Informationstjänster
Social- och hälsovårdsinformation och informationshantering 9.12.2021

EXEMPEL PÅ KLASSIFICERINGEN AV SYSTEM

I enlighet med lagen om kunduppgifter delas informationssystem för social- och hälsovården in i klasserna A och B. Dessutom finns det oklassificerad programvara som kan användas inom social- och hälsovården, men som inte är informationssystem avsedda för behandling av patientuppgifter eller klientuppgifter inom socialvården.

Ett informationssystem ska klassificeras enligt lagen om kunduppgifter. THL:s föreskrift 4/2021 och denna bilaga preciserar klassificeringen av systemen. Exemplen i detta dokument preciserar de grundläggande reglerna för fastställandet av klasser som beskrivs i lagen om kunduppgifter och föreskrift 4/2021. I anvisningarna för klassificeringen har man beaktat anvisningarna enligt tidigare författningar, de omständigheter som lyfts fram i lagen om kunduppgifter och dess motivering samt i riksdagens behandling och de frågor och behov av klarläggande som lyfts fram i tillämpningen av tidigare författningar.

Utgångspunkter för klassificeringen

Producenten av en informationssystemtjänst svarar för att informationssystemets användningsändamål fastställs och klassificeras. Klassificeringen ska göras med beaktande av systemets användningsändamål, typen av uppgifter som behandlas i systemet och hur kritiskt systemet är samt social- eller hälsovårdstjänsternas kontinuitet.

Klassificeringen är oberoende av om informationssystemet eller delsystemet också är en medicinteknisk produkt eller till vilken klass av medicintekniska produkter informationssystemet eller delsystemet eller en produkt som är ansluten till det hör enligt EU-förordning 2017/745 om medicintekniska produkter och lag 719/2021 om medicintekniska produkter.

Klassificeringsnivåerna för klassificering av system och verifiering av väsentliga krav är från den lägsta till den högsta (oklassificerad –) B – A1 – A2 – A3. Om ett system uppfyller kriterierna för att höra till en högre klassificeringsnivå ska det klassificeras enligt den högre nivån. Ett informationssystem eller delsystem som ska registreras eller certifieras hör endast till en klass.

Om det i ett enskilt fall är oklart till vilken klass informationssystemet hör, kan THL fatta beslut i ärendet i enlighet med lagen om kunduppgifter.

Bedömning av systemets risknivå och omfattningen av behandlingen av uppgifter

Producenten av en informationssystemtjänst ska bedöma omfattningen av den behandling av kunduppgifter som sker i ett informationssystem och risknivån för den behandling av kunduppgifter som sker via systemet. Bedömningen ska göras i förhållande till systemets användningsändamål. I klass A1 och A2 kan kraven inriktas och verifieras på *basnivå* eller *hög risknivå*. Vid bedömningen av risknivån beaktas följande:

- *omfattningen* av behandlingen av kunduppgifter, dvs. för hur stor grupp av tjänstetillhandahållare (användargruppens omfattning) och hur stor invånarpopulation informationssystemet är avsett att behandla uppgifter samt i vilken utsträckning det behandlar olika typer av kunduppgifter;

- systemets betydelse för klient- och patientsäkerheten och social- och hälsovårdstjänsternas funktion med beaktande av aspekter som rör beredskap och försörjningsberedskap;

- de behandlade kunduppgifternas *art och sensitivitet*, det vill säga känslighetsnivån hos de kunduppgifter som behandlas i systemet för individen som uppgifterna gäller;
    - vid bedömningen av känslighet och skyddsåtgärder beaktas uppgifternas identifierbarhet, uppkomsten och användningen av uppgifter i administrativ verksamhet, vårdverksamhet och verksamhet som anknyter till tjänsternas innehåll samt eventuellt specialskydd av uppgifterna;
- riskerna i samband med *integriteten* hos de uppgifter som produceras för riksomfattande bruk;
- *anslutningsbarheten* till andra informationssystem och systemets betydelse som en del av en större informationssystemhelhet;
- *utkontrakteringsriskerna* i samband med förvaring och behandling av uppgifter samt
- *avtalsrisker*.

