Datainspektionens vägledning

Diarienr: DI-2020-11495
Beslutsdatum: 2020-12-01

Behovs- och riskanalys inom hälso- och sjukvården - en vägledning

Innehåll

Postadress: Box 8114, 104 20 Stockholm
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00

Inledning

Datainspektionen inledde under våren 2019 tillsyn mot åtta vårdgivare inom hälso- och sjukvården i syfte bland annat att undersöka om tilldelning av behörigheter i vårdgivarnas respektive journalsystem har föregåtts av behovs- och riskanalyser. Granskningarna omfattade också hur tilldelningen av behörigheter genomförts och vilka åtkomstmöjligheter de tilldelade behörigheterna ger inom ramen för dels den inre sekretessen enligt 4 kap. patientdatalagen, dels den sammanhållna journalföringen enligt 6 kap. samma lag.

Behovs- och riskanalyser ska ligga till grund för bland annat behörighetstilldelning och är av väsentlig betydelse för att uppgifter om enskilda och deras hälsotillstånd ska skyddas och den personliga integriteten upprätthållas. De centrala och generellt gällande slutsatserna från tillsynerna vad gäller kraven på att genomföra behovs- och riskanalyser sammanfattas i den här vägledningen. Vägledningen syftar till att peka på vikten av att vårdgivare säkerställer att vederbörliga behovs- och riskanalyser sker och att ge stöd till vårdgivare vid genomförandet av sådana analyser inför tilldelning av behörigheter i journalsystem.

Gällande regler och normhierarkin

Dataskyddsförordningen den primära rättskällan

För att skydda den enskildes privatliv finns det EU-gemensamma regler om hur personuppgifter får behandlas. Dataskyddsförordningen, ofta förkortad GDPR[1], infördes den 25 maj 2018 och är den primära rättsliga regleringen vid behandling av personuppgifter. Den innehåller 99 artiklar, som gäller som svensk lagstiftning och kompletteras av 173 beaktandesatser (skäl) som i delar förklarar eller förtydligar avsikten med de olika artiklarna. Bestämmelserna i dataskyddsförordningen gäller vid all behandling av personuppgifter inom hälso- och sjukvården.

Innan dataskyddsförordningen infördes gällde personuppgiftslagen (PUL). Genom PUL infördes 1998 ett EU-direktiv om behandling av personuppgifter i svensk rätt.[2] PUL var sekundär lagstiftning och gällde i den mån inte andra

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/56/EG (allmän dataskyddsförordning).

[2] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

regler rörande personuppgiftsbehandling var tillämpliga. I och med dataskyddsförordningens införande har normhierarkin förändrats på ett centralt sätt när det är frågan om behandling av personuppgifter. Dataskyddsförordningen är istället primär lagstiftning och anger grundläggande regler för all personuppgiftsbehandling. Förordningen reglerar också dataskyddsmyndigheternas roll och ansvar för att övervaka efterlevnaden av förordningen. Det innebär att all svensk lagstiftning, när det är frågan om behandling av personuppgifter, ska ha anpassats efter förordningen och att nationella regler endast kan komplettera och fylla ut dataskyddsförordningen.[3]

När personuppgifter behandlas måste därför i första hand dataskyddsförordningens bestämmelser om skydd för den personliga integriteten beaktas och därefter (med avseende på personuppgiftsbehandlingen) kompletterande nationell lagstiftning, som till exempel patientdatalagen, följas.

