Informationsförmedlarna
Information och styrning av informationshanteringen 16.02.2022

FÖRESKRIFT OM DE VÄSENTLIGA KRAVEN PÅ OCH CERTIFIERINGEN AV VÄLBEFINNANDEAPPLIKATIONER SOM BEHANDLAR UPPGIFTER OM VÄLBEFINNANDE OCH SOM ANSLUTS TILL INFORMATIONSRESURSEN FÖR EGNA UPPGIFTER

Bemyndigande

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

Målgrupper

Tillverkare av välbefinnandeapplikationer
Folkpensionsanstalten
Bedömningsorgan för informationssäkerhet
Producenter och tillverkare av informationssystemtjänster för social- och hälsovården

Giltighetstid

Föreskriften träder i kraft den 16 februari 2022 och den gäller tills vidare.

Innehåll

1. Föreskriftens syfte

Syftet med denna föreskrift är att precisera de krav på de väsentliga välbefinnandeapplikationer som avses i lagen om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021), nedan *lagen om kunduppgifter*, samt de förfaranden och ansvar som ska användas i certifieringen av dessa. Föreskriften styr implementeringen av välbefinnandeapplikationer enligt kraven, lämnandet av de redogörelser som krävs för välbefinnandeapplikationerna, den samtestning och bedömning av informationssäkerheten som hör till certifieringen samt registreringen och ibruktagandet av välbefinnandeapplikationer.

2. Föreskriftens tillämpningsområde

Denna föreskrift gäller de förfaranden som ska iakttas vid påvisande av att välbefinnandeapplikationer som behandlar uppgifter om en enskild persons välbefinnande och som ska anslutas till informationsresursen för egna uppgifter överensstämmer med kraven samt innehållet i den utredning som ska ges (lagen om kunduppgifter, 7 kap. ”Väsentliga krav på informationssystem och välbefinnandeapplikationer”). Institutet för hälsa och välfärd (nedan THL) har med stöd av 34 § 4 mom. i lagen om kunduppgifter bemyndigats att meddela närmare föreskrifter om innehållet i de väsentliga kraven och om vilka väsentliga krav som välbefinnandeapplikationerna ska uppfylla. Enligt 35 § 3 mom. i lagen om kunduppgifter kan THL meddela föreskrifter också om de förfaranden som ska iakttas vid påvisande av överensstämmelse med kraven och om innehållet i den utredning som ska ges.

Denna föreskrift gäller välbefinnandeapplikationer som behandlar uppgifter om välbefinnande och som ansluts eller har anslutits till informationsresursen för egna uppgifter som ingår i social- och hälsovårdens riksomfattande informationssystemtjänster (nedan Kanta-tjänsterna). Alla välbefinnandeapplikationer som har anslutits till informationsresursen för egna uppgifter hör enligt 29 § i lagen om kunduppgifter till klass A. Välbefinnandeapplikationerna omfattas inte av klassificeringen i social- och hälsovårdens informationssystem vare sig i klasserna A och B eller vidare i A1, A2 och A3.

3. Definitioner

I denna föreskrift avses med:

Kunduppgift personuppgift som gäller en klient eller patient inom social- eller hälsovården som enligt 3 § i lagen om kunduppgifter är klientuppgift eller patientuppgift, ingår i en tjänstetillhandahållares klientdataregister och i allmänhet är antecknad av och administreras av en yrkesutbildad person inom social- och hälsovården.

Uppgifter om välbefinnande sådana uppgifter som en person producerat om sin hälsa och sitt välbefinnande och som personen själv har fört in i informationsresursen för egna uppgifter (3 § i lagen om kunduppgifter).

Välbefinnandeapplikation ett program i anslutning till informationsresursen för egna uppgifter som den enskilda använder och med vilket uppgifter om välbefinnande behandlas (3 § i lagen om kunduppgifter).

Integrationstjänst en tjänst som samlar information från olika utrustningar och/eller välbefinnandeapplikationer i informationsresursen för egna uppgifter. Integrationstjänsten kan till exempel vara en tjänst som samlar information från flera självmätningsapparater eller en tjänst som förmedlar uppgifter från en hälsouppföljningsplattform. Integrationstjänsten omfattas också av andra tillämpliga kriterier än av dem där integrationstjänsten nämns separat. Det är inte fråga om en sådan tjänst för förmedling av kunduppgifter som avses i THL:s föreskrift 4/2021 eller i motiveringen till 29 § i lagen om kunduppgifter (HE 212/2020).

Informationsresursen för egna uppgifter en inom de riksomfattande informationssystemtjänsterna upprättad centraliserad elektronisk informationsresurs för bevarande och behandling av uppgifter om välbefinnande (3 § i lagen om kunduppgifter).

Certifiering ett förfarande genom vilket man verifierar att en välbefinnandeapplikation uppfyller de väsentliga krav som ställs på den för att den ska få användas för produktion (3 § i lagen om kunduppgifter). Verifieringen av kraven på välbefinnandeapplikationer som hör till klass A görs genom en bedömning av informationssäkerheten och genom samtestning. Resultaten av en godkänd samtestning av en välbefinnandeapplikation och giltighetstiden för intyget över bedömning av informationssäkerheten antecknas i tillsynsmyndighetens register.

En välbefinnandeapplikation som förmedlar information vidare en tjänst som förmedlar information till olika enheter och/eller välbefinnandeapplikationer från informationsresursen för egna uppgifter. För välbefinnandeapplikationen som förmedlar uppgifter vidare gäller också andra kriterier i bilaga 1 i den här föreskriften än de i vilka välbefinnandeapplikationen som förmedlar uppgifter vidare nämns separat.

Informationssystem ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling som det i enlighet med de egenskaper som har planerats av tillverkaren är meningen att använda för elektronisk behandling av kunduppgifter och för registrering och uppdatering av kundhandlingar eller för anslutning till de riksomfattande informationssystemtjänsterna eller med vars hjälp en yrkesutbildad person inom social- och hälsovården kan använda uppgifter om välbefinnande (3 § i lagen om kunduppgifter).