Bedömningen av risknivån och de faktorer som ligger till grund för den påverkar bland annat skyddskraven för behandling av kunduppgifter som behandlas via systemet och skyddslösningarna (bland annat uppgifternas identifierbarhet och krypteringen av uppgifter vid överföring eller förvaring av uppgifter). Risknivån påverkar också inriktningen av vissa informationssäkerhetskrav och kravverifieringsnivån vid bedömningen av informationssäkerheten. Omfattningen av behandlingen av uppgifter och risknivån kan också påverka klassificeringen av ett system till exempel om användningsändamålet för ett informationssystem i klass B utvidgas eller om risknivån ökar.

Som stöd för bedömningen kan man använda ett verktyg för riskbedömning som finns som stödmaterial till föreskrifterna. Föreskrift 4/2021 och denna bilaga har företräde i styrningen av klassificeringen i förhållande till riskbedömningsverktyget.

Klass A – allmänt

Till klass A hör system för social- och hälsovården som

a) är anslutna till Kanta-tjänsterna direkt eller via informationsförmedlingsservicen eller som producerar strukturerade handlingar enligt de nationella specifikationerna eller andra datastrukturer som förmedlas till Kanta-tjänsterna

b) ska verifiera att informationssäkerhetskraven uppfylls, eftersom de uppgifter som behandlas i systemet utgör en betydande eller omfattande koncentration av patientuppgifter och/eller klientuppgifter inom socialvården. Skyddandet av koncentrationen förutsätter att kraven verifieras med tanke på den omfattande kundgruppens dataskydd eller säkerställandet av tillgången till social- och hälsovårdstjänster och beredskapen.

Klass A delas i sin tur in i underklasserna A1, A2 och A3. Underklasserna styr på vilken nivå och med vilka förfaranden (olika typer av testning, dokumentation osv.) kraven på systemen ska verifieras vid samtestning eller bedömning av informationssäkerheten.

Ett system som säljs eller marknadsförs som ett system som kan anslutas till Kanta-tjänsterna ska klassificeras i klass A3, A2 eller A1 (även i det fall att den tekniska anslutningen genomförs med hjälp av ett externt delsystem, teknisk Kanta-informationsförmedlingsservice eller en annan leverantörs produkt). Ett system i klass A1 kan ha

egenskaper som implementeras via Kanta-tjänsterna och vid samtestning av dessa stöder man sig på ett system i klass A3 eller A2.

Klass A1 innehåller system som inte kräver samtestning med FPA, men däremot en bedömning av informationssäkerheten och ett informationssäkerhetsintyg. Exempel på system som hör till klass A1:

a) Informationsförmedlingsservice för kunduppgifter, dvs. teknisk Kanta-informationsförmedlingsservice som utnyttjas vid implementeringen av en Kanta-anslutningspunkt för att ansluta andra system till Kanta-tjänsterna så att systemet inte innehåller egenskaper i klass A2 eller A3 och inte heller användargränssnittsegenskaper avsedda för slutanvändare som behandlar kunduppgifter. De krav som informationsförmedlingsservicen uppfyller kan också implementeras i informationssystem som hör till klasserna A2 och A3 i denna föreskrift, men som ändå inte utgör informationsförmedlingsservice.1 Om producenten av en informationssystemtjänst som tillhandahåller informationsförmedlingsservice också är en sådan mellanhand som avses i lagen om kunduppgifter, ska aktören i fråga också uppfylla kraven på en informationssäkerhetsplan enligt föreskrift 3/2021 och utarbeta en informationssäkerhetsplan.

b) System eller delsystem vars interoperabilitetskrav har verifierats via ett annat system, men som omfattas av informationssäkerhetskrav som ska verifieras. Till exempel det primära patientdatasystemet eller klientdatasystemet X för en tillhandahållare av specialitetsspecifika tjänster, där Kanta-samtestning och Kanta-gränssnitt samt en del av informationssäkerhetskraven har uppfyllts och certifierats via ett annat system Y, men de informationssäkerhetskrav som verifieras via gränssnittet eller andra informationssäkerhetskrav som är centrala för användarorganisationen förutsätter att informationssäkerhetskraven i fråga verifieras via system X.

