bland annat för tillsynen över informationssystemen och deras överensstämmelse med kraven. Tillhandahållare av social- och hälsovårdstjänster kan utnyttja uppgifterna i Valvira register över informationssystem till exempel som stöd för upphandlingar. Genom att anmäla informationssystem till registret med hjälp av klassificering och profiler kan man till exempel göra uppgifter om godkända och certifierade system 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 att systemet uppfyller de väsentliga kraven i 34 § 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 motsvarar de som implementerats i systemet. Om systemet 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 till Valviras register över informationssystem. Oberoende av anmälan ansvarar producenten av en informationssystemtjänst 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.

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

Enligt 34 § 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 5/2021 (särskilt kapitel 9) preciserar hur dessa omständigheter säkerställs. De väsentliga kraven kan uppfyllas med en helhet som består av ett eller flera informationssystem.

Anordnaren eller producenten av social- och hälsovårdstjänster ska säkerställa att

- användningsändamålet för de informationssystem eller delsystem som den använder som helhet motsvarar organisationens verksamhet;
- uppgifter om de informationssystem i klass A och klass B som den använder finns i Valviras register;
- de system i klass A1, A2 och A3 som den använder har ett giltigt informationssäkerhetsintyg;
- 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;
- de informationssystem eller delsystem som den använder i sin helhet uppfyller kraven för de nationella minimikravprofilerna i den mån verksamhet behöver informationssystem för de användningsändamål som beskrivs i profilerna;
- 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.

Som ett praktiskt verktyg för att säkerställa dessa omständigheter ska man använda informationssäkerhetsplanen enligt föreskrift 3/2021, där man ska beskriva de informationssystem som tjänstetillhandahållaren använder för behandling av patientuppgifter eller klientuppgifter inom socialvården. Uppgifterna om de informationssystem som används och deras överensstämmelse med kraven uppdateras vid behov som en del av den regelbundna egenkontrollen av informationssäkerhetsplanen med hjälp av till exempel Valviras register över informationssystem och uppgifter från producenter av informationssystemtjänster.

En tillhandahållare av social- och hälsovårdstjänster kan också utnyttja klassificeringen av väsentliga krav och kravprofilerna, Valviras register samt systemblanketten i informationssystemens kravspecifikationer, upphandlingar och utvecklingsarbete. När man gör riskbedömningar för olika informationssystem kan man utnyttja riskbedömningsmallen och riskbedömningsverktyget som används för klassificering och certifiering av

informationssystem, även om de i första hand är avsedda att hjälpa producenter av informationssystemtjänster att fastställa risknivån i sitt eget system.

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, kan en del av kraven i upphandlingen fastställas via väsentliga krav eller profiler. I Valviras register över informationssystem kan man kontrollera vilka system som hör till olika klasser och som uppfyller olika profiler. Valviras register över informationssystem 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.

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 systemet som ska upphandlas uppfyller de nationellt fastställda minimikraven.

