



KLAGANDE

Sahlgrenska Universitetssjukhuset, 232100-0131

Ombud: Chefsjurist Lina Kolsmyr

MOTPART

Integritetsskyddsmyndigheten

ÖVERKLAGAT BESLUT

Integritetsskyddsmyndighetens beslut 2020-12-02, se bilaga 1

SAKEN

Behandling av personuppgifter

FÖRVALTNINGSRÄTTENS AVGÖRANDE

Förvaltningsrätten avslår överklagandet.

YRKANDEN M.M.

Integritetsskyddsmyndigheten (IMY, tidigare Datainspektionen) beslutade den 2 december 2020 att påföra Sahlgrenska Universitetssjukhuset (Sahlgrenska) en administrativ sanktionsavgift om 3,5 miljoner kronor för överträdelser av artikel 5.1 f, 5.2, 32.1 och 32.2 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 95/46/EG (dataskyddsförordningen). IMY beslutade vidare att förelägga Sahlgrenska att se till att erforderliga behovs- och riskanalyser genomförs och dokumenteras för journalsystemen Melior och Nationell patientöversikt, att med stöd av dessa behovs- och riskanalyser tilldela varje användare individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården samt att dokumentera i journalsystemet Meliors loggar så att det där framgår vilka åtgärder som har vidtagits med personuppgifter om en patient. Skälen för beslutet och tillämpliga bestämmelser framgår av bilaga 1.

Sahlgrenska yrkar i första hand att IMY:s beslut ska upphävas och i andra hand att den påförda sanktionsavgiften ska sättas ned.

IMY anser att överklagandet ska avslås.

SKÄLEN FÖR AVGÖRANDET

Vad målet gäller

Målet aktualiserar en rad frågor. Den första frågan som förvaltningsrätten har att ta ställning till är om Sahlgrenska har brutit i sin personuppgiftshandtering och därmed överträtt bestämmelserna i 4 kap. 2 och 3 §§ patientdatalagen (2008:355), 6 kap. 7 § samma lag samt 4 kap. 2 och 9 §§ Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Om förvaltningsrätten kommer fram till att så är fallet måste förvaltningsrätten därefter ta ställning till om detta även kan anses utgöra en överträdelse av artikel 5.1 f, 5.2, 32.1 och 32.2 dataskyddsförordningen och om IMY haft grund för sitt val av ingripande i form av dels en administrativ sanktionsavgift, dels ett föreläggande. Om förvaltningsrätten kommer fram till att IMY haft fog för sitt beslut även i denna del måste slutligen den administrativa sanktionsavgiftens storlek prövas.

Har Sahlgrenska brutit i sin personuppgiftshandtering och därmed överträtt de nationella bestämmelserna?

Har Sahlgrenska genomfört erforderliga behovs- och riskanalyser?

Sahlgrenska har i denna del anfört i huvudsak följande. De risker som sjukhuset har identifierat i risk- och sårbarhetsanalyser beskriver att begränsade behörigheter leder till patientsäkerhetsrisker. Det finns inget hinder i 4 kap. 2 § HSLF-FS 2016:40 att inkludera patientsäkerhetsrisker i behovs- och riskanalysen. Sahlgrenska anser att behörigheter ska tilldelas utifrån en analys av både patient- och integritetsrisker. Av de aktuella bestämmelserna framgår endast att vårdgivarens beslut om behörighetstilldelning ska föregås av en behovs- och riskanalys. Utöver det ställer

lagstiftaren inga krav på vilket sätt behovs- och riskanalysen ska utföras eller vilka behov och risker som ska beaktas. Eftersom detaljerade föreskrifter saknas är det upp till den enskilda vårdgivaren att fylla ut ramlagstiftningen i enlighet med lagstiftarens syfte och intentioner. För att IMY ska kunna bedöma om Sahlgrenska uppfyller de krav som uppställs i data-skyddsförordningen krävs en helhetsbedömning där hela det systematiska informationssäkerhetsarbetet, tekniska förhållanden, interna regler, riktlinjer och rutiner samt utbildning beaktas.

Enligt Sahlgrenskas mening är det de behovs- och riskanalyser som genom organisatoriska och tekniska åtgärder har genomförts som ska beaktas, inte vad enskilda dokument har namngetts till. Utifrån en behovs- och riskanalys har Sahlgrenska gjort bedömningen att det finns ett stort behov av potentiell tillgång och därför har det varit nödvändigt att utforma behörigheterna i journalsystemen utifrån breda behörigheter. Vidare påstår IMY att den riskanalys som Sahlgrenska har beskrivit handlar om en annan riskbedömning än den som avses i HSLF-FS 2016:40. Sahlgrenska anser att det av den samlade dokumentation som visats, risk- och sårbarhetsanalysen, rutinerna för behörighetstilldelning och behörigheternas utformning i sig framgår att Sahlgrenska utformat behörigheterna utifrån en analys av olika risker som kan vara förknippad med alltför vid tillgänglighet.

Förvaltningsrätten gör i denna del följande bedömning.

IMY har i det överklagade beslutet identifierat ett antal krav som IMY menar att regleringen ställer när det kommer till vad en behovs- och riskanalys ska identifiera, exempelvis olika kategorier av uppgifter och olika kategorier av registrerade. Dessa krav anges även i den vägledning som IMY publicerade den 1 december 2020. I förarbetena till patientdatalagen, som IMY hänvisat till i det överklagade beslutet, anges bl.a. att syftet med bestämmelsen är 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. Vidare anges att det inte enbart behövs behovsanalyser. Även riskanalyser måste göras där man tar hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier som kan kräva särskilda riskbedömningar (prop. 2007/08:126 s. 148 f.).

Enligt förvaltningsrättens uppfattning gör de nämnda förarbetsuttalandena inte anspråk på att vara en uttömmande uppräknings av vad en behovs- och riskanalys alltid måste innehålla för att anses vara godtagbar. Olika verksamheter har olika behov och olika förutsättningar vilket givetvis också måste innebära att det inte går att fastställa universellt tillämpliga krav. Vad som enligt förvaltningsrättens mening däremot står klart är att en behovs- och riskanalys måste identifiera såväl de behov som olika verksamheter och användare kan ha, som de integritetsrisker som behandlingen kan leda till, inbegripet hur sannolika och allvarliga riskerna är (jfr beaktandeskäl 76 till dataskyddsförordningen). Detta för att behovs- och riskanalysen ska kunna uppfylla sitt syfte, att säkerställa en ändamålsenlig behörighetstilldelning inklusive uppgiftminimering. Detta följer av såväl förarbetena till patientdatalagen som dataskyddsförordningens beaktandesatser och artikel 24, 32.1 och 32.2 dataskyddsförordningen och borde ha varit känt för Sahlgrenska, oaktat den vägledning som IMY publicerade dagen före det överklagade beslutet.

Förvaltningsrätten instämmer i IMY:s bedömning att den process för behovs- och riskanalys som Sahlgrenska hänvisade till vid inspektionsfallet inte utgör en behovs- och riskanalys enligt kraven i 4 kap. 2 § HSLF-FS 2016:40. Denna kan varken anses innehålla en sådan

övergripande behovsinventering eller en sådan riskanalys som bestämmelsen förutsätter. Vidare instämmer förvaltningsrätten i IMY:s bedömning att det inte är en bedömning av en anställds eventuella benägenhet att otillbörligen bereda sig åtkomst till journaluppgifter som avses när det gäller kravet på att identifiera de integritetsrisker som en personuppgiftsbehandling kan leda till. Dokumentet "Tillgänglighet till drift av den elektroniska patientjournalen Melior" kan heller inte anses utgöra en behovs- och riskanalys. Dokumentet saknar nämnda behovsinventering och i fråga om identifiering av integritetsrisker nämns endast mycket kortfattat att en överföring av patientuppgifter som sker via öppna nät kan medföra risker i form av obehörig åtkomst till journalinformation. Enligt förvaltningsrättens mening har dokumentet i övrigt ett tydligt verksamhetsperspektiv snarare än ett integritetsperspektiv.

Även när det gäller risk- och sårbarhetsanalysen, den förenklade behovs- och riskanalysen och dokumentet "Behovs- och riskanalys vid behörighetstilldelning" gör förvaltningsrätten samma bedömning som IMY. Förvaltningsrätten anser därför vid en sammantagen bedömning, och särskilt med beaktande av syftet med en behovs- och riskanalys, att inget av de dokument som Sahlgrenska har presenterat kan anses utgöra en behovs- och riskanalys enligt kravet i 4 kap. 2 § HSLF-FS 2016:40.

Har Sahlgrenska begränsat användarnas behörigheter för åtkomst till journalsystemen till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter?

Förvaltningsrätten anser således att Sahlgrenska brustit i sin personuppgiftshantering såvitt avser skyldigheten att genomföra behovs- och riskanalyser innan tilldelning av behörighet sker. Förvaltningsrätten övergår därefter till att pröva den andra beslutspunkten i det överklagade beslutet, frågan om

Sahlgrenska har begränsat användarnas behörigheter för åtkomst till journal-systemen till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter.

Sahlgrenska har i denna del anfört i huvudsak följande. Sjukhuset har ett särskilt ansvar för specialiserad och högspecialiserad sjukvård, såväl på regional som på nationell nivå. Ofta kan en patient vara aktuell i flera verksamheter och över olika vårdgivar-, vårdenhets- och förvaltningsgränser. För komplexa sjukdomstillstånd finns ofta behov av att engagera olika kompetenser och belysa patientens tillstånd utifrån olika medicinska specialiteter. Samverkan i processen och möjlighet att enkelt ta del av andra specialiteters utredningar och bedömningar är av stor vikt för att kunna ge en god och säker vård även i medicinskt komplexa situationer. Sahlgrenska invänder mot att IMY ensam kan göra denna typ av avvägningar som kan äventyra patientsäkerheten på sjukhuset.

Förvaltningsrätten gör i denna del följande bedömning.