c) System som i stor omfattning behandlar basuppgifter eller administrativa patientuppgifter om en klient inom socialvården i klientens service- eller vårdprocesser, oberoende av om de är anslutna till Kanta-tjänsterna till exempel via ett system i klass A2 eller A3.

d) System som registrerar eller behandlar vårdrelaterade patientuppgifter eller klientuppgifter inom socialvården, oberoende av om de direkt eller indirekt ansluts till Kanta-tjänsterna, om behandlingen av uppgifterna är omfattande och identifierande. Till exempel i) läsare som kombinerar kunduppgifter från Kanta-tjänsterna eller andra informationssystem för kundspecifik granskning som genomförs av yrkesutbildade personer som producerar vård eller service, ii) datapoolsystem eller rapporteringssystem som samlar in och kombinerar uppgifter till kundspecifika vård- och serviceprocesser, om de behandlar kundspecifika identifierade uppgifter för primär användning av personuppgifter, det vill säga för andra ändamål än för sekundär användning enligt lag 552/2019.

e) System som behandlar klient- eller patientuppgifter enligt kriterierna för klass B och där behandlingen av kunduppgifter sker på en hög risknivå.

f) Ärendetjänster inom social- och hälsovården där man behandlar eller producerar kunduppgifter som hör till tjänstetillhandahållarens register och som innehåller gränssnitt eller funktioner för behandling av kunduppgifter som riktas till både anställda och kunder hos en tillhandahållare av social- och hälsovårdstjänster (kan också höra till klass A2 eller A3, om de ansluts till Kanta-tjänsterna).

[1] Informationssystem som hör till klass A2 eller A3 och som genomgår samtestning registreras inte som informationsförmedlingsservice för kunduppgifter. Ett delsystem i informationssystemet kan dock certifieras och registreras separat som Kanta-informationsförmedlingsservice.

Klass A2

Informationssystem i klass A2 kräver FPA:s samtestning och extern bedömning av informationssäkerheten, men de är system som betjänar ett begränsat datainnehåll eller användningsändamål. Systemen är direkt anslutna till Kanta-tjänsterna eller producerar eller utnyttjar handlingar eller datastrukturer som hämtas från Kanta-tjänsterna. Ett system i klass A2 kan inte ensamt uppfylla krav som ställs på en organisation som producerar flera olika social- och hälsovårdstjänster, till exempel i fråga om allt datainnehåll som behövs i verksamheten eller alla skyldigheter i samband med Kanta-tjänsterna. Testningen av systemen och bedömningen av informationssäkerheten ska begränsas till att omfatta systemets användningsändamål och särskilt beakta möjligheten att uppfylla kraven även via andra informationssystem som ansluts till systemet.

Exempel på system som hör till klass A2:

g) System som endast registrerar eller utnyttjar administrativa uppgifter i Kanta-tjänsterna, till exempel system som behandlar fullmakter för köpta tjänster.

h) Separata system som är anslutna till Kanta-tjänsterna och som innehåller vårdinformation från en viss specialitet eller en viss avdelning. Utöver dessa används i organisationen ett ”bassystem” som hör till klass A3 eller andra delsystem som uppfyller motsvarande krav.

i) Delsystem som ansluts till Kanta-tjänsterna och som utför en begränsad funktion eller innehåller vissa administrativa eller vårdrelaterade uppgifter i en modulär systemhelhet.

j) Patientdatasystem eller klientdatasystem inom socialvården som producerar endast vissa typer av journalhandlingar (mindre än 5 olika typer av handlingar eller gränssnitt eller endast datainnehåll inom en viss specialitet eller en viss tjänst). Systemen förmedlar journalhandlingar till Kanta-tjänsterna i CDA-format och klienthandlingar inom socialvården i standardformatet för socialvården.

k) Informationssystem som endast hämtar vissa typer av uppgifter enligt punkt j) i Kanta-tjänsterna, men inte skickar uppgifter till Kanta-tjänsterna.

l) Informationssystem som ansluts till Kanta-tjänsterna och där en riskbedömning visar att behandlingen av kunduppgifter inte är omfattande eller utgör en hög risk. Dessutom uppfyller systemen inte övriga kriterier för tillhörighet till klass A3.