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

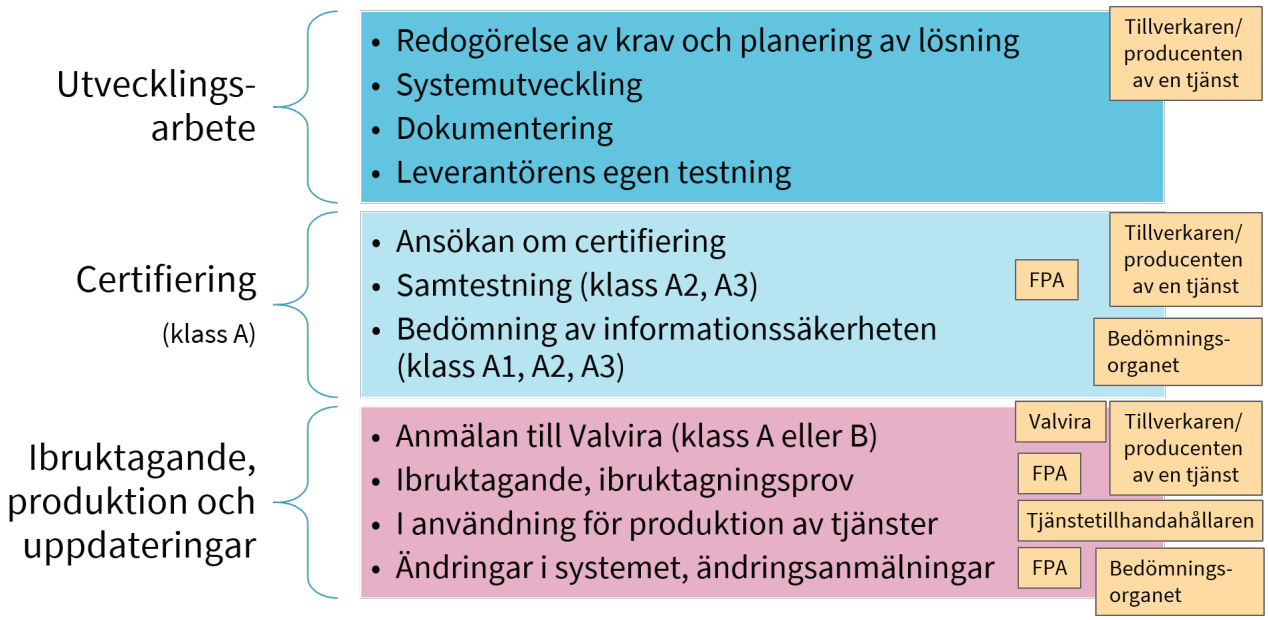
5 Tillämpningen av certifieringsprocessen

Certifieringen gäller informationssystem i klass A1, A2 eller A3. Klassificeringen av ett informationssystem görs i enlighet med föreskrift 4/2021 och dess bilaga 1. Godkänd certifiering är en förutsättning för registrering och ibruktagande av informationssystem 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 4/2021 och som utförs av tillverkaren av ett informationssystem i klass A eller producenten av en informationssystemtjänst är bland annat:

- specifikation av systemets användningsändamål
    - inklusive klassificering av systemet samt ställningstagande till vilka av profilerna för väsentliga krav och vilka andra väsentliga krav som ingår i systemets användningsändamål;
- planering och genomförande av systemet;
- egen testning av producenten av informationssystemtjänsten;
- nödvändig dokumentation
    - inklusive systemblanketten och dokumentationen av uppfyllandet av väsentliga krav som verifieras genom dokumentation.

I figur 2 finns en översikt över certifieringsprocessen, de föregående och efterföljande faserna samt aktörerna som deltar i processen. Även i anmälningar om systemändringar iakttas samma förfaranden, som följer anvisningarna i bilaga 2 till föreskrift 4/2021.



Figur 2. Certifieringsprocessen samt föregående och efterföljande åtgärder.

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 5/2021 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 i system som hör till klass A2 och A3 görs en bedömning av informationssäkerheten, men certifieringen av ett nytt system inleds genom samtestning.

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 meddelas på Traficoms webbplats. En systemblankett enligt föreskrift 5/2021 ska lämnas in till bedömningsorganet i samband med ansökan om bedömning av informationssäkerhet.

Om man genomför både samtestning och bedömning av informationssäkerheten för ett informationssystem kan informationssäkerhetsintyget skrivas först efter att samtestningen har slutförts. Ett informationssystem eller delsystem som hör till klass A och som godkänts vid bedömningen av informationssäkerhet får ett informationssäkerhetsintyg.

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 eventuellt behov av en ändringsanmälan. Vid eventuella uppföljande auditeringar ska man beakta avgränsningarna enligt föreskrift 4/2021 och praxis för

ändringsanmälningar enligt bilaga 2. Om den uppföljande auditeringen inte leder till ett nytt informationssäkerhetsintyg eller medför ändringar i uppgifterna som anmälts om informationssystemet, görs inga anteckningar om den uppföljande auditeringen i Valviras register över informationssystem.