Förvaltningsrätten ifrågasätter i och för sig inte vikten av samverkan mellan exempelvis olika vårdenheter eller medicinska specialiteter. Förvaltningsrätten anser dock att en korrekt behovs- och riskanalys är en grundläggande förutsättning för en ändamålsenlig behörighetstilldelning och att dessa frågor således har ett mycket nära samband. Med hänsyn till de brister som förvaltningsrätten menar att behovs- och riskanalyserna uppvisar kan Sahlgrenska inte anses ha begränsat användarnas behörigheter för åtkomst till journalsystemen till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter. Förvaltningsrätten instämmer i IMY:s bedömning att Sahlgrenska har överträtt bestämmelserna i 4 kap. 2 § patientdatalagen, 6 kap. 7 § samma lag och 4 kap. 2 § HSLF-FS 2016:40.

Har Sahlgrenska brustit i fråga om dokumentation av åtkomst?

Sahlgrenska har i denna del anfört i huvudsak följande. IMY har missuppfattat syftet med kraven på åtkomstkontroll i 4 kap. 3 § patientdatalagen och HSLF-FS 2016:40. Eftersom syftet är att vårdgivaren ska kontrollera om medarbetaren överskridit sin befogenhet, ska loggen innehålla de uppgifter om vidtagna åtgärder som är nödvändiga för att bedöma om åtkomsten varit befogad eller inte. Vidare anser Sahlgrenska att det skulle strida mot principen om uppgiftsminimering enligt artikel 5.1 c dataskyddsförordningen att logga fler uppgifter än vad som krävs enligt patientdatalagen och HSLF-FS 2016:40. Sahlgrenska invänder också mot att loggarna måste finnas i journalsystemet Melior. Det system som Sahlgrenska använder för att dokumentera åtkomst är SysLog. Det finns inte något krav på att loggarna måste finnas i ett visst system.

IMY har i yttrande till förvaltningsrätten anfört i huvudsak följande i denna del. Ordalydelsen i 4 kap. 9 § 1 HSLF-FS 2016:40 kan inte tolkas på annat sätt än att både åtkomsten till, och de åtgärder som vidtagits med uppgifter om en patient, exempelvis radering eller ändring ska dokumenteras. Förutsatt att loggarna innehåller dokumentationen enligt kraven i föreskrifterna har IMY inga synpunkter avseende vilket system som används för lagring och bearbetning av loggarna.

Förvaltningsrätten instämmer i IMY:s bedömning att det av nämnda bestämmelse följer ett krav på loggning av de åtgärder som har vidtagits med uppgifter om en patient och inte bara att kontrollera att en medarbetare berett sig åtkomst till en journal. Redan på denna grund brister Sahlgrenska och har överträtt bestämmelserna i 4 kap. 3 § patientdatalagen och 4 kap. 9 § 1 HSLF-FS 2016:40.

Innebär det nu sagda att Sahlgrenska även ska anses ha överträtt dataskyddsförordningens bestämmelser och har IMY haft grund för sitt val av ingripande i form av dels en administrativ sanktionsavgift, dels ett föreläggande?

De nationella bestämmelsernas förhållande till dataskyddsförordningen

Förvaltningsrätten bedömer således att Sahlgrenska har överträtt bestämmelserna i 4 kap. 2 och 3 §§ patientdatalagen, 6 kap. 7 § samma lag samt 4 kap. 2 och 9 §§ HSLF-FS 2016:40. Frågan aktualiseras därmed huruvida Sahlgrenska i och med detta även kan anses ha överträtt de bestämmelser i dataskyddsförordningen som IMY gör gällande och om myndigheten haft grund för sitt val av ingripande i form av dels en administrativ sanktionsavgift, dels ett föreläggande. Härmed aktualiseras frågan om hur de nationella bestämmelserna förhåller sig till bestämmelserna i dataskyddsförordningen.

IMY har i det överklagade beslutet redogjort för sin uppfattning av de i målet aktuella bestämmelsernas förhållande till dataskyddsförordningen. Förvaltningsrätten gör inte en annan bedömning i denna del. Förvaltningsrätten bedömer således att dataskyddsförordningens systematik, trots att det är en EU-förordning, medger kompletterande nationella bestämmelser i varje enskild medlemsstat, varvid de i målen aktuella svenska bestämmelserna utgör exempel på sådana kompletterande bestämmelser. Enligt förvaltningsrättens mening vinner detta synsätt även stöd i förarbetsuttalanden inför införandet av de svenska anpassningarna till dataskyddsförordningens ikraftträdande. I förarbetena anges bl.a. följande. Styrning och tilldelning och begränsning av behörigheter är sådana tekniska och organisatoriska åtgärder som den personuppgiftsansvarige ska vidta på eget initiativ enligt dataskyddsförordningen. Utan att den personuppgiftsansvariges eget ansvar för att vidta lämpliga åtgärder upphör, kan mer

specifika krav även fastställas i den nationella lagstiftningen med stöd av artikel 6.2 och 6.3 dataskyddsförordningen (prop. 2017/18:171 s. 138). Förvaltningsrättens slutsats i denna blir därför att en konstaterad överträdelse av 4 kap. 2 och 3 §§ patientdatalagen, 6 kap. 7 § samma lag samt 4 kap. 2 och 9 §§ HSLF-FS 2016:40 även kan innebära en överträdelse av 5.1 f, 5.2, 32.1 och 32.2 dataskyddsförordningen.

Betydelsen av andra integritetshöjande åtgärder

Sahlgrenska har även lyft fram ett antal integritetshöjande mekanismer som sjukhuset menar måste vägas in i bedömningen av huruvida lämpliga organisatoriska och tekniska åtgärder har vidtagits, exempelvis anställdas skyldighet att själva sekretessklassa information genom aktiva val, registrerades skydd genom offentlighets- och sekretesslagen (2009:400) och anställdas straffrättsliga och yrkesdisciplinära ansvar. Förvaltningsrätten instämmer dock i IMY:s bedömning att dessa andra åtgärder, som i och för sig har en integritetshöjande effekt, inte kan kompensera för de brister som konstaterats. De i målet aktuella bestämmelserna i dataskyddsförordningen tar sikte på tekniska och organisatoriska åtgärder som det åligger den personuppgiftsansvarige att vidta. Enligt förvaltningsrättens mening kan flera av de integritetshöjande faktorerna som Sahlgrenska har lyft fram inte anses vara sådana tekniska och organisatoriska åtgärder som bestämmelsen tar sikte på utan åtgärder som snarare tar sikte på enskilda individers bidrag till integritetshöjande mekanismer. Förvaltningsrätten anser vid en sammantagen bedömning att Sahlgrenskas underlåtenhet att genomföra behovs- och riskanalyser, att på grundval av dessa begränsa användarnas behörigheter för åtkomst till journalsystemen till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter samt att dokumentera vilka åtgärder som vidtagits med personuppgifter om en patient utgör en så pass allvarlig överträdelse att Sahlgrenska ska anses ha behandlat personuppgifter i strid med artikel 5.1 f, 5.2, 32.1 och 32.2 dataskyddsförordningen.

Finns det laglig grund för att påföra en administrativ sanktionsavgift?

Sahlgrenska har i denna del anfört i huvudsak följande. Av 6 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) framgår att IMY inte får ta ut sanktionsavgift vid andra överträdelser än de som avses i artikel 83 dataskyddsförordningen. Av artikel 83.5 d dataskyddsförordningen följer att sanktioner enligt dataskyddsförordningen kan beslutas för överträdelse av nationella bestämmelser endast i den mån de antagits på grundval av kapitel IX i dataskyddsförordningen.

Såsom redogjorts för gör förvaltningsrätten samma bedömning som IMY i fråga om hur de i målet aktuella nationella bestämmelserna förhåller sig till bestämmelserna i dataskyddsförordningen. Enligt förvaltningsrättens mening bygger Sahlgrenskas argumentation i denna del på ett felaktigt antagande att en överträdelse av nationella bestämmelser kan resultera i en sanktionsavgift enbart med stöd av artikel 83.5 d dataskyddsförordningen. Sahlgrenskas underlåtenhet att genomföra behovs- och riskanalyser och att på grundval av dessa tilldela behörigheter som begränsas till vad som enbart är nödvändigt utgör inte bara en överträdelse av de i målet aktuella nationella bestämmelserna, utan även av artikel 5.1 f, 5.2, 32.1 och 32.2 dataskyddsförordningen. Det föreligger således laglig grund att påföra sanktionsavgift med stöd av artikel 83.4 a och 83.5 a dataskyddsförordningen.

Kan ingripandet stanna vid ett föreläggande?

Sahlgrenska har i denna del anfört i huvudsak följande. Även om det inte förelegat något rättsligt hinder för IMY att ålägga Sahlgrenska en sanktionsavgift kan konstateras att sanktionsavgift endast är en av de korrigerande åtgärder som en tillsynsmyndighet har möjlighet att använda. Först dagen

innan det överklagade beslutet meddelades, dvs. den 1 december 2020, publicerade IMY en vägledning kring hur myndigheten anser att en behovs- och riskanalys ska göras. En sanktionsavgift kan mot denna bakgrund inte anses utgöra en lämplig, proportionell och nödvändig korrigerande åtgärd.

Förvaltningsrätten har bedömt att Sahlgrenska överträtt de grundläggande principerna för behandling i artikel 5 dataskyddsförordningen. Förvaltningsrätten kan konstatera att det har varit fråga om stora uppgiftssamlingar som varit tillgängliga för ett stort antal anställda. Förvaltningsrätten anser vidare att det är särskilt påkallat att beakta vilken kategori av personuppgifter det i många fall varit fråga om, nämligen känsliga uppgifter om enskildas hälsotillstånd och dylikt. Detta bör enligt förvaltningsrättens mening betraktas som en klart försvårande omständighet vid bedömningen av överträdelsens svårighetsgrad. Vidare instämmer förvaltningsrätten i IMY:s bedömning att även den omständigheten att Sahlgrenska år 2015 var föremål för en tillsyn varvid liknande brister då bedömdes föreligga talar för att en administrativ sanktionsavgift ska påföras. Vid en sammantagen bedömning anser förvaltningsrätten att överträdelsens karaktär och svårighetsgrad medför att IMY haft fog för att inte låta ingripandet stanna vid endast ett föreläggande.