Bedömning av informationssäkerhet en del av certifieringsprocessen där ett godkänt bedömningsorgan för informationssäkerhet verifierar informationssäkerhetskraven och utfärdar ett sådant intyg över bedömning av informationssäkerhet som avses i 37 § i lagen om kunduppgifter.

Bedömningsorgan för informationssäkerhet sådana företag, sammanslutningar och myndigheter som Transport- och kommunikationsverket med stöd av lagen om bedömningsorgan för informationssäkerhet (1405/2011) har godkänt att utföra bedömningar av informationssäkerhet.

Verifiering ett förfarande som påvisar att en välbefinnandeapplikation uppfyller de krav som ställs på den. Verifieringssätten är bl.a. genomgång av dokumentation, testning av välbefinnandeapplikationen, genomgång av meddelanden, loggar eller andra produkter som välbefinnandeapplikationen producerar och vid behov som kompletterande verifieringsmetod en dokumenterad intervju med tillverkaren av välbefinnandeapplikationen. Verifieringen behandlas närmare i kapitel 9.2.

Intyg över bedömning av informationssäkerhet eller informationssäkerhetsintyg ett intyg utfärdat av ett godkänt bedömningsorgan över att en välbefinnandeapplikation har godkänts vid en bedömning av informationssäkerheten.

Samtestning interoperabilitetstestning enligt 36 § i lagen om kunduppgifter som ordnas av FPA och som påvisar välbefinnandeapplikationens interoperabilitet med Kanta-tjänsterna och övriga anslutna informationssystem. Som resultat av samtestningen utarbetar FPA en samtestningsrapport och ger ett positivt utlåtande om uppfyllelsen av kraven på interoperabilitet (samtestningsutlåtande) när kraven som ska testas har verifierats med godkänt resultat.

4. Föreskriftens centrala innehåll och avgränsningar

En välbefinnandeapplikation som används vid behandling av uppgifter om välbefinnande ska uppfylla de väsentliga kraven på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet samt kraven på tillgänglighet. Enligt lagen ska den som producerar en välbefinnandeapplikation påvisa att välbefinnandeapplikationen överensstämmer med kraven. Till påvisandet hör en utredning om att välbefinnandeapplikationen uppfyller de väsentliga krav som motsvarar dess användningsändamål.

Den här föreskriften innehåller de väsentliga kraven på välbefinnandeapplikationer, vilka beskrivs i bilaga 1 *väsentliga krav på välbefinnandeapplikationer anslutna till informationsresursen för egna uppgifter.* I föreskriften preciseras dessutom de förfaranden som används vid anmälan, certifiering och verifiering av väsentliga krav.

Verifieringen av de väsentliga kraven i föreskriften kan vara en del av eller höra samman med en mer omfattande utvärdering av en välbefinnandeapplikation eller av välbefinnandeteknologier, där man även bedömer andra faktorer än dem som gäller kriterierna i föreskriften, såsom olika faktorer eller egenskaper som ansluter sig till kvaliteten på digitala tjänster mer omfattande. Det centrala i certifieringen enligt föreskriften är att välbefinnandeapplikationen fungerar tillsammans med informationsresursen för egna uppgifter och andra välbefinnandeapplikationer som anslutits till den, att de beskrivningar och den information som ges till medborgarna är tillräckliga samt att riskhanteringen i anslutning till dataskydd och informationssäkerhet fungerar. Resultatuppgifterna för en eventuell mer omfattande bedömning ska tydligt avskiljas från bedömningen och samtestningen av kraven i föreskriften så att bedömningen av kraven i föreskriften endast ger ett informationssäkerhetsintyg över kraven samt resultaten av samtestningen.

I den här föreskriften beskrivs inte de väsentliga krav på informationssystemen som avses i lagen om kunduppgifter eller de certifieringsförfaranden som beskrivs i THL:s föreskrifter 4/2021 och 5/2021. Enligt lagen om kunduppgifter är ett informationssystem ett system avsett att användas för elektronisk behandling av kunduppgifter och för registrering och uppdatering av kundhandlingar. Ifall systemet har planerats för behandling av kunduppgifter och uppgifter i kundhandlingar som hör till registerföringen hos en tillhandahållare av social- och hälsovårdstjänster uppfyller det definitionen av ett informationssystem. Det är exempelvis inte avgörande om informationssystemet tillhandahåller användargränssnitt både för yrkesutbildade personer och för medborgare. I många informationssystem finns till exempel funktioner som kunderna kan använda för att få sådana uppgifter om sig själva som finns i tjänstetillhandahållarens personregister eller lämna uppgifter till tjänstetillhandahållarnas processer och till handlingar i tjänstetillhandahållarens personregister eller till grund för dem.

Certifieringskraven för välbefinnandeapplikationer skiljer sig från dem för informationssystem. Orsaken till detta är att författningarna som gäller välbefinnandeapplikationer, användargruppen, typen av uppgifter som behandlas och uppgifternas innehåll, riskerna, Kanta-anslutningslösningarna samt ansvaret för egenkontroll och myndighetstillsyn avsevärt skiljer sig från informationssystemen. Ifall det är fråga om ett informationssystem som avses i lagen om kunduppgifter och som också uppfyller definitionen på en välbefinnandeapplikation:

- tillämpas i första hand föreskrifterna 4/2021 och 5/2021 och i andra hand föreskrift 6/2021 (denna föreskrift).
- Utförs certifieringen av systemet och verifieringen av de väsentliga kraven på systemet i första hand i enlighet med föreskrifterna 4/2021 och 5/2021.
- I dessa fall är det möjligt att i samtestningen testa och i bedömningen av informationssäkerheten verifiera kraven i både föreskrift 5/2021 och föreskrift 6/2021 som en del av en och samma certifieringsprocess.
- Då gör man i bedömningen av välbefinnandeapplikationernas informationssäkerhet ingen separat verifiering av de krav som verifierats genom en bedömning av informationssäkerheten enligt föreskrifterna 4/2021 och 5/2021 eller av motsvarande krav.
- Behandlingen av personuppgifter och eventuell behandling av kunduppgifter i systemet ska beaktas i informationssäkerhetsplanen för de tillhandahållare av social- och hälsovårdstjänster som använder systemet i enlighet med föreskrift 3/2021.
- Kraven på välbefinnandeapplikationerna och de informationssäkerhetskrav som inte motsvarar de krav som verifieras via föreskriften 5/2021 verifieras i enlighet med denna föreskrift (6/2021).