Det krävs ingen extern testning, verifiering eller bedömning av informationssäkerheten av andra krav än de nationellt specificerade kraven. Om man till exempel vid en bedömning av informationssäkerheten också verifierar andra krav än informationssäkerhetskraven enligt föreskrift 5/2021, 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 ingår nödvändiga avtal för att använda Kanta-tjänsterna, utför ett ibruktagningsprov och vidtar andra åtgärder som behövs för att ta systemet i bruk tillsammans med producenten av en informationssystemtjänst.

Producenten av en informationssystemtjänst ska i enlighet med 30 § i lagen om kunduppgifter anmäla till Valvira när en version av ett system som är avsett för produktion av tjänster inte längre stöds. Detta gäller även situationer där producenten av en informationssystemtjänst tar systemet ur bruk för produktion av tjänster. Dessa moment 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 4/2021*. 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 5/2021, 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 5/2021, 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, eftersom de olika kraven måste uppfyllas i informationssystem som används för produktion av tjänster. Dessa tidsfrister motsvarar de kravspecifika ikraftträdandetiderna (punkt 4).

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 bilddiganostik vid en senare tidpunkt krävas av system som uppfyller kraven för specialitetsspecifika profiler. De väsentliga kraven som är gällande är alltid med i nästa certifiering för systemet som uppfyller 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.

Ett systems *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 4/2021 och 5/2021 och som grund för klassificeringen och verifieringen av system föreslås enhetliga grunder för fastställandet av risknivån för systemklasserna (A1, A2, A3, B) samt för kraven och verifieringen. Grunderna för klassificeringen beskrivs i föreskrift 4/2021 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 själva systemet alltid också på verksamheten i de organisationer 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, VAHTI-anvisningarna och VAHTI-verktygen samt kommentarer och utvecklingsförslag till utkasten till föreskrifterna.

6.3 Kravinriktning i modulära systemhelheter

Eftersom produktionen av olika tjänster är förenade 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 5/2021, där man enligt föreskriften också antecknar vilka väsentliga krav som uppfylls via andra delsystem. 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.

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 till den del 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.

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 att riskerna i samband med tillgången till webbtjänster hanteras 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.

Många av de tekniska skyddsåtgärderna genomförs via de krav på identifiering, autentisering och åtkomsthantering som ställs på informationssystemen. 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 och 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 på EU- och EES-nivå gör det möjligt att även behandla uppgifter som hör till de särskilda kategorierna av personuppgifter i EU:s allmänna dataskyddsförordning med skyddsåtgärder på samma nivå i Finland och i EU- och EES-länder. Överföring av uppgifter även till tredjeländer och behandling 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 tekniska, organisatoriska och avtalsbaserade skyddsåtgärder krävas som komplement till överföringsgrunden. 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 beräkning och slutledning minskar också riskerna i samband med dataskyddet.

En del av de väsentliga kraven är också kopplade till beredskapsbehoven vid omfattande kris- eller störningssituationer. Dessa ställer vissa väsentliga krav till exempel 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 Informationssystemens krav i förhållande till e-tjänster och välbefinnandeapplikationer

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 hör till registerföringen hos en tillhandahållare av social- och hälsovårdstjänster och samt för behandling av uppgifter i kundhandlingar, uppfyller systemet definitionen av ett informationssystem. Det är inte avgörande till exempel om informationssystemet tillhandahåller användargränssnitt för både yrkesutbildade personer och allmänheten. I många informationssystem finns till exempel funktioner som kunderna kan använda för att få uppgifter om sig själva eller lämna uppgifter till tjänstetillhandahållarnas processer och handlingar eller som grund för dem.