Grundläggande principer måste följas och rättslig grund finnas
Dataskyddsförordningen anger i artikel 5 ett antal *grundläggande principer* för behandling av personuppgifter, som alla som omfattas av förordningen och som hanterar personuppgifter måste följa. Principerna rör krav på laglighet, öppenhet, ändamålsbegränsning, korrekthet, uppgiftsminimering och lagringsminimering.[4]

En av de grundläggande principerna rör kravet på säkerhet och innebär att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder. Lämplig säkerhet ska säkerställa exempelvis skydd mot obehörig eller otillåten behandling, förlust, förstöring eller skada genom olyckshändelse.[5]

Även den personuppgiftsansvariges ansvar tydliggörs i dataskyddsförordningen. Den så kallade *ansvarsskyldigheten* innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna efterlevs.[6] Kravet avser dels att säkerställa att behandlingen av personuppgifterna *utförs* i enlighet med dataskyddsförordningen, dels att den personuppgiftsansvarige ska kunna *visa* att behandlingen av personuppgifterna utförs i enlighet med förordningen.

[3] Kompletterande nationell lagstiftning (eller unionsrättslig reglering) förutsätter att det finns bestämmelser i dataskyddsförordningen som medger avvikande eller kompletterande bestämmelser i dataskyddsförordningen.
[4] Artikel 5.1.
[5] Artikel 5.1 f.
[6] Artikel 5.2.

Dataskyddsförordningen och förhållandet till kompletterande nationella bestämmelser

Som nämnts är en av de grundläggande principerna i dataskyddsförordningen laglighet.[7] För att behandlingen ska anses vara laglig krävs det att det finns en rättslig grund.[8] De rättsliga grunderna som kan aktualiseras inom hälso- och sjukvården är vanligen uppgift av allmänt intresse, men även rättslig förpliktelse och myndighetsutövning kan vara aktuella.[9] Samtycke kan som regel inte användas som rättslig grund för behandling av personuppgifter inom hälso- och sjukvården eftersom det råder ett ojämlikt förhållande mellan vårdgivaren och vårdtagaren och ett giltigt samtycke därför inte kan lämnas.[10]

När det är frågan om de rättsliga grunderna rättslig förpliktelse, allmänt intresse respektive myndighetsutövning får medlemsstaterna behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen till nationella förhållanden. Nationell rätt kan närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling.[11] Sådana bestämmelser finns för hälso- och sjukvården i patientdatalagen och annan kompletterande lagstiftning som rör personuppgiftsbehandling inom hälso- och sjukvårdsområdet.

Uppgifter om hälsa utgör känsliga personuppgifter. Behandling av särskilda kategorier av personuppgifter, så kallade känsliga personuppgifter, är som huvudregel förbjuden.

I dataskyddsförordningen finns ett antal undantag som medger när känsliga personuppgifter ändå får behandlas.[12] Känsliga personuppgifter får behandlas inom hälso- och sjukvården om det är nödvändigt för att tillhandahålla hälso- och sjukvård på grundval antingen av unionsrätten eller medlemsstaternas

[7] Artikel 5.1 a.
[8] Rättsliga grunder regleras i artikel 6.
[9] Artikel 6.1 c, e.
[10] Samtycke kan dock många gånger, när personuppgiftsbehandlingen sker utifrån en annan rättslig grund, användas som en integritetshöjande åtgärd.
[11] Artikel 6.2. Dataskyddsförordningen innehåller också ett krav att den grund för behandlingen som avses i punkt 1 c och e *ska* fastställas i enlighet med unionsrätt eller medlemsstaternas nationella rätt. Den rättsliga grunden kan även innehålla särskilda bestämmelse för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.
[12] Artikel 9, 9.2 h.

nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet. En förutsättning är att det finns en reglerad tystnadsplikt.[13]

Behandling av personuppgifter med stöd av de rättsliga grunderna allmänt intresse, myndighetsutövning och rättslig förpliktelse samt behandling av känsliga personuppgifter kräver att det finns stöd för det i kompletterande regler.

Patientdatalagen, patientdataförordningen och Socialstyrelsens föreskrifter innehåller kompletterande nationella bestämmelser
För svenskt vidkommande är såväl grunden för behandlingen som de särskilda villkoren för att behandla personuppgifter inom hälso- och sjukvården reglerade i patientdatalagen[14] och patientdataförordningen[15]. I patientdatalagen anges uttryckligen att lagen kompletterar dataskyddsförordningen.[16]

Av patientdatalagen framgår att lagens syfte är att informationshanteringen inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet.[17] Vidare ska personuppgifter utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Dessutom ska dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem.