Krav på utnyttjande av uppgifter som producerats via välbefinnandeapplikationer för informationssystem som används av tjänstetillhandahållare och yrkesutbildade personer kan i framtiden publiceras. Grunden för kraven är eventuella kommande nationella specifikationer med anknytning till ämnet. En välbefinnandeapplikation är enligt lagen om kunduppgifter ett program i anslutning till informationsresursen för egna uppgifter som den enskilde

använder. Enligt de övergångstider som nämns i övergångsbestämmelserna i lagen om kunduppgifter kan enskilda personer också få sina kunduppgifter till en välbefinnandeapplikation.

En välbefinnandeapplikation kan vara en medicinteknisk produkt eller innehålla delar som har medicinskt användningsändamål[1]. Om välbefinnandeapplikationen eller en utrustning i samband med den har ett användningsändamål enligt lagstiftningen om medicintekniska produkter, såsom ett diagnostiskt eller vårdstyrande ändamål ska kraven och skyldigheterna (bl.a. MD-förordningen (EU) 2017/745) som gäller den eller dess tillverkare samt utrustningen anmälas till Fimeas register. Den här föreskriften är oberoende av hur välbefinnandeapplikationer klassificeras på basis av lagstiftningen om medicintekniska produkter. Tillverkaren av en välbefinnandeapplikation ska ta ställning separat till om välbefinnandeapplikationen eller en del av den ska klassificeras som en medicinteknisk produkt.

Med den certifiering som avses i den här föreskriften avses inte frivillig certifiering av personuppgiftsansvariga eller av personuppgiftsbiträden enligt artiklarna 42-44 i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter (den allmänna dataskyddsförordningen). Certifiering enligt denna föreskrift betraktas således inte som en utredning av huruvida dataskyddsförordningen efterlevs eller ansvarsskyldigheten enligt dataskyddsförordningen uppfylls. Den certifiering som föreskrivs i lagen om kunduppgifter påverkar inte de befogenheter som dataombudsmannens byrå har på basis av dataskyddslagstiftningen.

5. Certifieringsprocessen

I certifieringsprocessen krävs av välbefinnandeapplikationer:

1. en utredning av att de väsentliga kraven uppfylls;

2. samtestning av Folkpensionsanstalten (nedan FPA) som leder till att FPA ger ett positivt utlåtande om interoperabilitet för en välbefinnandeapplikation som på ett godtagbart sätt uppfyller kraven på interoperabilitet;

3. en bedömning av informationssäkerheten där en godkänd välbefinnandeapplikation av klass A beviljas intyg över bedömning av informationssäkerheten av ett bedömningsorgan för informationssäkerhet.

Tillverkaren av en välbefinnandeapplikation ansvarar för att inleda och genomföra certifieringen.

1 Med en **medicinteknisk produkt** avses ett instrument, en apparat, en anordning, en programvara, ett implantat, en reagens, ett material eller en annan artikel som enligt tillverkaren är avsedd att användas på människor, antingen separat eller i kombination, för följande medicinska ändamål:

- diagnos, profylax, övervakning, prediktion, prognos, behandling eller lindring av sjukdom,
- diagnos, övervakning, behandling, lindring av eller kompensation för en skada eller funktionsnedsättning,
- undersökning, ersättning eller ändring av anatomin eller av en fysiologisk eller patologisk process eller ett fysiologiskt eller patologiskt tillstånd,
- tillhandahållande av information genom undersökning in vitro av prover från människokroppen, inklusive donationer av organ, blod och vävnad,

och som inte uppnår sin huvudsakliga, avsedda verkan i eller på människokroppen med hjälp av farmakologiska, immunologiska eller metaboliska medel, men som kan understödjas i sin funktion av sådana medel. Produkter avsedda för befruktningskontroll eller fertilitetsstöd ska också anses vara medicintekniska produkter (artikel 2 i Europaparlamentets och rådets förordning (EU) 2017/745 om medicintekniska produkter).

Tillverkaren av välbefinnandeapplikationen ska uppfylla och testa de egenskaper i välbefinnandeapplikationen som ska certifieras före samtestning eller bedömning av informationssäkerheten. Uppfyllandet av de väsentliga kraven ska dokumenteras enligt bilaga 1 så att det inte råder oklarheter om huruvida applikationen uppfyller de väsentliga kraven och så att den dokumentation som behövs för verifiering av de krav som ska verifieras på basis av dokumentationen finns tillgänglig.

Certifieringsprocessen genomförs i den ordning som beskrivs nedan:

1) Samtestning (36 § i lagen om kunduppgifter). Före samtestningen ska tillverkaren av välbefinnandeapplikationen ge FPA en utredning av hur kraven på välbefinnandeapplikationens funktionalitet har uppfyllts och testats och vilka krav på funktionaliteten som har uppfyllts. Tillverkaren av välbefinnandeapplikationen ska anmäla välbefinnandeapplikationen till FPA:s samtestning tillsammans med Kanta-tjänsterna enligt FPA:s anvisningar eller för bedömning av behovet av samtestning på grund av väsentliga ändringar i välbefinnandeapplikationen. Tidpunkten för och genomförandet av samtestningen ska avtalas med FPA. En utredning av hur de väsentliga kraven uppfylls (bilaga 1) ska lämnas till FPA i samband med ansökan om samtestning. Tillverkaren av välbefinnandeapplikationen ansvarar för att uppgifterna om uppfyllandet av de väsentliga kraven i bilaga 1 är korrekta och exakta. FPA ska kontrollera riktigheten i de primära uppgifterna och genomföra en samtestning i samarbete med tillverkaren av välbefinnandeapplikationen av de funktionaliteter, gränssnitt och innehåll baserade på informationsresursens specifikationer som genomförts på välbefinnandeapplikationen. Efter godkänd samtestning ger FPA ett samtestningsutlåtande. Ett utlåtande om samtestning är en förutsättning för att ett bedömningsorgan för informationssäkerhet ska bevilja ett intyg över bedömning av informationssäkerheten. FPA ska lämna ett samtestningsutlåtande åtminstone till tillverkaren av välbefinnandeapplikationen och till Tillstånds- och tillsynsverket för social- och hälsovården (nedan Valvira). Om en bedömning av informationssäkerheten pågår för välbefinnandeapplikationen ska FPA också lämna samtestningsutlåtandet till bedömningsorganet för informationssäkerhet.

