Informationsförmedlare
Information och styrning av informationshanteringen 3.5.2024

FÖRESKRIFT 4/2024 BILAGA 2: ANMÄLAN OM ÄNDRINGAR I INFORMATIONSSYSTEM OCH VÄLBEFINNANDEAPPLIKATIONER SOM HÖR TILL KLASS A

I denna bilaga beskrivs de ändringar i ett informationssystem och en välbefinnandeapplikation som tidigare samtestats eller godkänts vid en bedömning av informationssäkerheten som ska anmälas till FPA och bedömningsorganet för informationssäkerhet. Bilagan sammanställer och preciserar förfarandena vid ändringar av system och applikationer enligt lagen om kunduppgifter och föreskrift 4/2024.

Enligt 82 § i lagen om kunduppgifter ska Tillstånds- och tillsynsverket för social- och hälsovården underrättas om väsentliga ändringar i informationssystem och välbefinnandeapplikationer. I denna bilaga beskrivs inte de väsentliga ändringar som ska anmälas till Valvira, utan endast anmälningar till FPA och bedömningsorganet för informationssäkerhet om ändringar som gäller påvisande av överensstämmelse med kraven samt bevarande. Valvira kan ge separata anvisningar om anmälan av väsentliga ändringar, antingen på basis av denna bilaga eller på annat sätt. Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska dock iaktta den praxis som beskrivs i föreskrift 4/2024 när registreringen till Valvira och anmälan om ändringar hänför sig till certifieringsprocessen.

Bakgrund och grunder

I lagen om kunduppgifter föreskrivs att betydande ändringar i informationssystem och välbefinnandeapplikationer som hör till klass A ska anmälas till *bedömningsorganet för informationssäkerhet*. Ett nytt intyg över bedömning av informationssäkerhet ska utfärdas om det görs betydande ändringar i informationssystemet eller välbefinnandeapplikationen eller om de väsentliga kraven på informationssäkerhet hos systemet eller applikationen ändras på ett sådant sätt att det förutsätter att informationssäkerhetsintyget förnyas.

Det ska visas vid en samtestning som utförs tillsammans med FPA att de uppgifter i informationssystemen och välbefinnandeapplikationerna som ska registreras i Kanta-tjänsterna är interoperabla med Kanta-tjänsterna och andra klient- och patientdatasystem. Kravet på interoperabilitet gäller också situationer där väsentliga ändringar görs i systemen eller välbefinnandeapplikationerna. Därför föreskrivs i lagen om kunduppgifter att betydande ändringar i informationssystem och välbefinnandeapplikationer som har anslutits till Kanta-tjänsterna också ska anmälas till *FPA*.

Anmälan om ändringar till FPA är inte samma sak som anmälan till samtestning. Ändringsanmälan leder till att FPA bedömer om samtestning behövs. Det är möjligt att anmäla sig till samtestning även i andra situationer än i samband med systemändringar. Producenten av en informationssystemtjänst kan till exempel anmäla sig direkt till samtestning om systemet eller välbefinnandeapplikationen ansluts till en Kanta-tjänst, som det inte tidigare har varit anslutet till, exempelvis förutom receptcentret även till patientdataarkivet, förutom patientdataarkivet även till klientdataarkivet för socialvården eller till datalagret för egna uppgifter, eller förutom klientdataarkivet för socialvården även till patientdataarkivet. Mer information om anmälan till samtestning finns på FPA:s Kanta-sidor.

En förutsättning för samtestning och bedömning av informationssäkerheten är tillverkarens redogörelse för hur kraven på informationssystemets och välbefinnandeapplikationens funktion har implementerats och testats. I redogörelsen används en systemblankett enligt bilaga 4 till THL:s föreskrift 5/2024.