Sanktionsavgiftens storlek

De omständigheter som redogjorts för i ovanstående stycke är sådana omständigheter som enligt artikel 83.2 dataskyddsförordningen ska vägas in, inte bara vid beslut om huruvida en sanktionsavgift ska påföras eller inte utan även vid bestämmande av beloppet. Förvaltningsrätten anser att det inte har kommit fram tillräckliga omständigheter som kan sägas tala i förmildrande riktning i sådan mån att den påförda sanktionsavgiften inte framstår som effektiv, proportionell och avskräckande. Förvaltningsrätten bedömer således att den påförda sanktionsavgiften är väl avvägd.

FÖRVALTNINGSRÄTTENS SLUTSATSER

Förvaltningsrätten bedömer sammanfattningsvis att Sahlgrenska har underlåtit att genomföra och dokumentera behovs- och riskanalyser för journalsystemen Melior och Nationell patientöversikt, att med stöd av dessa behovs- och riskanalyser tilldela varje användare individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården och att i loggarna dokumentera så att det framgår vilka åtgärder som har vidtagits med personuppgifter om en patient. Detta innebär att Sahlgrenska har överträtt bestämmelserna i 4 kap. 2 och 3 §§ patientdatalagen, 6 kap. 7 § samma lag samt 4 kap. 2 och 9 §§ HSLF-FS 2016:40 samt artikel 5.1 f, 5.2, 32.1 och 32.2 dataskyddsförordningen. IMY har haft fog för att påföra Sahlgrenska en administrativ sanktionsavgift samt att förelägga Sahlgrenska att åtgärda de påpekade bristerna. Den administrativa sanktionsavgiften framstår som väl avvägd. Överklagandet ska alltså avslås i dess helhet.

HUR MAN ÖVERKLAGAR

Detta avgörande kan överklagas. Information om hur man överklagar finns i bilaga 2 (FR-03).

Anna Önell
Chefsrådmann

Nämndemännen Elisabeth Cedergren, Peter Lotha Altsved och Budh Sharma har också deltagit i avgörandet.

Förvaltningsrättsfiskalen Martin Une-Larsson har varit föredragande.



Beslut
2020-12-02

Diariennr
DI-2019-3840

1 (34)

Styrelsen för Sahlgrenska
Universitetssjukhuset
Blå stråket 5
413 45 Göteborg

FÖRVALTNINGSRÄTTEN
I STOCKHOLM

INKOM: 2020-12-22
MÅLNR: 28436-20
AKTBIL: 4

Tillsyn enligt dataskyddsförordningen och patientdatalagen - behovs- och riskanalys och frågor om åtkomst i journalsystem

Innehåll

Datainspektionens beslut	3
Redogörelse för tillsynsärendet	4
<i>Tidigare granskning av behovs- och riskanalys</i>	5
Vad som framkommit i ärendet	5
Sahlgrenska Universitetssjukhuset har i huvudsak uppgett följande.....	5
<i>Personuppgiftsansvarig</i>	5
<i>Journalsystem</i>	6
Inre sekretess	6
<i>Behovs- och riskanalys</i>	6
<i>Behörighetstilldelning avseende åtkomst till personuppgifter om patienter</i> ..	8
<i>Aktiva val</i>	9
<i>Behovs- och riskanalys</i>	9
<i>Behörighetstilldelning avseende åtkomst till personuppgifter om patienter</i> ..	9
Motivering av beslutet	10
<i>Krav på att göra behovs- och riskanalys</i>	14
Datainspektionens bedömning	16
<i>Sahlgrenska Universitetssjukhusets process för behovs- och riskanalys</i>	19
<i>Dokumentation av åtkomsten (loggar)</i>	27
Val av ingripande	29
<i>Rättslig reglering</i>	29
<i>Föreläggande</i>	30
<i>Sanktionsavgift</i>	31
Bilagor: Bilaga 1 – Hur man betalar sanktionsavgift.....	33
Hur man överklagar.....	34

Datainspektionens beslut

Datainspektionen har vid granskning den 23 april 2019 konstaterat att Styrelsen för Sahlgrenska Universitetssjukhuset (Sahlgrenska Universitetssjukhuset) behandlar personuppgifter i strid med artikel 5.1 f och 5.2 samt artikel 32.1 och 32.2 i dataskyddsförordningen¹ genom att

1. Sahlgrenska Universitetssjukhuset i egenskap av personuppgiftsansvarig inte uppfyller kravet på att det ska ha genomförts en behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemen Melior och Nationell patientöversikt i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) och 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Detta innebär att Sahlgrenska Universitetssjukhuset inte har vidtagit lämpliga organisatoriska åtgärder för att kunna säkerställa och kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.
2. Sahlgrenska Universitetssjukhuset inte begränsar användarnas behörigheter för åtkomst till journalsystemen Melior och Nationell patientöversikt till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Det innebär att Sahlgrenska Universitetssjukhuset inte har vidtagit åtgärder för att kunna säkerställa och kunna visa en lämplig säkerhet för personuppgifterna.
3. Sahlgrenska Universitetssjukhuset inte i Melior har dokumentation av åtkomst (loggar) där det framgår vilka åtgärder som har vidtagits med uppgifter om en patient enligt 4 kap. 3 § patientdatalagen och 4 kap. 9 § (punkt 1) HSLF-FS 2016:40. Det innebär att Sahlgrenska

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 95/46/EG (allmän dataskyddsförordning).

Universitetssjukhuset inte har vidtagit lämpliga organisatoriska åtgärder för att kunna säkerställa och kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.

Datainspektionen beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen och 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning att Sahlgrenska Universitetssjukhuset, för överträdelse av artikel 5.1 f och 5.2 samt artikel 32.1 och 32.2 i dataskyddsförordningen, ska betala en administrativ sanktionsavgift på 3 500 000 (tre miljoner femhundra tusen) kronor.

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Sahlgrenska Universitetssjukhuset att

1. se till att erforderlig behovs- och riskanalys genomförs och dokumenteras för journalsystemen Melior och Nationell patientöversikt och att därefter, med stöd av behovs- och riskanalysen, varje användare tilldelas individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen, 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40.
2. dokumentera i journalsystemet Meliors loggar så att det där framgår vilka åtgärder som har vidtagits med personuppgifter om en patient, i enlighet med artikel 32 i dataskyddsförordningen, 4 kap. 3 § patientdatalagen och 4 kap. 9 § (punkt 1) HSLF-FS 2016:40.

Redogörelse för tillsynsärendet

Datainspektionen inledde tillsyn genom skrivelse den 22 mars 2019 och har på plats den 23 april 2019 granskat om Styrelsens för Sahlgrenska Universitetssjukhuset (nedan kallat Sahlgrenska Universitetssjukhuset) beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Granskningen har även omfattat hur Sahlgrenska

Universitetssjukhuset tilldelat behörigheter för åtkomst till huvudjournalssystemet Melior och NPÖ, och vilka åtkomstmöjligheter de tilldelade behörigheterna ger inom såväl ramen för den inre sekretessen enligt 4 kap. patientdatalagen, som den sammanhållna journalföringen enligt 6 kap. patientdatalagen. Utöver detta har Datainspektionen granskat vilken dokumentation av åtkomst (loggar) som finns i journalsystemen.

Datainspektionen har endast granskat användares åtkomstmöjligheter till journalssystemet, dvs. vilken vårddokumentation användaren faktiskt kan ta del av och läsa. Tillsynen har inte omfattat vilka funktioner som ingått i behörigheten, dvs. vad användaren faktiskt kan göra i journalssystemet (exempelvis utfärda recept, skriva remisser etc).

Tidigare granskning av behovs- och riskanalys

Datainspektionen har tidigare genomfört en tillsyn avseende om Sahlgrenska Universitetssjukhuset hade genomfört en dokumenterad behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Av Datainspektionens beslut med diarienummer 1607-2013, meddelat den 27 mars 2015, framgår att Sahlgrenska Universitetssjukhuset inte uppfyllde kravet på att genomföra en behovs- och riskanalys enligt nämnda föreskrifter, och därför förelades att genomföra en sådan för huvudjournalssystemet.

Vad som framkommit i ärendet

Sahlgrenska Universitetssjukhuset har i huvudsak uppgett följande.

Personuppgiftsansvarig

Sahlgrenska Universitetssjukhuset har uppgett att Styrelsen för Sahlgrenska Universitetssjukhuset är personuppgiftsansvarig för den behandling av personuppgifter som Sahlgrenska Universitetssjukhuset utför i huvudjournalssystemet Melior. Sahlgrenska Universitetssjukhuset har vidare uppgett att Nationell patientöversikt (NPÖ) endast är en läsvy som presenterar information från anslutna system, och att ingen information lagras i NPÖ. Sahlgrenska Universitetssjukhuset är inte personuppgiftsansvarig för information som visas i NPÖ.

Journalsystem

Sahlgrenska Universitetssjukhuset har uppgett att de sedan 1998 använder sig av huvudjournalsystemet Melior inom ramen för den inre sekretessen. Allt ses som inre sekretess inom ramen för Västra Götalandsregionen.

Sedan den 6 maj 2014 består Melior inom Västra Götalandsregionen av en enda databas (GEM), istället för som tidigare 27 stycken. Det gick tidigare att komma åt andra enheters vårddokumentation men det var betydligt mer omständligt, vilket medförde att medarbetarna var motvilliga till att läsa journaler hos andra enheter. De nuvarande indelningen av enheter är desamma som tidigare men numera är det lättare att få åtkomst till andra enheters journaler.

Enligt underlag som Sahlgrenska Universitetssjukhuset inkommit med är 896 401 patienter journalförda i Melior hos Sahlgrenska Universitetssjukhuset. Antalet anställda vid Sahlgrenska Universitetssjukhuset är 16 731 st, och antalet aktiva konton i Melior är 24 638 st. Sahlgrenska Universitetssjukhuset har uppgett att anledningen till att antalet aktiva konton är större än antalet anställda är att Västra Götalandsregionen är en inre sekretess-zon, och att Sahlgrenska Universitetssjukhuset har samarbete med andra förvaltningar inom Västra Götalandsregionen där de anställda har behov av åtkomst till patientinformation vid Sahlgrenska Universitetssjukhuset.