Klass A3

Informationssystem i klass A3 förutsätter FPA:s samtestning och en extern bedömning av informationssäkerheten. System i klass A3 uppfyller på ett heltäckande sätt eller i betydande grad informationssystemkraven för en organisation som producerar social- och hälsovårdstjänster, inklusive kraven i samband med Kanta-tjänsterna. Om ett system uppfyller kriterierna för både klass A2 och A3 hör det till klass A3.

Exempel på system som hör till klass A3:

m) Elektroniska patientjournalsystem som används av en tillhandahållare av social- och hälsovårdstjänster som överför uppgifter till Kanta-tjänsterna eller hämtar uppgifter från Kanta-tjänsterna och som uppfyller alla eller de flesta av tjänstetillhandahållarens skyldigheter när det gäller behandlingen av patientuppgifter och anslutningen till Kanta-tjänsterna.

n) Klientdatasystem för socialvården som används av en tillhandahållare av social- och hälsovårdstjänster som överför uppgifter till Kanta-tjänsterna eller hämtar uppgifter från Kanta-tjänsterna och som uppfyller alla eller de flesta av tjänstetillhandahållarens skyldigheter när det gäller behandlingen av klientuppgifter inom socialvården och anslutningen till Kanta-tjänsterna.

o) Apotekssystem som är anslutna till Kanta-tjänsterna.

p) System avsedda för produktion och granskning av elektroniska recept.

q) System eller delsystem som upphandlas separat och med vilka man kan ansluta andra system till Kanta-tjänsterna och uppfylla väsentliga informationssäkerhetskrav helt eller i betydande grad så att producenten av en informationssystemtjänst även ansvarar för andra system som anslutits via tjänsten.

r) FPA:s Kanta-tjänster, inklusive de Kanta-tjänster som innehåller gränssnitt avsedda för tjänstetillhandahållare eller kunder.

En del av systemen som hör till klass A3 är i enlighet med kapitel 5 i föreskrift 4 *kritiska system i klass A3*, som omfattas av särskilda beredskapskrav för att trygga kontinuiteten i social- och hälsovårdstjänsterna.

Klass B

Till klass B hör informationssystem som är avsedda för behandling av klient- eller patientuppgifter, men som inte är direkt anslutna till Kanta-tjänsterna och som inte omfattas av behov av att verifiera väsentliga informationssäkerhetskrav enligt klass A1. Informationssystem i klass B ska implementera och uppfylla de väsentliga krav som ställs på dem, varav en del härrör direkt från lagstiftningen (se till exempel bilaga 3g i föreskrift 5/2021), även om det inte finns någon skyldighet att utföra en extern bedömning av informationssäkerheten eller samtestning för att verifiera kraven. Klass B kan också innehålla programvara som klassificeras som medicintekniska produkter och vars risker till exempel i samband med patientsäkerheten ska hanteras via författningar som gäller medicintekniska produkter.

Även system som hör till klass B ska beaktas i den informationssäkerhetsplan som tjänstetillhandahållaren ansvarar för i enlighet med föreskrift 3/2021.

Exempel på system som hör till klass B:

s) Ett separat system på en sjukhusenhet eller -specialitet som klassificeras som en medicinteknisk produkt. Systemet används i en administrativt, tekniskt och fysiskt skyddad driftsmiljö som begränsas från obehöriga och fungerar tillsammans med medicintekniska produkter inom en viss specialitet. Sjukhusets övriga system skapar journalhandlingar utifrån de uppgifter som systemet i fråga producerar.

t) Ett laboratorie- eller bilddiagnostiseringssystem som används i en administrativt, tekniskt och fysiskt skyddad driftsmiljö som begränsas från obehöriga och vars patientuppgifter registreras i Kanta-tjänsterna via ett annat system som hör till klass A2 eller A3.

u) Ett system som producerar enskilda dataelement för patientuppgifter eller klientuppgifter inom socialvården, och av dessa skapas patient- eller klienthandlingar via gränssnitt eller så förmedlas de till Kanta-tjänsterna via andra system.

v) Ett system som använder enskilda dataelement för patientuppgifter eller klientuppgifter inom socialvården, varav en del kan härstamma från gränssnitten i Kanta-tjänsterna och anslutna system eller från de handlingar som genereras av Kanta-tjänsterna.

w) Ett system som utnyttjar ett informationssystem eller delsystem i klass A3 för att ansluta till Kanta-tjänsterna och för vars del alla väsentliga krav i klass A uppfylls och verifieras via informationssystemet i fråga.