De kompletterande bestämmelserna i patientdatalagen syftar till att omhänderta både integritetsskydd och patientsäkerhet. Lagstiftaren har således genom regleringen gjort en avvägning när det gäller hur informationen ska behandlas för att uppfylla såväl kraven på patientsäkerhet som rätten till personlig integritet vid behandlingen av personuppgifter.

Socialstyrelsen har med stöd av patientdataförordningen utfärdat föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40, Socialstyrelsens föreskrifter). Föreskrifterna utgör kompletterande regler som ska tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården.[18]

[13] Artikel 9.3.
[14] Patientdatalagen (2008:355).
[15] Patientdataförordningen (2008:360).
[16] 1 kap. 4 § patientdatalagen.
[17] 1 kap. 2 § patientdatalagen.
[18] 1 kap. 1 § 2 stycket patientdatalagen.

Personuppgiftsansvariges ansvar för säkerheten vid behandling av personuppgifter

Att personuppgiftsansvariga har ett generellt ansvar för att genomföra *lämpliga tekniska och organisatoriska åtgärder* för att säkerställa och kunna visa att behandling av personuppgifter utförs i enlighet med dataskyddsförordningen framgår av de grundläggande principerna i artikel 5 men regleras även i artikel 24 i förordningen. Åtgärderna ska genomföras med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers fri- och rättigheter. Åtgärderna ska ses över och uppdateras vid behov.

Personuppgiftsansvariges mer preciserade ansvar för säkerheten i samband med behandling av personuppgifter regleras i artikel 32 i förordningen. Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Vid bedömningen ska beaktas den senaste utvecklingen, genomförandekostnaderna, behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter, som kan vara av varierande sannolikhetsgrad och allvar. Särskild hänsyn ska tas till de risker som behandlingen medför, i synnerhet för oavsiktlig eller olaglig förstöring, förlust eller ändring eller för obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Dataskyddsförordningen anger således att lämpliga åtgärder ska vara såväl tekniska som organisatoriska och att de ska säkerställa en säkerhetsnivå som är lämplig i förhållande till de risker för fysiska personers rättigheter och friheter som behandlingen medför. Det krävs därför att man som personuppgiftsansvarig dels identifierar de möjliga riskerna för de registrerades rättigheter och friheter, dels bedömer sannolikheten för att riskerna inträffar och allvarligheten om de inträffar. Vad som är ”lämpligt” varierar inte bara i förhållande till riskerna utan även utifrån behandlingens art, omfattning, sammanhang och ändamål. Det har således betydelse för bedömningen vilka tekniska och organisatoriska åtgärder som är lämpliga vad det är för personuppgifter som behandlas, hur många uppgifter det är frågan om, hur många som behandlar uppgifterna, under hur lång tid osv.

Hälso- och sjukvården har stort behov av information i sin verksamhet. Sedan patientdatalagen infördes har en mycket omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarnas storlek som hur många som delar information med varandra har ökat väsentligt. Det är dessutom frågan om känsliga personuppgifter. Uppgifterna rör personer som befinner sig i en beroendesituation då de är i behov av vård. Det är också ofta fråga om många

personuppgifter om var och en av dessa personer och uppgifterna kan över tid komma att behandlas av många personer inom vården. Detta innebär att kraven på säkerheten ökar eftersom bedömningen vad som är lämplig säkerhet, som beskrivits ovan, påverkas av behandlingens art och omfattning.