2) Bedömning av informationssäkerhet (37 § i lagen om kunduppgifter). Tillverkaren av en välbefinnandeapplikation anmäler välbefinnandeapplikationen till bedömning av informationssäkerheten som görs tillsammans med bedömningsorganet för informationssäkerhet eller till utvärdering av behovet av en ny bedömning av informationssäkerheten på grund av väsentliga ändringar i välbefinnandeapplikationen. Kriterierna för bedömning av informationssäkerheten ska vara de krav som anges på flikarna i bilaga 1, i vilka det som verifieringssätt antecknats den dokumentation som ska ses över i bedömningen, den funktionella testning som ska utföras i bedömningen (för att pröva genomförandet eller praktiken i samband med kraven på informationssäkerhet eller riktighet) eller den tekniska informationssäkerhetstestningen. De krav som ska ses över vid samtestningen behandlas inte på nytt i bedömningen av informationssäkerheten. Tillverkaren ska till bedömningsorganet lämna en utredning av att de väsentliga kraven har uppfyllts på en blankett enligt bilaga 1, vid behov den tilläggsdokumentation som krävs för att verifiera kraven och ett utlåtande om samtestning. De redogörelser och den dokumentation som behövs i de olika punkterna kan kombineras i samma dokument, varvid man måste se till att den dokumentation som behövs för att verifiera att respektive krav uppfyllts tydligt kommer fram via de uppgifter som fyllts i på blanketten i bilaga 1. I samband med bedömningen av informationssäkerhet ses rapporten om resultaten i testningen av tillgänglighet över. Välbefinnandeapplikationens tillgänglighet ska testas med hjälp av en tillgänglighetsbedömning som görs av tillverkaren själv eller av en utomstående aktör.

Om välbefinnandeapplikationen ska certifieras så att den genomgår både samtestning och bedömning av informationssäkerheten, ska tillverkaren av välbefinnandeapplikationen se till att samtestningen och bedömningen av informationssäkerheten gäller samma version av välbefinnandeapplikationen eller en sådan version där eventuella ändringar i välbefinnandeapplikationen relaterade till de väsentliga krav som ska samtestas inte påverkar de informationssäkerhetskrav som ska auditeras.

En välbefinnandeapplikation som godkänts i bedömningen får ett intyg över bedömning av informationssäkerhet och en tillhörande kontrollrapport av bedömningsorganet. Bedömningen ska göras i enlighet med de väsentliga kraven på välbefinnandeapplikationens användningsändamål eller med omfattningen av de ändringar som gjorts i

välbefinnandeapplikationen. Intyget är i kraft högst tre år. Intygets giltighetstid kan förlängas med högst tre år åt gången. Förnyande av överensstämmelse med kraven beskrivs i kapitel 8.

I krav där man som verifieringssätt alternativt har angett teknisk informationssäkerhetstestning eller dokumentation, kan verifieringen basera sig på ett tekniskt informationssäkerhetstest som utförs av bedömningsorganet eller på en bedömning av den testrapport som tillverkaren av välbefinnandeapplikationen lämnar in. Om alla de krav som är tillämpliga på välbefinnandeapplikationen och som innehåller teknisk informationssäkerhetstestning verifieras genom ett tekniskt informationssäkerhetstest som görs av bedömningsorganet som en del av certifieringen, antecknas i intyget över bedömning av informationssäkerheten "Externt tekniskt informationssäkerhetstest som utförts vid verifiering av informationssäkerhetskraven." I registreringen av välbefinnandeapplikationen samt i marknadsförings- eller informationsmaterialet kan uttrycket "Externt utfört informationssäkerhetstest" användas.

Lagen om kunduppgifter kräver inga regelbundna uppföljande auditeringar av informationssäkerheten, men producenten av en informationssystemtjänst och bedömningsorganet kan avtala om uppföljande auditeringar. Eventuella uppföljande auditeringar av informationssäkerheten hos en välbefinnandeapplikation ska skiljas åt från de bedömningar som syftar till att förnya intyget. Ett nytt intyg över bedömning av informationssäkerhet skrivs inte för uppföljande auditeringar och giltighetstiden för ett gammalt intyg förlängs inte som ett resultat av en uppföljande auditering. Om den uppföljande auditeringen inte leder till ett nytt informationssäkerhetsintyg eller till att uppgifterna i Valviras register över informationssystem måste uppdateras, behöver man inte göra någon anteckning om den uppföljande auditeringen i Valviras register över informationssystem.