Oklassificerade program och applikationer

Informationssystem som hör till klass A eller B är enligt definitionen i lagen om klientuppgifter informationssystem som planerats för behandling av kunduppgifter inom social- och hälsovården. Inom social- och hälsovårdstjänsterna kan man använda programvara och applikationer som inte är informationssystem avsedda för behandling av klient- och patientuppgifter. Även när denna programvara används ska dock kunduppgifternas dataskydd och informationssäkerhet tillgodoses i enlighet med de lagar som gäller behandlingen av person- och kunduppgifter och andra lagar, till exempel utifrån åtgärderna i tjänstetillhandahållarens informationssäkerhetsplan.

Egenskaperna hos sådana oklassificerade program som beskrivs nedan kan också ingå i informationssystem i klass A eller B, varvid dessa egenskaper och kraven som de omfattas av granskas som en del av informationssystemet i fråga.

Exempel på oklassificerade program och applikationer:

- Allmänna ordbehandlings- eller kontorsprogram som även kan användas för behandling av klient- och patientuppgifter.

- Sjukhusets eller en annan tjänsteproducents administrativa stödsystem som används i en skyddad miljö och vars centrala användningsändamål inte är behandling av klient- eller patientuppgifter, även om de kan innehålla vissa kunduppgifter. Till exempel ett måltidsbeställningssystem, ett materialförvaltningssystem eller organisationens system för hantering av användarnas åtkomsträttigheter med vilket man inte behandlar sekretessbelagda klient- eller patientuppgifter och vars uttryckliga användningsändamål inte är behandling av klient- eller patientuppgifter.

- Kund- eller kommunfaktureringssystem vars användningsändamål inte är behandling av sekretessbelagda klient- eller patientuppgifter.

- Allmänna nät- och molntjänster för slutanvändare när de inte självständigt bildar ett informationssystem eller delsystem som är avsett för behandling av kunduppgifter.

- Allmänna databas-, applikationsserver-, integrationsplattforms- eller andra infrastrukturprodukter, om de inte fungerar som informationsförmedlingsservice för kunduppgifter, självständigt bildar ett informationssystem eller fungerar som en del av ett informationssystem. Producenten av en informationssystemtjänst ansvarar dock för att anmäla och verifiera de väsentliga kraven på ett informationssystem som hör till klass B eller A, även då en del av de väsentliga kraven på systemet uppfylls via en allmän plattform eller en plattform som administreras av en tredje part.

- System eller applikationer som används för kommunikation och vars användningsändamål inte omfattar hantering eller behandling av klient- eller patientuppgifter enligt tillverkarens specifikationer.

- Programvara som används för styrning och drift av en medicinteknisk produkt (CE-märkt) och vars riskhantering följer bestämmelserna för medicintekniska produkter.

- Informationssystem eller informationssystemtjänster avsedda för sekundär användning av klient- och patientuppgifter som behandlar anonymiserade eller icke-identifierade klient- eller patientuppgifter eller klient- eller patientuppgifter som behandlas som sammanfattningar på befolkningsnivå, till exempel tjänster för beslutsstöd, patientgrupperingstjänster eller lednings- eller rapporteringssystem som inte behandlar kundernas identifikationsuppgifter eller visar eller avslöjar sådana uppgifter för användaren. Om systemets användningsändamål dessutom är att behandla identifierbara klient- eller patientuppgifter som en del av produktionen eller ordnandet av de tjänster som kunden tillhandahålls, och en enskild kund kan identifieras med uppgifterna, hör dock systemet till klass B eller A.

- Allmänna ärendehanteringssystem som tillverkaren inte har avsett särskilt för behandling av klient- eller patienthandlingar inom social- eller hälsovården och uppgifterna i dem, och som inte innehåller egenskaper som gör att systemen ansluts till Kanta-tjänsterna, även om man skulle behandla uppgifter om klientrelationer inom social- och hälsovårdstjänsterna med systemen.