Här är det också centralt att framhålla att uppgifter som behandlas inom vården ska skyddas såväl mot aktörer utanför verksamheten som mot obefogad åtkomst inifrån verksamheten då riskerna, till exempel för oavsiktlig eller olaglig förstöring, förlust eller för obehörigt röjande eller obehörig åtkomst, även omfattar behandling av aktörer inom verksamheten.

Nationella bestämmelser som kompletterar dataskyddsförordningens krav på säkerhet återfinns främst i 4 och 6 kap. patientdatalagen samt 3 och 4 kap. Socialstyrelsens föreskrifter, HSLF-FS 2016:40.

En behovs- och riskanalys ska genomföras innan tilldelning av behörighet till journalsystem sker

Behovs- och riskanalysen en central organisatorisk säkerhetsåtgärd
Det framgår av 4 kap. 2 § patientdatalagen att vårdgivaren ska bestämma villkor för tilldelning av behörighet för åtkomst till uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Av 4 kap. 2 § Socialstyrelsens föreskrifter följer att vårdgivaren ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Det innebär att nationell rätt föreskriver krav på en lämplig organisatorisk säkerhetsåtgärd som *ska* vidtas innan tilldelning av behörigheter till journalsystem sker.

Att genomföra en behovs- och riskanalys som uppfyller kraven enligt dataskyddsförordningen och nationell lagstiftning är i första ledet frågan om en strategisk analys på strategisk nivå.

Behovsanalysen behöver kompletteras med en bedömning av risken för patienters fri- och rättigheter
Det framgår, som redovisats, av dataskyddsförordningens bestämmelser om säkerhet och framhålls även i förarbetena till patientdatalagen och i Socialstyrelsens föreskrifter att det inte bara är frågan om *behovsanalyser* utan även om *riskanalyser* i vilka man ska ta hänsyn till olika slags risker för

enskilda fysiska personers fri- och rättigheter som kan följa av en alltför vid tillgänglighet avseende vissa slags uppgifter.[19]

Det framgår av dataskyddsförordningens beaktandesatser att bedömningen av hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs om uppgiftsbehandlingen inbegriper en risk eller en hög risk.[20]

Faktorer som bör beaktas vid bedömningen av risken för patienters rättigheter och friheter är bland annat om det är frågan om personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv, om det sker behandling av personuppgifter rörande sårbara fysiska personer – framför allt barn – eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.[21] Även skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier av uppgifter som kan kräva särskilda riskbedömningar.

Åtkomstbegränsning ska ske till vad varje befattningshavare behöver för att kunna utföra sina arbetsuppgifter

Enligt 4 kap. 2 § patientdatalagen ska behörighet för personalens elektroniska åtkomst till uppgifter om patienter *begränsas till vad befattningshavaren behöver* för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården. Däri ligger enligt förarbetena bland annat att behörigheter ska följas upp och förändras eller inskränkas efter hand som ändringar i den enskilde befattningshavarens arbetsuppgifter ger anledning till det.[22] Syftet med bestämmelsen angavs enligt förarbetena vara att ”inpränta skyldigheten för den ansvariga vårdgivaren att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver”. Här kan noteras att förarbetena skrevs långt före dataskyddsförordningen, men att förarbetsuttalandena stämmer väl överens med vad som nu gäller enligt den grundläggande principen om uppgiftsminimering i förordningen.[23]

---

[19] Prop. 2007/08:126 s. 148–149.

[20] Skäl 76. Även skäl 39 och 83 innehåller skrivningar som ger vägledning om den närmare innebörden av dataskyddsförordningens krav på säkerhet vid behandling av personuppgifter.

[21] Skäl 75 till dataskyddsförordningen.

[22] Prop. 2007/08:126 s. 148–149. Bestämmelsen i 4 kap. 2 § HSLF-FS 2016:40 motsvarar i princip 8 § vårdregisterlagen.

[23] Artikel 5.1 c.