6. Registrering av en välbefinnandeapplikation

Tillverkaren av en välbefinnandeapplikation ska göra en anmälan om välbefinnandeapplikationen till Tillstånds- och tillsynsverket för social- och hälsovården innan välbefinnandeapplikationen tas i användning för produktion av tjänster (30 § i lagen om kunduppgifter). Vid anmälan ska Valviras anvisningar eller föreskrifter om anmälan av en välbefinnandeapplikationen följas. Anmälan ska åtföljas av ett utlåtande om samtestning, ett intyg över bedömning av informationssäkerheten och en redogörelse enligt bilaga 1 som motsvarar de väsentliga krav som setts över vid samtestningen och bedömningen. Tillverkaren av välbefinnandeapplikationen ansvarar för att uppgifterna om uppfyllandet av de väsentliga kraven i bilaga 1 är korrekta och exakta. De uppgifter som ska anmälas ska motsvara de väsentliga krav som har uppfyllts i eller som ska uppfyllas via välbefinnandeapplikationen. Uppgifterna om välbefinnandeapplikationen ska vara publicerade i Valviras register över informationssystem innan välbefinnandeapplikationen får tas i bruk. Genom anmälan till Valvira och där tillhörande beskrivningar försäkrar tillverkaren av en välbefinnandeapplikation att välbefinnandeapplikationen, då den är korrekt installerad och används i enlighet med användningssyftet och anvisningarna, uppfyller de väsentliga krav som föreskrivs i 34 § i lagen om kunduppgifter och i denna föreskrift.

Valvira kan meddela närmare anvisningar om registeranmälningarna och be tillverkaren av en välbefinnandeapplikation, FPA eller bedömningsorganet om ytterligare information för att säkerställa uppgifternas riktighet.

7. Ibruktagande av en välbefinnandeapplikation och uppföljning efter ibruktagandet

En välbefinnandeapplikation får tas i bruk för produktion av tjänster och anslutas till Kanta-tjänsterna efter att välbefinnandeapplikationen har certifierats i enlighet med 35 § i lagen om kunduppgifter och dess uppgifter finns i Valviras register över informationssystem.

En välbefinnandeapplikation ska uppfylla de väsentliga krav som motsvarar välbefinnandeapplikationens användningsändamål innan den kan tas i bruk för produktion av tjänster. Tillverkaren av en välbefinnandeapplikation ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera de erfarenheter av välbefinnandeapplikationen som fås under den tid det används för produktion av tjänster i enlighet med 32 § i lagen om kunduppgifter. Alla som använder en välbefinnandeapplikation, FPA och Valvira ska underrättas om betydande avvikelser i välbefinnandeapplikationen (se kapitel 9.4).

Tillverkaren av en välbefinnandeapplikation ska följa ändringarna i de väsentliga kraven på välbefinnandeapplikationer och göra de korrigeringar som ändringarna kräver. Väsentliga ändringar i välbefinnandeapplikationen ska anmälas till bedömningsorganet för informationssäkerhet och till FPA. Intyget över bedömning av informationssäkerhet eller samtestningen ska förnyas om det görs betydande ändringar i välbefinnandeapplikationen eller om de väsentliga kraven har ändrats på ett sätt som kräver ny certifiering. I kraven i bilaga 1 beskrivs vissa ändringar som anses väsentliga och sådana som ska anmälas. THL kan ge anvisningar om vilka ändringar i en välbefinnandeapplikation som tidigare samtestats eller godkänts i en bedömning av informationssäkerheten som ska anmälas till FPA och till bedömningsorganet för informationssäkerhet.

8. Förnyande av överensstämmelse med kraven

När ett intyg över bedömning av informationssäkerhet som getts en välbefinnandeapplikation börjar bli föråldrad ska tillverkaren av välbefinnandeapplikationen kontakta bedömningsorganet för informationssäkerhet för förnyande av informationssäkerhetsintyget. Tillverkaren av välbefinnandeapplikationen ska också kontakta FPA för att behovet av samtestning av välbefinnandeapplikationen ska kunna bedömas på nytt.

Bedömningsorganet för informationssäkerhet och FPA ska kontaktas senast 6 månader innan informationssäkerhetsintyget går ut.

Välbefinnandeapplikationen ska vid behov samtestas i förhållande till gällande specifikationer eller de specifikationer som krävs vid samtestning innan ett nytt intyg över bedömning av informationssäkerhet beviljas. FPA ger ett positivt samtestningsutlåtande över samtestning som utförts med godkänt resultat.

För den ovan beskrivna bedömningen ska tillverkaren av välbefinnandeapplikationen ge FPA aktuell information om vilka av de krav som ska samtestas i anslutning till informationsresursen för egna uppgifter som har uppfyllts och vilka specifikationsversioner implementeringarna baseras på. En implementering ska ändras så att den grundar sig på en aktuell eller erforderlig specifikationsversion innan man ansöker om samtestning, ifall:

- implementeringen grundar sig på en föråldrad specifikation och tidsfristen, som fastställts i samband med den nya ersättande specifikationen eller i författningar, för när den nya specifikationsversionen ska tas i bruk har löpt ut; eller

- implementeringen inte motsvarar den publicerade specifikation eller specifikationsversion som krävs i produktionsmiljön för informationsresursen för egna uppgifter; eller

- implementeringen inte motsvarar den publicerade specifikationsversion som krävs för samtestning med informationsresursen för egna uppgifter, även om implementeringar enligt den äldre versionen som utgår fortfarande skulle stödas i produktionsmiljön för informationsresursen för egna uppgifter.

Bedömningsorganet för informationssäkerhet utför en bedömning av informationssäkerheten i syfte att förnya informationssäkerhetsintyget genom att verifiera alla väsentliga informationssäkerhetskrav som är relevanta för välbefinnandeapplikationen. I verifieringen av respektive krav kan man stödja sig på samma förfaranden och dokumentation som i det tidigare beviljade informationssäkerhetsintyget, om inte sätten att implementera eller

uppfylla kravet har ändrats i välbefinnandeapplikationen eller om det inte har skett förändringar i systemets driftsmiljö som påverkar uppfyllandet av kraven. Bedömningsorganet för informationssäkerhet ger ett informationssäkerhetsintyg över godkänd bedömning av informationssäkerheten i enlighet med kapitel 5 i den här föreskriften.

På grund av förnyandet av överensstämmelsen med kraven ska tillverkaren av en välbefinnandeapplikation lämna de uppdaterade uppgifterna om välbefinnandeapplikationen till Valvira, så att uppgifterna kan uppdateras i Valviras register över informationssystem.