Om informationssystemen, välbefinnandeapplikationerna eller specifikationerna ändras kan man förenkla förfarandena för ny testning eller ny bedömning genom att begränsa ändringarna till vissa funktioner eller innehåll. Till exempel förutsätter implementering av en ny handlingstyp eller ett nytt strukturerat innehåll i systemet inte nödvändigtvis att alla funktioner i anslutning till informationsförmedling testas på nytt

Denna bilaga ersätter bilaga 2 till den tidigare föreskriften 4/2021. Innehållet i bilagan har beretts i myndighetssamarbete (THL, FPA, Valvira, Transport- och kommunikationsverket, SHM, bedömningsorgan för

informationssäkerhet) utifrån enkäter som dessa instanser fått samt erfarenheter från certifieringsprocessen. Termerna som används i bilagan motsvarar termerna i lagen om kunduppgifter och i föreskrift 4/2024.

Förfarandet vid anmälan om ändringar

Producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ska underrätta FPA och bedömningsorganet för informationssäkerhet om väsentliga ändringar i system eller välbefinnandeapplikationer som hör till klass A i enlighet med 82 § i lagen om kunduppgifter, THL:s föreskrift 4/2024 och denna bilaga. På basis av anmälan bedömer FPA eller bedömningsorganet för informationssäkerhet om ändringarna förutsätter en ny samtestning eller en sådan ny bedömning av informationssäkerheten som medför att ett nytt informationssäkerhetsintyg ska utfärdas för informationssystemet, välbefinnandeapplikationen eller delsystemet.

Om producenten av en informationssystemtjänst är någon annan än den ursprungliga tillverkaren av systemet, ska tillverkaren och producenten av informationssystemtjänsten sinsemellan komma överens om vem som ansvarar för att utarbeta och underrätta om ändringsanmälan. Detsamma gäller en situation där någon annan än den ursprungliga tillverkaren av välbefinnandeapplikationen ansvarar för certifieringen eller registreringen av välbefinnandeapplikationen.

När producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation byts ut måste man se till att kraven på systemet och dess uppdateringar fortfarande uppfylls och att detta finns dokumenterat.

Ändringsanmälan ska åtföljas av en systemblankett som fyllts i enligt THL:s föreskrifter 4/2024 och 5/2024 (föreskrift 5/2024, bilaga 4). Blanketten ska lämnas in till FPA när man gör en ändringsanmälan till FPA för bedömning av behovet av samtestning. Blanketten ska också lämnas in tillsammans med ändringsanmälan till bedömningsorganet för informationssäkerhet för att organet ska kunna avgöra om det är nödvändigt att göra en ny bedömning av informationssäkerheten. *På systemblanketten ska man med anteckningarna i föreskrift 5/2024 anteckna funktioner, datainnehåll och informationssäkerhetskrav som är nya eller som innehåller betydande ändringar och som implementerats i systemet eller välbefinnandeapplikationen eller som uppfylls via systemet. Nya och ändrade väsentliga krav som implementerats i systemet eller välbefinnandeapplikationen måste i blanketten tydligt särskiljas från de väsentliga krav som tidigare verifierats. Den systemblankett som lämnas in till FPA eller bedömningsorganet ska innehålla aktuella uppgifter om versionen av informationssystemet eller välbefinnandeapplikationen. Blanketten ska innehålla aktuella beskrivningar av de väsentliga krav och profiler i enlighet med föreskrift 5/2024 som implementerats i systemversionen i fråga.*

FPA och bedömningsorganet för informationssäkerhet kan ge närmare anvisningar om de blanketter och kontaktkanaler som ska användas vid ändringsanmälningar samt om man redan i samband med ändringsanmälan kan lämna även andra uppgifter eller material till exempel i situationer där det är sannolikt att en ny samtestning eller bedömning av informationssäkerheten behövs.

Om denna bilaga inte innehåller något svar på om det behövs en bedömning av behovet av en ny samtestning, kan man få råd via FPA:s Kanta-tjänster eller THL. Man kan fråga bedömningsorganet eller THL om behovet av en ny bedömning av informationssäkerheten om de regler som beskrivs i bilagan inte är tillämpliga.

Väsentliga ändringar

Betydande ändringar i ett informationssystem eller en välbefinnandeapplikation som hör till klass A2 eller A3 ska anmälas till FPA, som bedömer behovet av en ny samtestning av informationssystemet eller välbefinnadeapplikationen eller behovet av en kompletterande samtestning. Betydande ändringar i ett informationssystem som hör till klass A1 ska inte anmälas till FPA.