Enligt förarbetena till patientdatalagen bör avgörande för beslut om behörighet för till exempel olika kategorier av hälso- och sjukvårdspersonal till elektronisk åtkomst till uppgifter i patientjournaler vara att behörigheten ska begränsas till vad befattningshavaren behöver för ändamålet en god och säker patientvård. Förarbetena framhåller att en mer vidsträckt eller grovmaskig behörighetstilldelning bör – även om den skulle ha poänger utifrån effektivitetssynpunkt – anses som en obefogad spridning av journaluppgifter inom en verksamhet och bör inte accepteras. Idag strider en alltför vid behörighetstilldelning mot den grundläggande principen om uppgiftsminimering

Olika behörighetsnivåer och skikt för att begränsa åtkomsten kan behövas
Vid tilldelning av behörighet framgår det av förarbetena till patientdatalagen bland annat att det ska finnas olika behörighetskategorier i journalsystemet.[24] Ju mer omfattande ett informationssystem är, desto fler *behörighetsnivåer* måste det finnas.

Uppgifter bör enligt förarbetsuttalanden också *lagras i olika skikt* så att mer känsliga uppgifter kräver aktiva val eller annars inte är lika enkelt åtkomliga för personalen som mindre känsliga uppgifter. Här kan noteras att användning av aktiva val inte i sig utgör en sådan begränsning av behörighet som avses i 4 kap. 2 § patientdatalagen. Denna bestämmelse kräver att behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, det vill säga endast de som har behov av uppgifter ska ha åtkomstmöjlighet till dem. För en medarbetare som ska ha åtkomstmöjligheter till vissa, särskilt känsliga, uppgifter ska dock aktiva val användas som en integritetshöjande åtgärd, genom att säkerställa att det krävs medvetna ställningstaganden innan åtkomst sker till uppgifterna.

När det gäller personal som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad torde det för flertalet befattningshavare enligt förarbetena räcka med tillgång till uppgifter som endast indirekt kan härledas till enskilda patienter. Elektronisk åtkomst till kodnycklar, personnummer och andra uppgifter som direkt pekar ut enskilda patienter bör på detta område, enligt förarbetena, kunna vara starkt begränsad till enstaka personer.

När en behovs- och riskanalys saknas inför tilldelning av behörighet i ett journalsystem inom hälso- och sjukvården, saknas grunden för att den

[24] Prop. 2007/08:126 s. 148-149.

personuppgiftsansvarige på ett lagligt sätt ska kunna tilldela sina användare en korrekt behörighet. Den personuppgiftsansvarige är ansvarig för, och ska ha kontroll över, den personuppgiftsbehandling som sker inom ramen för verksamheten. Att tilldela användare en vid åtkomst till journalsystem, utan att denna grundas på en utförd behovs- och riskanalys, innebär att den personuppgiftsansvarige inte har tillräcklig kontroll över den personuppgifts-behandling som sker i journalsystemet och heller inte kan visa att denne har den kontroll som krävs.

Kravet på en behovs- och riskanalys omfattar både det så kallade inre sekretessområdet och sammanhållen journalföring

Bestämmelserna i 4 kap. patientdatalagen rör den inre sekretessen, det vill säga reglerar hur integritetsskyddet ska hanteras inom en vårdgivares verksamhet och särskilt medarbetares möjligheter att bereda sig tillgång till personuppgifter som finns elektroniskt tillgängliga i en vårdgivares organisation. Som nämnts har en vårdgivare enligt 4 kap. 2 § patientdatalagen att bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Kravet på en behovs- och riskanalys omfattar naturligt medarbetare som finns i vårdgivarens organisation.[25]

Bestämmelserna i 6 kap. patientdatalagen rör sammanhållen journalföring. Detta innebär att en vårdgivare – under de villkor som anges i 6 kap. 2 § patientdatalagen – får ha direktåtkomst till personuppgifter som behandlas av andra vårdgivare för ändamål som rör vårddokumentation. Tillgången till information sker genom att en vårdgivare gör uppgifter om en patient som vårdgivaren registrerar om patienten tillgängliga för andra vårdgivare som deltar i den sammanhållna journalföringen.[26] Av 6 kap. 7 § patientdatalagen följer att bestämmelserna i 4 kap. 2 § även gäller för behörighetstilldelning vid sammanhållen journalföring. Kravet på att vårdgivaren ska utföra en behovs- och riskanalys innan tilldelning av behörigheter i systemet sker, gäller således även i system för sammanhållen journalföring.