9. Väsentliga krav

Tillverkaren av en välbefinnandeapplikation ansvarar för planeringen och tillverkningen av välbefinnandeapplikationen. En välbefinnandeapplikation som används vid behandling av uppgifter om välbefinnande ska uppfylla de väsentliga kraven på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. Enligt lagen om kunduppgifter ska en välbefinnandeapplikation också uppfylla kraven på tillgänglighet. Tillverkaren av en välbefinnandeapplikation ansvarar för att specificera välbefinnandeapplikationens användningsändamål och för redogörelsen för överensstämmelse med kraven samt för certifieringen och registreringen av välbefinnandeapplikationen. En redogörelse för överensstämmelse med kraven görs med hjälp av blanketten i bilaga 1. Genom redogörelsen försäkrar tillverkaren av en välbefinnandeapplikation att välbefinnandeapplikationen uppfyller de väsentliga krav som gäller den och beskriver hur de väsentliga kraven uppfylls. En redogörelse enligt bilaga 1 är en förutsättning för certifiering och registrering av en välbefinnandeapplikation.

Kraven är avsedda att säkerställa att välbefinnandeapplikationerna stämmer överens med kraven och att förtydliga och stöda utvecklingen, testningen, certifieringen, bedömningen och upphandlingen av välbefinnandeapplikationer samt kommunikationen mellan olika parter. Tillverkaren av en välbefinnandeapplikation ska i regel uppfylla de krav i bilaga 1 som är tillämpliga på välbefinnandeapplikationen, såvida det inte finns något annat omnämnande om hurdana välbefinnandeapplikationer kravet gäller.

En välbefinnandeapplikation ska förutom de föreskrivna kraven i lagen om kunduppgifter och i denna föreskrift även uppfylla kraven i andra författningar som gäller den. Om välbefinnandeapplikationen till exempel lagrar personuppgifter någon annanstans än i informationsresursen för egna uppgifter, ska ansvaret för registerföringen i anslutning till välbefinnandeapplikationen och därtill hörande administrations-, skydds- och tillsynsansvar definieras och beskrivas enligt bestämmelserna. Ifall det som ett led i certifieringen observeras att välbefinnandeapplikationen inte uppfyller de krav i andra författningar som gäller den, kan certifieringen inte godkännas.

9.1 De väsentliga kravens delområden

Till kraven hör följande delområden för vilkas ifyllande och beskrivning på blanketten i föreskriftens bilaga 1 tillverkaren av en välbefinnandeapplikation ansvarar:

Basuppgifter

Basuppgifterna om en välbefinnandeapplikation ska fyllas i på fliken Basuppgifter i bilaga 1. Till basuppgifterna hör också en beskrivning av välbefinnandeapplikationens användningsändamål, för vilken tillverkaren av välbefinnandeapplikationen ansvarar. Användarna ska också ges nödvändig information om välbefinnandeapplikationen och vid behov anvisningar om hur den tas i bruk och används.

Författningar och anvisningar

På fliken Författningar och anvisningar i bilaga 1 beskrivs hur man i en välbefinnandeapplikation uppfyller de centrala skyldigheterna i olika författningar. Välbefinnandeapplikationens användningsändamål, karaktär och begränsningar inverkar också på vilka krav från olika författningar som gäller välfärdsapplikationen.

Grundläggande krav

På fliken Grundläggande krav i bilaga 1 rapporterar tillverkaren av en välbefinnandeapplikation om de grundläggande kraven på välbefinnandeapplikationen samt om bland annat typen av välbefinnandeapplikation och omständigheterna kring eventuell reklam.

Beskrivningar för medborgare

På fliken Beskrivningar för medborgare i bilaga 1 beskrivs de viktigaste omständigheterna som de som använder en välbefinnandeapplikation måste informeras om genom en tydlig kommunikation i överensstämmelse med kraven.

Informationssäkerhets- och dataskyddskrav

Kraven på informationssäkerhet och dataskydd för välbefinnandeapplikationer har samlats på fliken Informationssäkerhets- och dataskyddskrav i bilaga 1 till denna föreskrift.

Funktionella krav

De centrala funktionella kraven beskrivs på fliken Funktionella krav i bilaga 1 De funktionella kraven på funktionerna och informationsinnehållen i en välbefinnandeapplikation finns också på andra flikar, och de ses över vid en samtestning eller i en bedömning av informationssäkerheten.

Tillgänglighetskrav

Välbefinnandeapplikationerna ska uppfylla tillgänglighetskraven. Tillgänglighetskraven finns på fliken Tillgänglighetskrav i föreskriftens bilaga 1.

Samtestningskrav

Interoperabiliteten ska påvisas vid en samtestning som ordnas av FPA. Samtestningskraven finns på fliken Samtestningskrav i bilaga 1.

9.2 Hur kraven verifieras

De krav som beskrivs i bilaga 1 är bindande krav. Det ska beskrivas hur alla de krav som är tillämpliga på en välbefinnandeapplikation uppfylls. De krav som ingår i samtestningen och bedömningen ska verifieras. Välbefinnandeapplikationen ska uppfylla alla de krav som är tillämpliga på välbefinnandeapplikationen i fråga. Om något krav inte är tillämpligt på välbefinnandeapplikationen, ska tillverkaren av välbefinnandeapplikationen tydligt anteckna detta i en utredning med hjälp av bilaga 1. FPA som ansvarar för testningen av interoperabilitet eller det bedömningsorgan som ansvarar för bedömningen av informationssäkerhet kan emellertid fatta beslut om huruvida kravet ska tillämpas på välbefinnandeapplikationen. Om ett obligatoriskt väsentligt krav inte uppfylls kan bedömaren fastställa en tidsfrist för uppfyllandet av kravet innan testningen eller bedömningen av informationssäkerheten godkänns som en del av den pågående certifieringsprocessen.