Sahlgrenska Universitetssjukhuset ingår inte i ett system för sammanhållen journalföring genom Melior, men ingår i sammanhållen journalföring genom systemet NPÖ.

Inre sekretess

Behovs- och riskanalys

Vid inspektionstillfället uppgav Sahlgrenska Universitetssjukhuset i huvudsak följande.

När en ny medarbetare anställs görs först en behovsanalys, bestående av en bedömning av vilka system medarbetaren behöver åtkomst till.

Bedömningen görs i två steg: 1) vilket uppdrag personen har och 2) vilka system personen behöver ha åtkomst till för att kunna utföra sitt arbete/uppdrag. På grund av en begränsning i systemet görs ingen

bedömning av vilka uppgifter i Melior som medarbetaren ska kunna ta del av.

Därefter görs en riskanalys som består av en bedömning på individnivå av om personen som ska tilldelas behörighet kommer att följa riktlinjerna för att ta del av uppgifter i Melior. Om så inte är fallet ska personen normalt inte anställas.

Vid inspektionstillfället kan Sahlgrenska Universitetssjukhuset inte uppvisa en analys för personer som anställs och det är oklart om den dokumenteras.

Sahlgrenska Universitetssjukhuset har i synpunkter på inspektionsprotokollet som inkom till Datainspektionen den 27 juni 2019 uppgett att Sahlgrenska Universitetssjukhuset i september 2011 genomförde en omfattande riskanalys, *Tillgänglighet till drift av den elektroniska patientjournalen Melior*, avseende patientsäkerhet, informationssäkerhet och teknisk säkerhet. Utgångspunkten för riskanalysen var vid det tillfället att förenkla åtkomsten till patientdata mellan de olika enheterna inom sjukhuset då Socialstyrelsen ansåg att den uppdelning på olika databaser som förelåg vid tillfället innebar en patientsäkerhetsrisk. 27 databaser sammanfördes till en sjukhusgemensam databas och den generella rollen som tilldelas samtlig personal med behov av tillgång till patientjournalen infördes.

Tidigare granskning av behovs- och riskanalys

Med anledning av Datainspektionens tidigare granskning har Sahlgrenska Universitetssjukhuset inkommit med ett antal dokument, däribland en risk- och sårbarhetsanalys och en så kallad förenklad behovs- och riskanalys med titeln *Behovs- och riskanalys vid tilldelning av individuell behörighet till journalsystem*, vilka uppges ha tagits fram under våren 2019, för att visa hur Sahlgrenska Universitetssjukhuset har agerat efter inspektionens tidigare beslut.

Den 13 september 2019 inkom Sahlgrenska Universitetssjukhuset även med dokumentet *Behovs- och riskanalys vid behörighetstilldelning*, av vilket det framgår att "I vården är patientens liv och hälsa viktigare än integriteten vilken betyder att tillgängligheten och riktigheten väger tyngre än konfidentialiteten ur ett patientsäkerhetsperspektiv. I patientjournalsystemet (Melior) måste medarbetaren göra ett aktivt val för

att kunna ta del av patientinformation från andra vårdenheter-/processer. Vi gör den bedömningen att den funktionen är tillräcklig för att tillgodose kravet på konfidentialitet. Vi anser att det är i enlighet med HSLF-FS 2016:40.

Sahlgrenska Universitetssjukhuset accepterar risken med att konfidentialiteten inte prioriteras lika högt som riktighet och tillgänglighet till dess att Sahlgrenska Universitetssjukhuset har en teknisk eller organisatorisk möjlighet att prioritera upp konfidentialiteten”.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Sahlgrenska Universitetssjukhuset har i huvudsak uppgett följande.

Det finns två olika roller när det gäller tilldelning av läsbehörigheter till Melior; en generell roll som tilldelas alla medarbetare inom hälso- och sjukvården, och en så kallad verksamhetsroll.

När det gäller den generella rollen finns det två olika varianter; en ”generell” och en ”generell inklusive nödåtkomst”. Alla medarbetare inom hälso- och sjukvården har tilldelats en generell roll – med eller utan nödåtkomst.

Skillnaden mellan de olika varianterna är att varianten ”generell inklusive nödåtkomst” tilldelas läkare och sjuksköterskor, och innebär att användaren har möjlighet att öppna spärrade journaler även utanför den egna verksamheten, för det fall att patienten inte kan lämna sitt medgivande. Varianten ”generell” tilldelas övrig vårdpersonal samt sekreterare, det vill säga de användare som inte är läkare eller sjuksköterskor men som ska ha behörighet till Melior.

Med den generella rollen har medarbetaren åtkomst till samtliga enheters vårddokumentation, med undantag för enheten klinisk genetik som inte är inkluderad i de generella behörigheterna. Det finns inga ytterligare begränsningar för åtkomsten i Melior, bortsett från vårddokumentation som patienten själv har spärrat.

Verksamhetsrollen ger åtkomst till spärrad information avseende en viss enhet. En medarbetare måste ha ett uppdrag för att tilldelas verksamhetsrollen och kan endast tilldelas den rollen avseende den enhet

som medarbetaren tillhör. Varje verksamhet har en sådan verksamhetsroll och totalt uppgår antalet sådana verksamhetsroller till ca 60-70 st.

Aktiva val

Sahlgrenska Universitetssjukhuset har under inspektionen förevisat hur behörigheterna ser ut i systemet, och uppgett bland annat följande.

När en medarbetare loggar in i Melior styrs denne till den enhet som medarbetaren tillhör. När medarbetaren är inloggad finns det sex flikar i högerkanten som ger åtkomst till olika delar av den journal som medarbetaren valt att ta del av. Som utgångspunkt visas endast journalen vid den enhet som har valts vid inloggningen, men genom aktiva val kan medarbetaren få åtkomst till andra enheters journaler.

Om en medarbetare är inloggad som sjuksköterska syns inledningsvis endast sjuksköterskors journalanteckningar. Medarbetaren kan emellertid få tillgång till andra yrkeskategoriers journalanteckningar genom att bocka för rutor avseende olika yrkeskategorier. Det finns även möjlighet att bocka för en enda ruta som avser alla yrkeskategorier, och därigenom få del av samtliga yrkeskategoriers journalanteckningar.

Sammanhållen journalföring

Sahlgrenska Universitetssjukhuset deltar i system för sammanhållen journalföring genom NPÖ, och har i huvudsak uppgett följande.

Behovs- och riskanalys

Sahlgrenska Universitetssjukhuset har inte gjort någon behovs- och riskanalys före tilldelning av behörighet i NPÖ.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter

Patienten måste vara inskriven hos Sahlgrenska Universitetssjukhuset i Melior för att medarbetaren ska kunna använda NPÖ.

Åtkomst till NPÖ ges till vårdpersonal, framförallt läkare och sjuksköterskor, och det krävs ett medarbetaruppdrag för att få en sådan behörighet. Som utgångspunkt är det endast läkare och sjuksköterskor som får åtkomst till NPÖ, men andra kategorier kan få åtkomst efter en egen ansökan om behörighet. I sådana fall får medarbetaren söka ett medarbetaruppdrag för sammanhållen journalföring. Tilldelningen av behörigheterna grundar sig på

behov och färre medarbetare har tillgång till NPÖ än till Melior. Till exempel behöver undersköterskor kunna anteckna i journalen i Melior men de behöver inte ha tillgång till NPÖ. De som har behörighet till NPÖ kan se all vårddokumentation som finns där, men aktiva val krävs.

Dokumentation av åtkomsten (loggar)

Sahlgrenska Universitetssjukhuset har uppgett följande.

Den dokumentation som visas vid uttag av åtkomstloggarna i Melior är uppgifter om patienten, vilken användare som har öppnat journalen, vilken del av journalen som har öppnats och klockslag och datum för det senaste öppnandet.

Det framgår inte vid vilken vårdenhet åtgärderna vidtogs eller vilka åtgärder som användaren specifikt har vidtagit. Sahlgrenska Universitetssjukhuset har uppgett att information om vilken enhet användaren är anställd på kan kontrolleras genom en sökning på var användaren är anställd. Olika loggar måste då kombineras med varandra.

Motivering av beslutet

Gällande regler

Dataskyddsförordningen den primära rättskällan

Dataskyddsförordningen, ofta förkortad GDPR, infördes den 25 maj 2018 och är den primära rättsliga regleringen vid behandling av personuppgifter. Detta gäller även inom hälso- och sjukvården.

De grundläggande principerna för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. En grundläggande princip är kravet på säkerhet enligt artikel 5.1 f, som anger att personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Av artikel 5.2 framgår den s.k. ansvarsskyldigheten, dvs. att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i punkt 1 efterlevs.

Artikel 24 handlar om den personuppgiftsansvariges ansvar. Av artikel 24.1 framgår att den personuppgiftsansvarige ansvarar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. 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.

Artikel 32 reglerar säkerheten i samband med behandlingen. Enligt punkt 1 ska den personuppgiftsansvarige och personuppgiftsbiträdet med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (...). Enligt punkt 2 ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

I skäl 75 anges att vid bedömningen av risken för fysiska personers rättigheter och friheter ska olika faktorer beaktas. Bland annat nämns personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

Vidare följer av skäl 76 att 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 huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

Även skälen 39 och 83 innehåller skrivningar som ger vägledning om den närmare innebörden av dataskyddsförordningens krav på säkerhet vid behandling av personuppgifter.

Dataskyddsförordningen och förhållandet till kompletterande nationella bestämmelser

Enligt artikel 5.1 a i dataskyddsförordningen ska personuppgifterna behandlas på ett lagligt sätt. För att behandlingen ska anses vara laglig krävs rättslig grund genom att åtminstone ett av villkoren i artikel 6.1 är uppfyllda. Tillhandahållande av hälso- och sjukvård är en sådan uppgift av allmänt intresse som avses i artikel 6.1 e.