Om ett informationssystem eller en välbefinnandeapplikation övergår från klass A1 eller klass B till klass A2 eller A3, inleds en samtestning med FPA på motsvarande sätt som när man ansöker om samtestning för ett nytt system.

Betydande ändringar i ett informationssystem eller en välbefinnandeapplikation som hör till klass A1, A2 eller A3 ska anmälas till bedömningsorganet för informationssäkerhet, som bedömer om det är nödvändigt att göra en ny bedömning av informationssäkerheten för informationssystemet eller välbefinnandeapplikationen.

Om ett informationssystem övergår från klass B till klass A1, A2 eller A3, inleds tillsammans med bedömningsorganet för informationssäkerhet en bedömning av informationssäkerheten på motsvarande sätt som när man ansöker om bedömning av informationssäkerheten för ett nytt system.

De ändringar som beskrivs nedan är sådana ändringar som förutsätter en anmälan till FPA:s Kanta-tjänster för bedömning av behovet av samtestning *samt* en anmälan till bedömningsorganet för informationssäkerhet för att bedömningsorganet ska kunna besluta om det behövs en ny bedömning av informationssäkerheten för systemet.

1. I systemet eller välbefinnandeapplikationen implementeras funktioner på basis av de nationella specifikationerna, och i dessa specifikationer eller i den tillhörande publikationsplanen nämns att ibruktagandet av en specifikation förutsätter en bedömning av behovet av omtestning och förnyelse av informationssäkerhetsintyget.
2. Systemets eller välbefinnandeapplikationens användargrupp eller anslutningsmodell förändras väsentligt i samband med en ny version, till exempel utökas användargruppen från professionella användare till att även omfatta kunder eller patienter inom social- och hälsovårdstjänsterna, eller så börjar systemet användas förutom av privata serviceproducenter även av offentliga serviceproducenter eller tvärtom.
3. Systemets eller välbefinnadeapplikationens användargränssnitt eller funktion förnyas i betydande grad eller så görs betydande ändringar i dem. Sådana ändringar ska anmälas om ändringarna också kan påverka riktigheten hos de uppgifter eller handlingar som skickas till eller hämtas från Kanta-tjänsterna, funktionen hos Kanta-gränssnitten eller meddelandestrukturerna eller sättet på vilket informationssäkerhetskraven uppfylls.
4. Systemet eller välbefinnandeapplikationen ansluts direkt till Kanta-tjänsterna när det tidigare har varit anslutet till Kanta-tjänsterna via informationsförmedlingsservice för kunduppgifter eller via ett annat system som förmedlar uppgifter från Kanta-tjänsterna.
5. Tillsynsmyndigheten, till exempel Valvira, kräver en bedömning av behovet att testa systemet eller en ny version av det på nytt eller en bedömning av om det är nödvändigt att göra en ny bedömning av informationssäkerheten för systemet eller välbefinnandeapplikationen.
6. Tillverkaren av informationssystemet eller välbefinnandeapplikationen eller producenten av informationssystemtjänsten gör betydande ändringar i dokumentationsarrangemangen i anslutning till bedömningskraven för informationssäkerheten eller organiseringen av utvecklingsarbetet med systemet eller välbefinnandeapplikationen (till exempel betydande förändringar i affärsverksamheten såsom en företagsfusion eller ett företagsförvärv, byte av utvecklingsteamet som producerat systemet eller välbefinnandeapplikationen).
7. De väsentliga kraven på system eller välbefinnandeapplikation X har samtestats med godkänt resultat eller godkänts i en bedömning av informationssäkerheten via system eller produkt Y, och system Y ändras så att ändringen kan påverka hur de väsentliga kraven uppfylls i system eller välbefinnandeapplikation X.
8. Betydande brister eller fel som påverkar patient- eller klientsäkerheten påträffas i systemet eller välbefinnandeapplikationen. I fråga om betydande fel ska man särskilt se till att underrätta tillsynsmyndigheten (Valvira) och användarna av systemet eller applikationen.