Som en del av verifieringen rapporterar bedömaren (och i tillämpliga delar/vid behov testaren av interoperabilitet) följande för alla krav som bedömningen (eller testningen) omfattar:

- hur väl kraven uppfylls, något av följande alternativ
    - kravet uppfylls helt
    - kravet uppfylls delvis och den del som inte uppfylls kompenseras; kompensationssättet ska beskrivas
    - kravet uppfylls inte

- om kravet inte kan tillämpas eller endast delvis kan tillämpas på den välbefinnandeapplikation som bedöms, ska detta omnämnas och motiveras

- verifieringssättet och information om hur uppfyllandet av kravet har konstaterats, till exempel hänvisning till dokumentation, testrapport eller output av programvara.

Uppfyllandet av tillämpliga väsentliga krav ska påvisas som en del av certifieringen så att certifieringen av välbefinnandeapplikationen kan godkännas.

Vid verifieringen av kraven används följande verifieringssätt:

- V: validering eller teknisk inspektion, till exempel genomgång av välbefinnandeapplikationens logg, en meddelandeinstans eller en rapport från systemet;

- T: testning, där i tillämpliga delar

    - YT: ses över som en del av FPA:s samtestning
    - TT: välbefinnandeapplikationen ses över genom användning (med funktionell testning) av existensen av och ändamålsenligheten en hos en egenskap, som en del av informationssäkerhetsbedömningen (även de beskrivningar som visas för slutanvändaren)
    - HT: teknisk dataskydds- och sårbarhetstestning och bedömning av säkerhetsnivån, som en del av informationssäkerhetsbedömningen
    - ST: testning av tillgänglighetskraven som en del av den bedömning av tillgänglighetskraven som välbefinnandeapplikationens tillverkare själv eller en extern aktör gör. I samband med bedömningen av informationssäkerhet ses rapporten om resultaten i tillgänglighetstestningen över.

- D: genomgång av välbefinnandeapplikationens dokumentation (även annan än den som visas för slutanvändaren):

- (kompletterande) H: intervju och dokumentering av intervjun som en del av bedömningen av informationssäkerhet, med vilken bedömningen kan fördjupas och kompletteras; en intervju är inte godtagbar som primär metod för verifiering av krav i välbefinnandeapplikationer av klass A

Verifieringar märkta YT görs som en del av samtestningen med FPA. Verifieringar märkta D, HT, TT och V görs som en del av bedömningen av informationssäkerhet.

Vid verifiering av krav ska man använda ett verifieringssätt som är tillräckligt för att verifiera varje krav eller kravpunkt. Ett tillräckligt verifieringssätt anges separat för varje krav. De administrativa och i tillämpliga delar även de tekniska verifieringssätten enligt Transport- och kommunikationsverket Traficoms anvisningar är en viktig utgångspunkt för den tillämpning som ska göras i bedömningen.

Särskilt i tekniska informationssäkerhets- och sårbarhetstester (verifieringssätt HT) bör man tillämpa ett lämpligt allmänt ramverk för informationssäkerhetstestning, såsom OWASP ASVS eller MASVS, i den mån kraven motsvarar eller är förenliga med informationssäkerhetskraven i bilaga 1.

9.3 Versionshantering av krav och specifikationer

FPA eller THL publicerar uppgifter om vilka de gällande specifikationerna och specifikationsversionerna är, och med stöd av vilka versioner överensstämmelsen med kraven ska verifieras. FPA publicerar aktuella uppgifter om vilka specifikationer och specifikationsversioner som krävs i Kanta-tjänsternas produktionsmiljö och i samtestning med Kanta-gränssnitt.

Om det i samband med att FPA:s eller THL:s nya specifikationer eller specifikationsversioner träder i kraft krävs att en tidigare implementering av en välbefinnandeapplikation ändras på ett sätt som kräver ny certifiering, anger FPA eller THL detta i samband med att specifikationerna publiceras. Om en ny certifiering eller en ny bedömning av certifieringsbehovet krävs, ska dessa åtgärder genomföras inom den tidsfrist som anges i föreskriften eller i anslutning till specifikationen. Om dessa åtgärder eller tidsfrister inte krävs är också implementeringar enligt tidigare specifikationsversioner godtagbara vid testning och i användning för produktion av tjänster.

9.4 Betydande avvikelser

Betydande avvikelser är:

- avvikelser som medför betydande risker för dataskyddet, informationssäkerheten, social- och hälsovårdstjänsternas verksamhet eller för patient- eller klientsäkerheten,
- sådana avvikelser från de väsentliga kraven på en välbefinnandeapplikation som används för produktion av tjänster, vilka medför betydande eller långvariga återverkningar eller ytterligare avvikelser för flera aktörer eller flera andra välbefinnandeapplikationer,
- föråldrat informationssäkerhetsintyg för en välbefinnandeapplikation som är i produktionsbruk,
- egenskaper hos en välbefinnandeapplikation i produktionsbruk som grundar sig på en föråldrad specifikationsversion vars giltighet har upphört, eller stödet i informationsresursen för egna uppgifter har upphört eller håller på att upphöra,
- tidsfristerna för de korrigeringsbehov som observerats i certifieringsprocessen har inte iakttagits, eller
- andra avvikelser som tillsynsmyndigheten (t.ex. Valvira, Regionförvaltningsverket i Södra Finland eller Dataombudsmannens byrå) konstaterat utgöra betydande avvikelser

Betydande avvikelser ska anmälas enligt 32 § i lagen om kunduppgifter. En tillverkare av en välbefinnandeapplikation och vid behov en tjänstetillhandahållare som en betydande avvikelse gäller, ska vidta åtgärder för att rätta till avvikelsen. Valvira publicerar information om avvikelser i välbefinnandeapplikationer som en del av registret över informationssystem.

Om det som en del av certifieringsprocessen upptäcks en sådan avvikelse från de väsentliga kraven som skulle leda till en betydande avvikelse i användningen för produktion av tjänster, kan certifieringen inte slutföras med godkänt resultat innan avvikelsen har korrigerats. Krav som inte uppfylls eller som uppfylls på ett bristfälligt sätt kan medföra behov av korrigering innan samtestningen eller bedömningen av informationssäkerheten godkänns, enligt beskrivningen i avsnitt 9.2.