Inom hälso- och sjukvården kan även de rättsliga grunderna rättslig förpliktelse i artikel 6.1 c och myndighetsutövning enligt artikel 6.1 e aktualiseras.

När det är frågan om de rättsliga grunderna rättslig förpliktelse, allmänt intresse respektive myndighetsutövning får medlemsstaterna, enligt artikel 6.2, behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen till nationella förhållanden. Nationell rätt kan närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Men det finns inte bara en möjlighet att införa nationella regler utan också en skyldighet; artikel 6.3 anger att den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med unionsrätten 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.

Av artikel 9 framgår att behandling av särskilda kategorier av personuppgifter (s.k. känsliga personuppgifter) är förbjuden. Känsliga personuppgifter är bland annat uppgifter om hälsa. I artikel 9.2 anges undantagen då känsliga personuppgifter ändå får behandlas.

Artikel 9.2 h anger att behandling av känsliga personuppgifter får ske om behandlingen är nödvändig av skäl som hör samman med bland annat tillhandahållande av hälso- och sjukvård på grundval av unionsrätten eller

medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda. Artikel 9.3 ställer krav på reglerad tystnadsplikt.

Det innebär att såväl de rättsliga grunderna allmänt intresse, myndighetsutövning och rättslig förpliktelse som behandling av känsliga personuppgifter med stöd av undantaget i artikel 9.2 h behöver kompletterande regler.

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 (2008:355), och patientdataförordningen (2008:360). I 1 kap. 4 § patientdatalagen anges att lagen kompletterar dataskyddsförordningen.

Patientdatalagens syfte är att informationshanteringen inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet. Dess syfte är även att personuppgifter ska 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 (1 kap. 2 § patientdatalagen).

Enligt 2 kap. 6 § patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I en region och en kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

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). Föreskrifterna utgör sådana

kompletterande regler, som ska tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården.

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

Krav på att göra behovs- och riskanalys

Vårdgivaren ska enligt 4 kap. 2 § HSLF-FS 2016:40 göra en behovs-och riskanalys, innan tilldelning av behörigheter i systemet sker.

Att det krävs såväl analys av behoven som riskerna framgår av förarbetena till patientdatalagen, prop. 2007/08:126 s. 148-149, enligt följande.

Behörighet för personalens elektroniska åtkomst till uppgifter om patienter ska begränsas till vad befattningshavaren behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården. Däri ligger bl.a. att behörigheter ska följas upp och förändras eller inskränkas efter hand som ändringar i den enskilde befattningshavarens arbetsuppgifter ger anledning till det. Bestämmelsen motsvarar i princip 8 § vårdregisterlagen. Syftet med bestämmelsen är 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. Men det behövs inte bara behovsanalyser. Även riskanalyser måste göras där man tar hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier som kan kräva särskilda riskbedömningar.

Generellt sett kan sägas att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. Avgörande för beslut om behörighet för t.ex. olika kategorier av hälso- och sjukvårdspersonal till elektronisk åtkomst till uppgifter i patientjournaler bör vara att behörigheten ska begränsas till vad befattningshavaren behöver för ändamålet en god och säker patientvård. 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 som sådan inte accepteras.

Vidare bör uppgifter 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. När det gäller personal som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad torde det för flertalet befattningshavare 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 kunna vara starkt begränsad till enstaka personer.

Inre sekretess

Bestämmelserna i 4 kap. patientdatalagen rör den inre sekretessen, dvs. 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.

Det framgår av 4 kap. 2 § patientdatalagen att vårdgivaren ska 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.

Enligt 4 kap. 2 § HSLF-FS 2016:40 ska vårdgivaren 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.

Sammanhållen journalföring

Bestämmelserna i 6 kap. patientdatalagen rör sammanhållen journalföring, vilket innebär att en vårdgivare – under de villkor som anges i 2 § i samma kapitel – får ha direktåtkomst till personuppgifter som behandlas av andra vårdgivare för ändamål som rör vårddokumentation. Tillgången till information sker genom att en vårdgivare gör de uppgifter om en patient som vårdgivaren registrerar om patienten tillgängliga för andra vårdgivare som deltar i den sammanhållna journalföringen (se prop. 2007/08:126 s. 247).

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 även i system för sammanhållen journalföring.

Dokumentation av åtkomst (loggar)

Av 4 kap. 3 § patientdatalagen framgår att en vårdgivare ska se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och systematiskt kontrolleras.

Enligt 4 kap. 9 § HSLF-FS 2016:40 ska vårdgivaren ansvara för att

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient,
2. det av loggarna framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits,
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
4. användarens och patientens identitet framgår av loggarna.

Datainspektionens bedömning

Personuppgiftsansvariges ansvar för säkerheten

Såsom beskrivits ovan ges i Socialstyrelsens föreskrifter vårdgivaren ett ansvar för informationshanteringen inom vården, såsom exempelvis att genomföra en behovs- och riskanalys innan tilldelning av behörigheter i systemet sker. Inom den offentliga hälso- och sjukvården sammanfaller inte alltid begreppet vårdgivare med den personuppgiftsansvarige.

Av såväl de grundläggande principerna i artikel 5, som artikel 24.1 dataskyddsförordningen, framgår det att det är den personuppgiftsansvariga som ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.

Datainspektionen kan konstatera att dataskyddsförordningen i egenskap av EU-förordning är direkt tillämplig i svensk rätt och att det i förordningen anges när kompletterande reglering ska eller får införas nationellt. Det finns exempelvis utrymme att i nationellt reglera vem som är personuppgiftsansvarig enligt artikel 4 dataskyddsförordningen. Det är däremot inte möjligt att ge avvikande reglering gällande den personuppgiftsansvariges ansvar att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Det innebär att Socialstyrelsens föreskrifter som anger att det är vårdgivaren som ska vidta vissa åtgärder, inte förändrar att ansvaret att vidta lämpliga säkerhetsåtgärder vilar på den personuppgiftsansvarige enligt dataskyddsförordningen. Datainspektionen kan konstatera att Sahlgrenska Universitetssjukhuset, i egenskap av personuppgiftsansvarig, är ansvarig för att dessa åtgärder vidtas.

Som tidigare beskrivits ställs det i artikel 24.1 i dataskyddsförordningen ett generellt krav på den personuppgiftsansvarige att vidta lämpliga tekniska

och organisatoriska åtgärder. 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 dataskyddsförordningen.

Säkerheten i samband med behandlingen regleras mer specifikt i artiklarna 5.1 f och 32 i dataskyddsförordningen.

I artikel 32.1 anges det att de lämpliga åtgärderna ska vara såväl tekniska som organisatoriska och 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 identifierar de möjliga riskerna för de registrerades rättigheter och friheter och 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 vad det är för personuppgifter som behandlas, hur många uppgifter det är frågan om, hur många som behandlar uppgifterna osv.

Hälso- och sjukvården har stort behov av information i sin verksamhet. Det är därför naturligt att digitaliseringens möjligheter tillvaratas så mycket som möjligt inom vården. Sedan patientdatalagen infördes har en mycket omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarna storlek som hur många som delar information med varandra har ökat väsentligt. Denna ökning innebär samtidigt att kraven ökar på den personuppgiftsansvarige, eftersom bedömningen vad som är en lämplig säkerhet påverkas av behandlingens omfattning.

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 väldigt många personer inom vården. Detta sammantaget ställer stora krav på den personuppgiftsansvarige.

Uppgifterna som behandlas måste skyddas såväl mot aktörer utanför verksamheten som mot obefogad åtkomst inifrån verksamheten. Det framgår av artikel 32.2 att den personuppgiftsansvarige, vid bedömning av lämplig

säkerhetsnivå, i synnerhet ska beakta riskerna för oavsiktlig eller olaglig förstöring, förlust eller för obehörigt röjande eller obehörig åtkomst. För att kunna veta vad som är en obehörig åtkomst måste den personuppgiftsansvarige ha klart för sig vad som är en behörig åtkomst.

Behovs- och riskanalys

I 4 kap. 2 § Socialstyrelsens föreskrifter (HSLF-FS 2016:40) som kompletterar patientdatalagen finns det angivet, att vårdgivaren ska göra en behovs-och riskanalys innan tilldelning av behörigheter i systemet sker. Det innebär att nationell rätt föreskriver krav på en lämplig organisatorisk åtgärd som *ska* vidtas innan tilldelning av behörigheter till journalsystem sker.

En behovs- och riskanalys ska dels innehålla en analys av behoven, dels en analys av de risker utifrån ett integritetssperspektiv som kan vara förknippade med en alltför vid tilldelning av behörighet för åtkomst till personuppgifter om patienter. Såväl behoven som riskerna måste bedömas utifrån de uppgifter som behöver behandlas i verksamheten, vilka processer det är frågan om och vilka risker för den enskildes integritet som föreligger.

Bedömningarna av riskerna behöver ske utifrån organisationsnivå, där exempelvis en viss verksamhetsdel eller arbetsuppgift kan vara mer integritetskänslig än en annan, men också utifrån individnivå, om det är frågan om särskilda omständigheter som behöver beaktas, såsom exempelvis att det är frågan om skyddade personuppgifter, allmänt kända personer eller på annat sätt särskilt utsatta personer. Även storleken på systemet påverkar riskbedömningen. Av förarbetena till patientdatalagen framgår att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. (prop. 2007/08:126 s. 149). Det är således frågan om en strategisk analys på strategisk nivå, som ska ge en behörighetsstruktur som är anpassad till verksamheten och denna ska hållas uppdaterad.

Regleringen ställer sammanfattningsvis krav på att riskanalysen identifierar

- olika kategorier av uppgifter (exempelvis uppgifter om hälsa),
- kategorier av registrerade (exempelvis sårbara fysiska personer och barn), eller
- omfattningen (exempelvis antalet personuppgifter och registrerade)

- negativa konsekvenser för registrerade (exempelvis skador, betydande social eller ekonomisk nackdel, berövande av rättigheter och friheter),

och hur de påverkar risken för fysiska personers rättigheter och friheter vid behandling av personuppgifter. Det gäller såväl inom den inre sekretessen som vid sammanhållen journalföring.