Betydande ändringar som förutsätter anmälan till FPA:s Kanta-tjänster för bedömning av behovet av samtestning, men som inte förutsätter anmälan till bedömningsorganet för informationssäkerhet är följande typer av ändringar:

9. I systemet eller välbefinnadeapplikationen görs ändringar som påverkar Kanta-gränssnittet, de Kanta-serviceförfrågningar som systemet använder eller meddelande- eller dokumentstrukturerna som används i dessa.

Betydande ändringar som förutsätter anmälan till bedömningsorganet för informationssäkerhet, men som inte förutsätter anmälan till FPA:s Kanta-tjänster för bedömning av behovet av samtestning är följande typer av ändringar:

10. Informationssystemets eller välbefinnandeapplikationens användningsändamål ökar avsevärt till exempel från en enskild tjänsteproducent till ett stort område, eller så stiger informationssystemets risknivå från basnivå till hög nivå på grund av ändringar i systemet eller applikationen eller andra omständigheter som påverkar risknivån. Risknivån fastställs enligt föreskrift 4/2024.
11. I drifts- eller prestationsmiljön för ett system som producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation ansvarar för görs betydande ändringar som påverkar hur de väsentliga kraven på informationssäkerhet i driftsmiljön uppfylls. Ändringen kan till exempel vara sådan att systemet eller en av dess viktiga delkomponenter överförs från miljön för producenten av en social- och hälsovårdstjänst eller producenten av en informationssystemtjänst till en extern producent av plattforms- eller programvarutjänster. Anmälningsbehovet gäller inte installation av ett godkänt system som genomgått en bedömning av informationssäkerheten med godkänt resultat i en ny kundmiljö där kraven uppfylls på motsvarande nivå och med motsvarande förfaranden som i tidigare driftsmiljöer. I de nya bedömningarna av informationssäkerheten bör man dock gå igenom om systemet har installerats i sådana nya driftsmiljöer där riskerna avviker från de tidigare.
12. Betydande brister eller fel som påverkar informationssäkerheten påträffas i systemet eller välbefinnandeapplikationen och korrigeringen av dessa måste säkerställas genom en bedömning av informationssäkerheten. I fråga om betydande fel ska man särskilt se till att underrätta tillsynsmyndigheterna (särskilt Valvira) och användarna av systemet eller välbefinnandeapplikationen.

Systemet eller välbefinnandeapplikationen behöver inte anmälas för bedömning av behovet av en ny bedömning av informationssäkerheten eller behovet av en ny samtestning i följande situationer. Även i dessa situationer måste man dock se till att Valviras register över informationssystem samt FPA:s Kanta-tjänster och bedömningsorganet för informationssäkerhet har aktuella uppgifter om produktnamnen på de system som används i produktion och om systemens tillverkare:

13. Ett system eller en applikation som tidigare testats eller som genomgått en bedömning av informationssäkerheten med godkänt resultat förses med ett nytt innehåll eller en ny funktion som inte påverkar Kanta-gränssnitten eller uppfyllandet av informationssäkerhetskraven, till exempel att en ny statusvy för avdelningens bäddplatser införs i ett sjukhussystem eller att en ny funktion för att visa påminnelser för användarna införs i ett klientdatasystem inom socialvården.
14. Systemets eller välbefinnandeapplikationens försäljningsnamn eller produktnamn ändras, men inga betydande ändringar görs i systemet eller välbefinnandeapplikationen som påverkar Kanta-gränssnitten, informationssäkerhetskraven eller funktionen. Det är tillåtet att uppdatera intyget över bedömning av informationssäkerhet med systemets eller välbefinnandeapplikationens nya produktnamn så att namnen på versioner som är i produktion framgår av intyget och intygets giltighetstid förblir oförändrad.
15. Företagets namn eller FO-nummer ändras, men ändringen påverkar inte företagets produkter, välbefinnandeapplikationer eller informationssystem.
16. Kontaktpersonen för eller kontaktuppgifterna till tillverkaren av informationssystemet eller välbefinnandeapplikationen eller producenten av informationssystemtjänsten ändras vid bedömning av informationssäkerheten eller samtestning.