Enligt lagen om kunduppgifter är en välbefinnandeapplikation ett program i anslutning till informationsresursen för egna uppgifter som behandlar uppgifter om välbefinnande och som används av enskilda personer. Enligt övergångstiderna i lagen om kunduppgifter kan enskilda personer också få sina kunduppgifter till en välbefinnandeapplikation. Certifieringskraven för välbefinnandeapplikationer skiljer sig 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 skiljer sig avsevärt från informationssystemen. I en informationssystemlösning som är både ett informationssystem och en välbefinnandeapplikation iakttas i första

hand föreskrifterna 4/2021 och 5/2021, i andra hand föreskriften 6/2021. I dessa fall är det möjligt att vid samtestningen och bedömningen av informationssäkerhet testa och verifiera kraven i både föreskrift 5/2021 och föreskrift 6/2021 som en del av en enda certifieringsprocess. Då gör man ingen separat verifiering vid välbefinnandeapplikationernas bedömning av informationssäkerheten av de krav som verifierats genom en bedömning av informationssäkerheten enligt föreskrifterna 4/2021 och 5/2021 eller av motsvarande krav. Krav på utnyttjande av uppgifter som producerats via välbefinnandeapplikationer för informationssystem som används av tjänstetillhandahållare och yrkesutbildade personer kan i framtiden publiceras baserat på eventuella nationella specifikationer om ämnet.

När man planerar, genomför och bedömer lösningar för e-tjänster och välbefinnandeapplikationer måste man ta hänsyn till att lösningen används av allmänheten och individer i stället för 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 e-tjänster eller välbefinnandeapplikationer som innehåller användargränssnitt för allmänheten.

7 Mer information om beredningen av föreskrifterna 4/2021 och 5/2021

Vid beredningen av föreskrifterna 4/2021 och 5/2021 jämte bilagor har man utöver de behov som grundar sig på lag även beaktat erfarenheterna från de föreskrifter som utfärdats med stöd av lagen om klientuppgifter, som trädde i kraft 2014, och behoven av att precisera dem. Dessutom har man beaktat ett antal behov som tillhandahållare av social- och hälsovårdstjänster, producenter av informationssystemtjänster samt nationella myndigheter riktat mot de nationella specifikationerna och Kanta-tjänsterna Vid beredningen av föreskriften och kraven har man hört centrala intressentgrupper. 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 utvidgas 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. Även de förfaranden och metoder som används för att verifiera kraven skärps.

I de föreskrifter som publiceras 2021 har man kombinerat och komprimerat innehållet i flera tidigare separata anvisningar. Flera tidigare separata anvisnings- och översiktsdokument slopas i samband med att föreskrifterna träder i kraft.

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

I samband med beredningen av föreskrifterna, klassificeringen och profilerna ordnade man också en omfattande remissrunda och presenterade ämnet i flera olika samarbetsgrupper och vid olika evenemang. Utifrån responsen från remissrundan har det gjorts flera preciseringar, kompletteringar och korrigeringar i föreskrifterna 4/2021 och 5/2021 samt i kraven i dem, bland annat avseende de begrepp som använts, klassificeringen av systemen, verifieringssätten, beaktandet av riskerna i samband med systemen, övriga författningar som gäller ämnet samt innehållet i vissa krav. Jämfört med utkastversionen har innehållet i den slutliga föreskriften förtydligats bland annat i förhållande till EU:s allmänna dataskyddsförordning och dess tolkningar på EU-nivå (bland annat baserat på material från Dataombudsmannens byrå och Europeiska dataskyddsstyrelsen), SHM:s förordningsutkast om åtkomsträtt till klientuppgifter, förordningen om medicintekniska produkter och lagen om medicintekniska produkter, ISO-standarder, lagen om informationshantering inom den offentliga förvaltningen, statsrådets beslut om målen med försörjningsberedskapen, riktlinjerna för molntjänster inom den offentliga förvaltningen samt VAHTI-, Pitukri- och Katakri-rekommendationerna.