Risikanalysen ska även innefatta särskilda riskbedömningar exempelvis utifrån om det förekommer skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter (prop. 2007/08:126 s. 148-149).

Risikanalysen ska också omfatta en 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 (skäl 76).

Det är således genom behovs- och risikanalysen som den personuppgiftsansvarige tar reda på vem som behöver åtkomst, vilka uppgifter åtkomstmöjligheten ska omfatta, vid vilka tidpunkter och i vilka sammanhang åtkomsten behövs, och samtidigt analyserar vilka risker för den enskildes fri- och rättigheter som behandlingen kan leda till. Resultatet ska sedan leda till de tekniska och organisatoriska åtgärder som behövs för att säkerställa att inte någon annan åtkomst än den som behovs- och risikanalysen visar är befogad ska kunna ske.

När en behovs- och risikanalys saknas inför tilldelning av behörighet i systemet, saknas grunden för att den 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 risikanalys, innebär att den personuppgiftsansvarige inte har tillräcklig kontroll över den personuppgiftsbehandling som sker i journalsystemet och heller inte kan visa att denne har den kontroll som krävs.

Sahlgrenska Universitetssjukhusets process för behovs- och riskanalys

Sahlgrenska Universitetssjukhuset har inom ramen för tillsynsändet hänvisat till tre olika processer eller dokument som uppges utgöra en behovs- och riskanalys. Beträffande den process som Sahlgrenska Universitetssjukhuset hänvisade till vid inspektionstillfället bestod denna dels i en bedömning av vilka uppdrag personen har och vilka system personen behöver ha åtkomst till, dels i en bedömning på individnivå av om den medarbetare som skulle anställas verkade benägen att ta del av uppgifter i journalsystemet i strid med gällande riktlinjer.

Datainspektionen kan konstatera att Sahlgrenska Universitetssjukhuset inte har genomfört en analys som avser verksamhetens, olika processers och personalkategoriernas behov av att behandla uppgifter. Det som beskrivs är istället enbart en bedömning av vilka system en medarbetare behöver ha åtkomst till.

Den riskanalys Sahlgrenska Universitetssjukhusets beskriver handlar om en annan riskbedömning än den som avses i Socialstyrelsens föreskrifter. I behovs- och riskanalysen ska risker för den enskildes integritet identifieras. Såsom framgår av förarbetena till patientdatalagen kan vissa uppgifter kräva särskild riskbedömning och som exempel anges skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter. Det är alltså inte bedömningen av den anställda som avses i detta sammanhang. Tvärtom har lagstiftaren lyft just att även om hälso- och sjukvården bör kunna ha stort förtroende för sina anställda så är det inte i sig ett tillräckligt skydd,

Den inom hälso- och sjukvården djupt rotade etiska principen om förtroendesekretess för uppgifter som kommer fram i kontakten mellan hälso- och sjukvårdspersonal och patient utgör självklart en stark motkraft mot att skvallra om patienter eller annars sprida uppgifter på ett oacceptabelt sätt bland arbetskamrater. Detsamma gäller i fråga om benägenheten att ta reda på uppgifter om patienter som vårdas på arbetsplatsen men som man inte själv har en yrkesmässig relation till. Med tanke på hälso- och sjukvårdens omfattning och det stora antalet anställd hälso- och sjukvårdspersonal, omkring 300 000 personer bara i kommunernas och landstingens hälso- och sjukvård, kan man emellertid inte utgå från att sådant inte alls förekommer.

Utvecklingen mot gemensamma brett tillgängliga elektroniska journalsystem inom de stora vårdgivarnas verksamhet innebär samtidigt ökade risker för integritetsintrång. Om den ökade potentiella tillgängligheten till journaluppgifter inte hanteras på ett bra sätt så att patienterna kan känna sig säkra på att känslig information inte läses av obehöriga, finns det stor risk för att patienterna väljer att stå utanför system med elektronisk åtkomst.

Det behövs en blandning av preventiva och reaktiva åtgärder för att patientuppgifter inte ska hanteras på ett oacceptabelt sätt (prop. 2007/08:126 s. 147-147).

Den process som Sahlgrenska redogjorde för vid inspektionstillfället utgör således inte en behovs- och riskanalys enligt 4 kap. 2 § HSLF-FS 2016:40.

Dokumentet *Tillgänglighet till drift av den elektroniska patientjournalen Melior*

Sahlgrenska Universitetssjukhuset har i kompletterande information som inkom till Datainspektionen den 27 juni 2019 uppgett att dokumentet *Tillgänglighet till drift av den elektroniska patientjournalen Melior* utgör en behovs- och riskanalys. Dokumentet uppges ha upprättats 2011 och ha som utgångspunkt att förenkla åtkomsten till patientdata mellan de olika enheterna inom sjukhuset. Det kan emellertid konstateras att det av dokumentet framgår att det syftar till att genomföra en riskanalys avseende driften av journalsystemet Melior. I avsnittet "Riskidentifiering och bakomliggande orsaker" hänförs de identifierade riskerna antingen till "Del 1: Patientsäkerhet och verksamhetsperspektiv" eller "Del 2: Teknisk säkerhet med avseende på tillgänglighet till drift".

Beträffande behovsanalysen så innehåller dokumentet ingen analys av vilka uppgifter medarbetarna har behov av för att kunna utföra sina arbetsuppgifter. Beträffande riskanalysen, är exempel på risker som identifieras i Del 1: Patientsäkerhet och verksamhetsperspektiv att "Alla IT-relaterade avvikelser som kan påverka patientsäkerheten rapporteras inte", eller "Fel patient dikteras in på fel diktat". Risker som identifieras i Del 2: Teknisk säkerhet med avseende på tillgänglighet till drift, är t ex "obehörig åtkomst till journalinformation", orsakad genom att "överföring sker via öppna nät". Det är risker ur ett informationssäkerhetsperspektiv, men dokumentet innehåller ingen analys av de risker som kan vara förknippade med en alltför vid tillgänglighet avseende olika typer av personuppgifter.

Dokumentet är således en analys ur ett verksamhetsperspektiv och uppfyller inte kraven på en behovs- och riskanalys ur ett integritetsperspektiv enligt 4 kap. 2 § HSLF-FS 2016:40.

Dokumentet risk- och sårbarhetsanalys

Sahlgrenska Universitetssjukhuset har även med anledning av Datainspektionens förfrågan om vilka åtgärder som vidtagits efter

myndighetens beslut 1607-2013, i vilket Sahlgrenska Universitetssjukhuset förelades att ta fram en dokumenterad behovs- och riskanalys, uppgett att det under våren 2019 genomfördes en behovs- och riskanalys. Sahlgrenska Universitetssjukhuset har inkommit med tre olika dokument, en risk- och sårbarhetsanalys, en så kallad förenklad behovs- och riskanalys med titeln *Behovs- och riskanalys vid tilldelning av individuell behörighet till journalsystem*, och ett dokument med titeln *Behovs- och riskanalys vid behörighetstilldelning* som kan sägas utgöra en kortfattad redogörelse för hur de två andra dokumenten används i verksamheten. Inledningsvis kan det konstateras att dokumenten togs fram först fyra år efter Datainspektionens föreläggande. Därtill utgör inget av de inlämnade dokumenten en behovs- och riskanalys utifrån ett integritetsperspektiv.

Beträffande risk- och sårbarhetsanalysen så är det en analys som ska utföras enligt lagstiftningen om höjd beredskap och krisberedskap². En sådan sker för andra ändamål och är inte detsamma som en behovs- och riskanalys enligt i 4 kap. 2 § HSLF-FS 2016:40.

Det framgår av risk- och sårbarhetsanalysen att en åtgärd för att hantera en alltför vid behörighet ska vara att genomföra en förenklad behovs- och riskanalys vid behörighetstilldelning. Dokumentet fastställer således att en behovs- och riskanalys ska göras, men utgör inte i sig en sådan. Dokumentet innehåller ingen analys av vilka uppgifter medarbetarna har behov av i journalsystemet för att kunna utföra sina arbetsuppgifter. Det finns delar som berör risken för den enskildes integritet, men de så kallade identifierade konsekvenserna utgör inte en analys av risker i det aktuella fallet utan snarare ett konstaterande av fakta, såsom t ex att en konsekvens av att det inre sekretessområdet är omfattande är att "VGR har många medarbetare vilken kan leda till att behörigheterna blir för vida, vilket ger medarbetarna mer behörighet än de behöver". I vissa delar innehåller dokumentet identifierade risker som emellertid inte tar sikte på skyddet för den enskildes integritet; till exempel konstateras att en konsekvens av att medarbetarna inte känner till vad som gäller vid åtkomst till patientuppgifter är att "patienter vid begäran om loggutdrag kan se att obehörig tittat i journal, bad will för SU".

² Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Sammanfattningsvis kan Datainspektionen konstatera att dokumentet inte innehåller analyser av behovet av tillgång till personuppgifter eller de risker för den enskildes integritet som uppkommer genom en alltför vid behörighetstilldelning, och därmed inte uppfyller kraven på en behovs- och riskanalys ur ett integritetsperspektiv enligt 4 kap. 2 § HSLF-FS 2016:40.

Den förenklade behovs- och riskanalysen

Beträffande den förenklade behovs- och riskanalys som Sahlgrenska i risk- och sårbarhetsanalysen fastställer ska göras vid behörighetstilldelning kan det inledningsvis konstateras att det inte är förenligt med i 4 kap. 2 § HSLF-FS 2016:40 att enbart utföra en förenklad behovs- och riskanalys. Vidare består dokumentet av en lista med 14 frågor som ska besvaras med ja eller nej, såsom t ex ”känner medarbetaren till att datorn inte får lämnas olåst, utan uppsyn?”. Datainspektionen kan konstatera att det snarare är frågan om ett dokument som ska användas för att skapa förutsättningar för en god informationssäkerhet på individnivå. Det är en organisatorisk åtgärd för att säkerställa en lämplig säkerhetsnivå, men det är inte en analys av behovet av tillgång till personuppgifter eller vilka risker för den enskildes integritet som uppkommer genom en alltför vid behörighetsstyrning. Därmed uppfyller inte heller detta dokument kraven på en behovs- och riskanalys ur ett integritetsperspektiv enligt 4 kap. 2 § HSLF-FS 2016:40.