Om en välbefinnandeapplikation som används för produktion av tjänster inte uppfyller de gällande väsentliga kraven på den eller om dess överensstämmelse med kraven har föråldrats, ska tillverkaren av välbefinnandeapplikationen underrätta Valvira och FPA om detta. Valvira och de tjänstetillhandahållare som använder välbefinnandeapplikationen ska i enlighet med 32 § i lagen om kunduppgifter underrättas om betydande avvikelser. Om avvikelsen beror på välbefinnandeapplikationen eller på den verksamhet som tillverkaren av välbefinnandeapplikationen bedriver, ska tillverkaren av välbefinnandeapplikationen bedöma den risk som avvikelserna medför och planera nödvändiga korrigeringar eller fortsatta åtgärder utifrån riskbedömningen. Denna åtgärd ska vidtas utöver vad som föreskrivs i 32 § i lagen om kunduppgifter om uppföljning efter ibruktagandet av en välbefinnandeapplikation.

9.5 Dataskydds- och beredskapskrav på tredjepartstjänster

Tillverkaren av en välbefinnandeapplikation måste beakta dataskydds- och informationssäkerhetsrisker samt beredskapsbehov i sin verksamhet. Tillverkaren av en välbefinnandeapplikation ansvarar för de väsentliga krav som gäller välbefinnandeapplikationen även till de delar där välbefinnandeapplikationen stöder sig på verktyg eller plattformar som produceras av en tredje part eller på ICT-tjänster som tillhandahåller delade resurser. Samma grundkrav tillämpas också i situationer där man använder kapacitetstjänster som produceras av en tredje part, såsom serveruthyrning, serverhantering, backuptjänster, serverhallstjänster eller molntjänster.

Plattformstjänster, inklusive molntjänster som tillhandahåller delade resurser, kan produceras av andra parter än tillverkaren av en välbefinnandeapplikation. Liksom i den offentliga förvaltningens riktlinjer för molntjänster kan också icke-offentlig information som ska behandlas i en välbefinnandeapplikation behandlas i en offentlig molntjänst, när informationssäkerheten och dataskyddet har implementerats och verifierats på behörigt sätt. Den egentliga välbefinnandeapplikationen kan också genomföras exempelvis som en molnbaserad SaaS-tjänst ifall de väsentliga kraven kan uppfyllas och verifieras, och om riskhanteringen har beaktats på en tillräcklig nivå i överensstämmelse med kraven på informationssäkerhet och dataskydd i bilaga 1. Tillverkaren av en välbefinnandeapplikation kan använda molnbaserade PaaS- eller IaaS-lösningar för att genomföra välbefinnandeapplikationen på ett skalbart sätt utöver eller som ett alternativ till att välbefinnandeapplikationens tekniska prestationsmiljö i sin helhet administreras av tillverkaren av välbefinnandeapplikationen. 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.

Många av de tekniska skyddsåtgärderna genomförs via de krav på identifiering, autentisering och åtkomsthantering som ställs på välbefinnandeapplikationen. Tekniska skyddsåtgärder för plattformstjänster från tredje part är bland annat kryptering av datakommunikation och informationslagring eller användning av slutna nätverk. Uppgifter om välbefinnande som ska förvaras i externa tjänster ska med beaktande av uppgifternas känslighet krypteras tillräckligt starkt så att endast tillverkaren av en välbefinnandeapplikation har de nycklar som behövs för att dekryptera uppgifterna. Avtalsmässigt ska man se till att alla aktörer som deltar i behandlingen av uppgifter och tillverkningen av en välbefinnandeapplikation agerar tillräckligt enhetligt för att skydda uppgifterna om välbefinnande.

10. Handledning och rådgivning

Institutet för hälsa och välfärd ger på begäran råd och handledning om tillämpningen av denna föreskrift. Närmare information om de väsentliga kraven, certifieringsprocessen och specificeringen av välbefinnandeapplikationer finns på webbplatsen Kanta.fi och THL:s webbplats.

11. Ikraftträdande

Denna föreskrift träder i kraft den 16 februari 2022 och gäller tills vidare.

Förfaranden och krav enligt denna föreskrift iakttas vid certifieringen och registreringen av välbefinnandeapplikationer genast när föreskriften har trätt i kraft. Kraven enligt föreskriften börjar gälla för alla välbefinnandeapplikationer avsedda för produktion av tjänster den 1 januari 2023. Innan dess ska alla välbefinnandeapplikationer som används för produktion av tjänster certifieras med godkänt resultat och registreras. En välbefinnandeapplikation som uppfyllt de tidigare kriterierna för godkännande kan vara ansluten till informationsresursen för egna uppgifter tills kraven för produktionsanvändning börjar gälla (1.1.2023). Innan dess ska applikationen certifieras och registreras i enlighet med denna föreskrift.

Denna föreskrift kan ändras genom uppdatering, eller en ny föreskrift kan ges (och den tidigare upphävas), när man börjar tillämpa de övergångsbestämmelser i 52 § i lagen om kunduppgifter som påverkar en välbefinnandeapplikation. Dessa är bland annat 13 § 2 mom., 20 § 4 mom. och 21 § 4 mom i lagen om kunduppgifter.

Sirpa Soini
Direktör för Informationsförmedlarna

Jarmo Kärki
Enhetschef

Sändlista

Folkpensionsanstalten
Social- och hälsovårdsministeriet
Finansministeriet
Tillstånds- och tillsynsverket för social- och hälsovården Valvira
Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea
Transport- och kommunikationsverket Traficom
Bedömningsorgan för informationssäkerhet
Regionförvaltningsverken
Healthtech Finland
Finlands Kommunförbund rf
HL7 Finland Personal Health SIG
Dataombudsmannens byrå

Denna föreskrift har publicerats i myndigheternas föreskriftssamlingar

(FINLEX ® – Myndigheternas föreskriftssamlingar: Institutet för hälsa och välfärd) och finns på

registratorskontoret vid Institutet för hälsa och välfärd samt på

Internet-adressen

https://thl.fi/sv/web/informationshantering-inom-social-och-halsovarden/foreskrifter-och-specifikationer/foreskrifter