[25] Se även prop. 2007/08:126 s. 141ff och s. 239.
[26] Prop. 2007/08:126 s. 247.

Genomförande av behovs- och riskanalysen – sex steg
I avsnittet ges en översiktlig bild av de sex steg som bör följas när behovs- och riskanalysen genomförs.

Behovs- och riskanalysens sex grundläggande steg.

1. Analysera och fastställ verksamhetens behov
2. Identifiera och analysera riskerna för enskildas personliga integritet
3. Identifiera och vidta lämpliga tekniska och organisatoriska åtgärder för att minska riskerna
4. Fastställ, utifrån analyserna, en behörighetsstruktur som stödjer behoven och minimerar riskerna
5. Dokumentera samtliga steg
6. Se kontinuerligt över behörighetsstrukturen och vilka åtgärder som är lämpliga för att minska riskerna.

En behovs- och riskanalys inleds vanligen med en analys av *behoven*. Verksamhetetens behov av åtkomst till uppgifter om patienter för att kunna erbjuda adekvat vård fastställs genom analysen, och ska omfatta vad medarbetare behöver för att kunna fullgöra sina arbetsuppgifter. Behovs- och riskanalysen ska också, som har beskrivits i föregående avsnitt, omfatta en analys av *risker utifrån ett integritetsperspektiv* som kan vara förknippade med en alltför vid tilldelning av behörighet till åtkomst av patientuppgifter.

Riskanalysen ska omfatta en objektiv bedömning av hur sannolik och allvarlig risken för de registrerades rättigheter och friheter är och i vart fall fastställa om det är frågan om en risk eller en hög risk.

Det är genom behovs- och riskanalysen som den personuppgiftsansvarige tar reda på vem som behöver åtkomst, vilka uppgifter åtkomstmöjligheten ska omfatta, vid vilka tidpunkter och i vilka sammanhang eller processer åtkomsten behövs. Samtidigt analyseras vilka risker för den enskildes fri- och rättigheter som behandlingen kan leda till.

Analysen ska sedan leda till att identifiera de *tekniska och organisatoriska åtgärder* som behövs för att dels kunna ge nödvändiga behörigheter, dels säkerställa att ingen tilldelning av behörighet ger vidare åtkomstmöjligheter än den som behovs- och riskanalysen visar är befogad. Dessa tekniska och organisatoriska åtgärder ska sedan genomföras.

Den strategiska analysen ska resultera i en *behörighetsstruktur* som är anpassad till verksamhetens behov såväl på organisatorisk som på individuell nivå. Denna behöver mynna ut i instruktioner om behörighetstilldelning som sedan genomförs. En viktig organisatorisk åtgärd är således att ge anvisning

till de som har befogenhet att tilldela behörigheter om hur detta ska gå till och vad som ska beaktas så att det, med behovs- och riskanalysen som grund, blir en korrekt behörighetstilldelning i varje enskilt fall.

En väl genomarbetad *dokumentation* av gjorda analyser och bedömningar är central för att vårdgivaren ska kunna visa att behörighetstilldelningen är ändamålsenlig och uppfyller de krav som ställs enligt dataskyddsförordningen, patientdatalagen och Socialstyrelsens föreskrifter.