Dokumentet Behovs- och riskanalys vid behörighetstilldelning

Sahlgrenska Universitetssjukhuset har även lämnat in ett dokument i vilket det kortfattat redogörs för arbetet med behovs- och riskanalys. Dokumentet beskriver kortfattat hur risk- och sårbarhetsanalysen och den förenklade behovs- och riskanalysen används i verksamheten, och hur Sahlgrenska Universitetssjukhuset prioriterar riktighet och tillgänglighet framför konfidentialitet. Dokumentet innehåller inga analyser av behovet av tillgång till personuppgifter eller de risker för den enskildes integritet som uppkommer genom en alltför vid behörighetstilldelning, och uppfyller således inte kraven på en behovs- och riskanalys ur enligt 4 kap. 2 § HSLF-FS 2016:40. Istället visar dokumentet att Sahlgrenska Universitetssjukhuset medvetet prioriterar ned kravet på konfidentialitet.

Datainspektionens sammanfattande bedömning

Såsom angivits ovan ska i en behovs- och riskanalys såväl behoven som riskerna bedömas utifrån de uppgifter som behöver behandlas i verksamheten, vilka processer det är frågan om och vilka risker för den enskildes integritet som föreligger på såväl organisatorisk som individuell nivå. Det är således frågan om en strategisk analys på strategisk nivå, som ska ge en behörighetsstruktur som är anpassad till verksamheten. Den bör mynna ut i instruktioner om behörighetstilldelning men det är inte instruktionerna till den som tilldelar behörigheter som är analysen.

Vid Datainspektionens granskning har Sahlgrenska Universitetssjukhuset inte kunnat förevisa någon behovs- och riskanalys- vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen. Sahlgrenska Universitetssjukhusets dokument saknar den grundläggande inventeringen av användarnas behov av åtkomst och analys av risker, och det har heller inte gjorts någon avvägning mellan behov och de faktiska integritetsrisker som personuppgiftsbehandlingen ger upphov till.

Sammanfattningsvis kan Datainspektionen konstatera att de dokument som har redovisats inte var för sig eller tillsammans uppfyller de krav som ställs på en behovs- och riskanalys och att Sahlgrenska Universitetssjukhuset inte har kunnat visa att de genomfört en behovs- och riskanalys i den mening som avses i 4 kap. 2 § HSLF-FS 2016:40, vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen, enligt 4 respektive 6 kap. patientdatalagen. Detta innebär att Sahlgrenska Universitetssjukhuset inte har vidtagit lämpliga organisatoriska åtgärder i enlighet med artikel 5.1 f och artikel 31.1 och 31.2 för att kunna säkerställa och, i enlighet med artikel 5.2, kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter

Som har redovisats ovan kan en vårdgivare ha ett berättigat intresse av att ha en omfattande behandling av uppgifter om enskildas hälsa. Oaktat detta ska åtkomstmöjligheter till personuppgifter om patienter vara begränsade till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter.

När det gäller tilldelning av behörighet för elektronisk åtkomst enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen framgår det av förarbetena, prop. 2007/08:126 s. 148-149, bl.a. att det ska finnas olika behörighetskategorier i journalsystemet och att behörigheterna ska begränsas till vad användaren

behöver för att ge patienten en god och säker vård. Det framgår även att ”en mer vidsträckt eller grovmaskig behörighetstilldelning bör anses som en obefogad spridning av journaluppgifter inom en verksamhet och bör som sådan inte accepteras.”

Inom hälso- och sjukvården är det den som behöver uppgifterna i sitt arbete som kan vara behörig att få åtkomst till dem. Det gäller såväl inom en vårdgivare som mellan vårdgivare. Det är, som redan nämnts, genom behovs- och riskanalysen som den personuppgiftsansvarige tar reda på vem som behöver åtkomst, vilka uppgifter åtkomsten ska omfatta, vid vilka tidpunkter och i vilka sammanhang åtkomsten behövs, och samtidigt analyserar vilka risker för den enskildes fri- och rättigheter som behandlingen kan leda till. Resultatet ska sedan leda till de tekniska och organisatoriska åtgärder som behövs för att säkerställa att ingen tilldelning av behörighet ger vidare åtkomstmöjligheter än den som behovs- och riskanalysen visar är befogad. En viktig organisatorisk åtgärd är 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.

Som framkommit i ärendet är ca 900 000 patienter journalförda i Melior hos Sahlgrenska Universitetssjukhuset och antalet aktiva konton i Melior är närmare 25 000, vilket överstiger antalet anställda vid Sahlgrenska Universitetssjukhuset som vid inspektionstillfället var närmare 18 000.

Sahlgrenska Universitetssjukhuset har tilldelat de medarbetare som arbetar med hälso- och sjukvård en generell behörighetsroll – med eller utan nödåtkomst – som ger åtkomst till samtliga enheters vårddokumentation, med undantag för enheten klinisk genetik som inte är inkluderad i de generella behörigheterna. Merparten av användarna har således haft faktisk åtkomstmöjlighet till merparten av dessa uppgifter. Det innebär att Sahlgrenska Universitetssjukhuset inte i tillräcklig utsträckning har begränsat användarnas behörigheter för åtkomst till personuppgifter om patienter i journalsystemet Melior.

Därtill kan det konstateras att Sahlgrenska Universitetssjukhuset har gett direktåtkomst till personuppgifter om patienter vid Sahlgrenska Universitetssjukhuset för medarbetare vid andra förvaltningar inom Västra Götalandsregionen.

Åtkomst till personuppgifter i Melior förutsätter att användaren gör aktiva val. Sahlgrenska Universitetssjukhuset har uppgett att de bedömer att funktionen aktiva val är tillräcklig för att tillgodose kravet på konfidentialitet och att det är i enlighet med HSLF-FS 2016:40. Datainspektionen kan emellertid konstatera att patientdatalagen ställer krav på både begränsning av behörigheter och aktiva val. Funktionen aktiva val är därför inte en åtgärd för att kompensera för en utebliven åtkomstbegränsning. Att Sahlgrenska Universitetssjukhuset använder sig av ovanstående aktiva val är en integritetshöjande åtgärd, men utgör inte 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, dvs. endast de som har behov av uppgifterna ska ha åtkomstmöjlighet till dem.

Av förarbetena till patientdatalagen, prop. 2007/08:126, s. 149, framgår att syftet med bestämmelserna är att inpränta skyldigheten för den ansvarige vårdgivaren att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver. Eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden, behöver användarnas åtkomst till uppgifterna i Melior begränsas för att återspegla detta. Av förarbetena framgår dessutom att uppgifter bör 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.

Att tilldelningen av behörigheter inte har föregåtts av en behovs- och riskanalys innebär att Sahlgrenska Universitetssjukhuset inte har analyserat användarnas behov av åtkomst till uppgifterna, riskerna som denna åtkomst kan medföra och därmed inte heller identifierat vilken åtkomst som är befogad för användarna utifrån en sådan analys. Sahlgrenska Universitetssjukhuset har därmed inte använt sig av lämpliga åtgärder, i enlighet med artikel 32, för att begränsa användarnas åtkomst till patienternas uppgifter i journalsystemet.

Beträffande den behandling av personuppgifter som Sahlgrenska Universitetssjukhuset utför inom ramen för den sammanhållna journalföringen i systemet NPÖ kan det inledningsvis konstateras att

Sahlgrenska Universitetssjukhuset har uppgett att Sahlgrenska Universitetssjukhuset inte är personuppgiftsansvarig för den information som visas i NPÖ. Datainspektionen delar inte denna uppfattning. Enligt 2 kap. 6 § patientdatalagen är i en region varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Enligt andra stycket i bestämmelsen omfattar personuppgiftsansvaret även sådan behandling av personuppgifter som vårdgivaren, eller den myndighet i en region eller en kommun som är personuppgiftsansvarig, utför när vårdgivaren eller myndigheten genom direktåtkomst i ett enskilt fall bereder sig tillgång till personuppgifter om en patient hos en annan vårdgivare eller annan myndighet i samma region eller kommun. Sahlgrenska Universitetssjukhuset är således personuppgiftsansvarig för den behandling av personuppgifter som sker när medarbetarna tar del av uppgifter i NPÖ.

När det gäller åtkomst till personuppgifter inom ramen för den sammanhållna journalföringen i systemet NPÖ har ca 7 000 användare vid Sahlgrenska Universitetssjukhuset åtkomst. Datainspektionen kan konstatera att det har gjorts en begränsning vad gäller antalet användare i förhållande till de ca 25 000 som har behörighet i Melior, men det har inte gjorts någon begränsning när det gäller vilken dokumentation som dessa användare kan ta del av i systemet NPÖ.

Detta har i sin tur inneburit att det funnits en risk för obehörig åtkomst och obefogad spridning av personuppgifter dels inom ramen för den inre sekretessen, dels inom ramen för den sammanhållna journalföringen.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att Sahlgrenska Universitetssjukhuset har behandlat personuppgifter i strid med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen genom att Sahlgrenska Universitetssjukhuset inte har begränsat användarnas behörigheter för åtkomst till journalsystemet Melior till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att Sahlgrenska Universitetssjukhuset inte har vidtagit åtgärder för att kunna säkerställa och, i enlighet med artikel 5.2 i dataskyddsförordningen, kunna visa en lämplig säkerhet för personuppgifterna.