I den mån en verksamhet inte är statisk är behörigheter en färskvara. För att säkerställa en korrekt behörighetstilldelning behöver tilldelade behörigheter löpande kontrolleras och behörighetsstrukturen *löpande hållas uppdaterad*.[27]

Som redan har framhållits utgör en behovs- och riskanalys grunden för att den personuppgiftsansvarige på ett lagligt sätt ska kunna tilldela sina användare en korrekt behörighet. Den är också grunden för den personuppgiftsansvariges kontroll över den personuppgiftsbehandling som sker i journalsystemet och att denne kan visa att denne har den kontroll som krävs.

Konsekvenser av att en behovs- och riskanalys inte har genomförts

Som nämnts är behovs- och riskanalysen grundläggande för att en korrekt behörighetstilldelning ska kunna ske.

Att tilldelningen av behörigheter inte har föregåtts av en behovs- och riskanalys innebär att personuppgiftsansvarige inte har analyserat användarnas behov av åtkomst till uppgifterna, riskerna som denna åtkomst kan medföra och därmed inte heller identifierat vilka åtkomstmöjligheter som är befogade att tilldela användarna. Den ansvarige har i sådana fall inte använt sig av lämpliga åtgärder för att begränsa behörigheter för åtkomst till journalsystemet till enbart vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Om bristen på analys leder till en för snäv tilldelning av behörigheter kan det leda till att personalen inte kan ta del av de uppgifter de behöver för att utföra sitt arbete, vilket utgör en risk för patientens liv och hälsa.

Om bristen på analys istället leder till att användarnas behörigheter inte begränsas till vad som enbart behövs för att de ska kunna fullgöra sina arbetsuppgifter kan det leda till att uppgifterna hamnar i orätta händer och används för otillåtna syften. Att patientens rätt till privatliv inte respekteras

[27] 4 kap. 3 § HSLF-FS 2016:40.

kan påverka patienternas förtroende för vården. Det kan i sin tur påverka såväl patienternas vilja till att dela data, som patienternas vilja att lämna korrekta och fullständiga uppgifter till sin vårdgivare. I en rapport från myndigheten för vård- och omsorgsanalys uppger 8 procent av respondenterna i en enkät att de har hållit inne med uppgifter av oro för över att någon annan skulle kunna se uppgifterna. Ytterligare 8 procent uppger att de övervägt det.[28]

Det är därför väsentligt för hälso- och sjukvården att ha en behörighetsstruktur som har sin grund i väl genomförda behovs- och riskanalyser så att användarna vare sig tilldelas för vida eller för snäva behörigheter för åtkomst till journalsystemen.

Eftersom en behovs- och riskanalys är en föreskriven organisatorisk åtgärd som ska vidtas innan tilldelning av behörigheter sker kan det också leda till rättsliga konsekvenser om personuppgiftsansvarige underlåter att genomföra behovs- och riskanalyser.

Den personuppgiftsansvarige har i ett sådant fall inte använt sig av lämpliga åtgärder för att begränsa användarnas åtkomst till patienternas uppgifter i journalsystemet till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Detta strider såväl mot principen om uppgiftsminimering enligt artikel 5.1 c dataskyddsförordningen och kravet på att säkerställa lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig åtkomst eller otillåten behandling enligt artikel 5.1 f, vilket även framgår av artikel 32, som mot 4 kap. 2 § patientdatalagen och 4 kap. 2 § Socialstyrelsens föreskrifter.

Kan den personuppgiftsansvarige inte visa att bestämmelsen om uppgifts-minimering följs och att den personuppgiftsansvarige vidtagit åtgärder för att kunna säkerställa en lämplig säkerhet för personuppgifterna, har den personuppgiftsansvarige inte heller uppfyllt ansvarsskyldigheten enligt artikel 5.2 i dataskyddsförordningen.

När det skett en överträdelse av dataskyddsförordningen har Datainspektionen ett antal korrigerande befogenheter att tillgå.[29] Tillsynsmyndigheten kan bland annat förelägga den personuppgiftsansvarige att se till att behandlingen sker i enlighet med förordningen och om så krävs på ett specifikt sätt och inom en specifik period.

---

[28] Myndigheten för vård- och omsorgsanalys rapport *För säkerhets skull - Befolkningens inställning till nytta och risker med digitala hälsouppgifter* 2017:10 s. 76-77

[29] Artikel 58.2 a–j i dataskyddsförordningen.

Av artikel 58.2 dataskyddsförordningen följer att tillsynsmyndigheterna, i Sverige Datainspektionen[30], i enlighet med artikel 83 ska påföra sanktionsavgifter utöver, eller i stället för, andra korrigerande åtgärder beroende på omständigheterna i varje enskilt fall. Sanktionsavgifter enligt dataskyddsförordningen är inte obetydliga och ska vara effektiva, proportionella och avskräckande. En eventuell sanktionsavgift kan inom vårdområdet för samma överträdelse medföra helt olika utfall, beroende på om det är frågan om en privat eller offentlig vårdgivare.

Beroende på om överträdelsen avser artiklar som omfattas av artikel 83.4 eller 83.5 i dataskyddsförordningen kan sanktionsavgifterna bli olika höga. Vid överträdelse av mer centrala artiklar kan sanktionsavgifterna för företag uppgå till 20 miljoner EUR eller till max 4 procent av den globala årsomsättningen under föregående budgetår, beroende på vilket belopp som är högst. Alternativt är maxgränsen för sanktionsbeloppet 10 miljoner EUR eller max 2 procent av den globala årsomsättningen under föregående budgetår, beroende på vilket belopp som är högst.

För myndigheter får nationella regler ange att myndigheter kan påföras administrativa sanktionsavgifter.[31] Enligt 6 kap. 2 § dataskyddslagen kan sanktionsavgifter beslutas för myndigheter, men till högst 5 miljoner kronor alternativt 10 miljoner kronor beroende på om överträdelsen avser artiklar som omfattas av artikel 83.4 eller 83.5 i dataskyddsförordningen.

När det är frågan om överträdelser av grundläggande principer och känsliga personuppgifter aktualiseras den högre skalan av sanktionsavgifterna.[32]

Av artikel 83.2 dataskyddsförordningen framgår de faktorer som Datainspektionen har att beakta för att bestämma om en administrativ sanktionsavgift ska påföras, men också vad som ska påverka sanktionsavgiftens storlek. Av central betydelse för bedömningen av en överträdelses allvar är dess karaktär, svårighetsgrad och varaktighet samt graden av ansvar hos den personuppgiftsansvarige (och personuppgiftsbiträdet) med beaktande av de tekniska och organisatoriska åtgärder som genomförts enligt dataskyddsförordningen.[33]

[30] Från och med den 1 januari 2021 byter Datainspektionen namn till Integritetsskyddsmyndigheten.
[31] Artikel 83.7 dataskyddsförordningen.
[32] Artikel 83.5 a dataskyddsförordningen.
[33] Bland annat artikel 32 dataskyddsförordningen.

Om det är fråga om en mindre överträdelse får tillsynsmyndigheten utfärda en reprimand i stället för att påföra en sanktionsavgift.[34] Att inte genomföra en behovs- och riskanalys inför tilldelning av behörigheter utgör inte en mindre överträdelse.

Det kan sammanfattningsvis konstateras att det är av central betydelse att personuppgiftsansvarige gör en behovs- och riskanalys innan tilldelning av behörigheter sker. Det är frågan om känsliga personuppgifter, ofta stora uppgiftssamlingar, många har tillgång till uppgifterna och risken för de registrerades grundläggande fri- och rättigheter om uppgifter obehörigen röjs är vanligen förhållandevis hög. Avsaknad av en behovs- och riskanalys som har lett till en för bred eller grovmaskig behörighetstilldelning medför vanligen att sanktionsavgift ska utgå.

[34] Skäl 148 till dataskyddsförordningen.