Dokumentation av åtkomsten (loggar)

Datainspektionen kan konstatera att loggarna som visar åtkomst i Melior innehåller uppgifter om användarens namn och roll, patienternas identitet, vilken del av journalen som har öppnats (t.ex journal, remisser, intyg – någon av ”de sex flikarna”) och vid vilket datum och klockslag åtgärderna vidtogs. Det framgår inte vid vilken vårdenhet som åtgärden vidtogs eller vilka åtgärder som användaren specifikt har vidtagit. Sahlgrenska har uppgett att information om vilken vårdenhet användaren är anställd på kan kontrolleras genom en sökning på var användaren är anställd. Sahlgrenska menar därför att genom att kombinera olika loggar kan man få fram vid vilken vårdenhet som åtgärden har vidtagits. Varje loggpost i loggarna utgör åtgärden ”öppna journal”. Därutöver framgår det inte vilka åtgärder som användaren har vidtagit med uppgifter om en patient.

Sahlgrenska Universitetssjukhuset har i yttrande som inkom till Datainspektionen den 17 mars 2020 uppgett att de åtgärder som framgår av loggarna är om en medarbetare öppnat journalen, om tillgång till uppgifter skett genom aktivt val och om medarbetaren från journalen har gjort ett uthopp till andra vårdenheter. Sahlgrenska Universitetssjukhuset uppger vidare att dokumentationen i loggarna skapar förutsättningar för att genomföra åtkomstkontroller på ett ändamålsenligt sätt, och att loggarna uppfyller kravet på att logga vilka åtgärder som har vidtagits med uppgifter om en patient.

Det framgår av Socialstyrelsens Handbok vid tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) att ”vårdgivaren ansvarar bland annat för att det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient. Ett aktivt val för att få tillgång till uppgifter om en patient är ett exempel på en åtgärd som ska loggas”.

Datainspektionen konstaterar att syftet med kravet på att åtgärd ska dokumenteras i loggarna inte bara är att kontrollera om en medarbetare berett sig åtkomst journalen, utan även vilka åtgärder som vidtagits med uppgifter om en patient. Den i loggarna dokumenterade åtgärden ”öppna journal” är ett *exempel* på en åtgärd som ska loggas, och därutöver ska även andra åtgärder som vidtas med uppgifter om en patient dokumenteras i loggarna. Andra sådana åtgärder kan vara att personuppgifter upprättats, kopierats, överförts, spärrats, makulerats eller skrivits ut. Syftet med

säkerhetsåtgärden loggar är att besvara frågan vem som gjorde vad, det vill säga vem som vidtog vilken åtgärd, med vilka personuppgifter och när. Detta utgör en viktig del för att den personuppgiftsansvarige ska uppfylla kravet på lämpliga säkerhetsåtgärder för att ha kontroll över personuppgifterna och hur de behandlas. Syftet med säkerhetsåtgärden åtkomstkontroll är att säkerställa att användare inte använder sina behörigheter på fel sätt genom att läsa, ändra eller ta bort information som de inte ska behandla. Att Sahlgrenska Universitetssjukhuset enbart infört dokumentation av åtgärden ”öppna journal”, är således inte tillräckligt för att uppfylla kravet i 4 kap. 9 § (punkt 1) HSLF-FS 2016:40 på att det av dokumentationen av åtkomsten ska framgå vilka åtgärder som har vidtagits med uppgifter om en patient.

Sahlgrenska Universitetssjukhuset har således behandlat och behandlar personuppgifter i strid med 4 kap. 3 § patientdatalagen och 4 kap. 9 § (punkt 1) HSLF-FS 2016:40. Detta innebär att Sahlgrenska Universitetssjukhuset inte har vidtagit tekniska och organisatoriska åtgärder som är lämpliga i förhållande till risken. Sahlgrenska Universitetssjukhuset uppfyller därmed inte kravet på säkerställa en lämplig säkerhet för behandlingen av personuppgifterna, enligt artikel 32 i dataskyddsförordningen.

Val av ingripande

Rättslig reglering

Om det skett en överträdelse av dataskyddsförordningen har Datainspektionen ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen. 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.

Av artikel 58.2 i dataskyddsförordningen följer att Datainspektionen i enlighet med artikel 83 ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

För myndigheter får enligt artikel 83.7 i dataskyddsförordningen nationella regler ange att myndigheter kan påföras administrativa sanktionsavgifter. Enligt 6 kap. 2 § dataskyddslagen kan sanktionsavgifter beslutas för myndigheter, men till högst 5 000 000 kronor alternativt 10 000 000 kronor

beroende på om överträdelsen avser artiklar som omfattas av artikel 83.4 eller 83.5 i dataskyddsförordningen.

I artikel 83.2 i dataskyddsförordningen anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras, men också vad som ska påverka sanktionsavgiftens storlek. Av central betydelse för bedömningen av överträdelsens allvar är dess karaktär, svårighetsgrad och varaktighet. Om det är fråga om en mindre överträdelse får tillsynsmyndigheten, enligt skäl 148 i dataskyddsförordningen, utfärda en reprimand i stället för att påföra en sanktionsavgift.

Föreläggande

Hälso- och sjukvården har, som nämnts, stort behov av information i sin verksamhet och under senare år har en mycket omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarna storlek som hur många som delar information med varandra har ökat väsentligt. Detta ökar kraven på den personuppgiftsansvarige, eftersom bedömningen vad som är lämplig säkerhet påverkas av behandlingens omfattning.

Inom hälso- och sjukvården innebär det att ett stort ansvar vilar på den personuppgiftsansvarige att skydda uppgifterna från obehörig åtkomst, bland annat genom att ha en behörighetstilldelning som är än mer finfördelad. Det är därför väsentligt att det sker en reell analys av behoven utifrån olika verksamheter och olika befattningshavare. Lika viktigt är det att det sker en faktisk analys av de risker som utifrån ett integritetssperspektiv kan uppstå vid en alltför vid tilldelning av behörighet till åtkomst. Utifrån denna analys ska sedan den enskilde befattningshavarens åtkomst begränsas. Denna behörighet ska sedan följas upp och förändras eller inskränkas efter hand som ändringar i den enskilde befattningshavarens arbetsuppgifter ger anledning till det.

Datainspektionens tillsyn har visat att Sahlgrenska Universitetssjukhuset inte har vidtagit lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i journalsystemet genom att Sahlgrenska Universitetssjukhus i egenskap av personuppgiftsansvarig inte följt de krav som ställs i patientdatalagen och Socialstyrelsens föreskrifter. Sahlgrenska Universitetssjukhuset har därigenom underlåtit att följa kraven i artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen. Underlåtenheten omfattar

såväl den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen förelägger därför med stöd av artikel 58.2 d i dataskyddsförordningen Sahlgrenska Universitetssjukhuset att se till att erforderlig behovs- och riskanalys genomförs och dokumenteras för journalsystemen Melior och Nationell patientöversikt och att därefter, med stöd av behovs- och riskanalysen, varje användare tilldelas individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen, 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40.

Sahlgrenska Universitetssjukhuset har också underlåtit att i loggarna i Melior ange vilka åtgärder som har vidtagits med uppgifter om en patient, ett krav som framgår av 4 kap. 3 § patientdatalagen och 4 kap. 9 § (punkt 1) HSLF-FS 2016:40. Datainspektionen förelägger därför Sahlgrenska Universitetssjukhuset att införa dokumentation i loggarna i Melior där det ska framgå vilka åtgärder som har vidtagits med personuppgifter om en patient enligt 4 kap. 3 § patientdatalagen och 4 kap. 9 § (punkt 1) HSLF-FS 2016:40.

Sanktionsavgift

Datainspektionen kan konstatera att överträdelserna i grunden avser Sahlgrenska Universitetssjukhuset skyldighet att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifter enligt dataskyddsförordningen.

I detta fall är det frågan om stora uppgiftssamlingar med känsliga personuppgifter och vidsträckta behörigheter. Vårdgivaren behöver med nödvändighet ha en omfattande behandling av uppgifter om enskildas hälsa. Den får dock inte vara oinskränkt utan ska baseras på vad enskilda medarbetare behöver för att kunna utföra sina uppgifter. Datainspektionen konstaterar att det är frågan om uppgifter som omfattar direkt identifiering av den enskilde genom såväl namn, kontaktuppgifter som personnummer, uppgifter om hälsa, men att det också kan röra sig om andra privata uppgifter om exempelvis familjeförhållanden, sexualliv och livsstil. Patienten är beroende av att få vård och är därmed i en utsatt situation. Uppgifternas

karaktär, omfattning och patienternas beroendeställning ger vårdgivare ett särskilt ansvar att säkerställa patienternas rätt till adekvat skydd för deras personuppgifter.

Ytterligare försvårande omständigheter är att behandlingen av personuppgifter om patienter i huvudjournalssystemet hör till kärnan i en vårdgivares verksamhet, att behandlingen omfattar många patienter och att möjligheten till åtkomst avser inte bara en stor andel av de anställda utan att Sahlgrenska Universitetssjukhuset därtill har gett åtkomst till ett stort antal medarbetare på andra förvaltningar inom Västra Götalandsregionen. I detta fall rör det sig om omkring 900 000 patienter inom ramen för den inre sekretessen, närmare 18 000 anställda och 25 000 aktiva konton. Det finns endast en enhet, enheten för klinisk genetik, där uppgifterna inte är åtkomlig för användarna utanför dessa enheter eftersom enheten är exkluderad från de generella behörigheterna.

Datainspektionen kan dessutom konstatera att Sahlgrenska Universitetssjukhuset inte har följt Datainspektionens beslut från den 27 mars 2015. I beslutet förelades Sahlgrenska Universitetssjukhuset att genomföra en dokumenterad behovs- och riskanalys enligt det dåvarande kravet 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14, vilket motsvarar nuvarande bestämmelse i 4 kap. 2 § HSLF-FS 2016:40. Detta är en försvårande omständighet, enligt artikel 83.2 e i dataskyddsförordningen.

De brister som nu konstaterats har således varit kända för Sahlgrenska universitetssjukhuset under flera års tid vilket innebär att agerandet skett uppsåtligt och därmed bedöms som allvarligare.

Datainspektionen konstaterar också att Sahlgrenska Universitetssjukhuset i information som inkommit i ärendet har uppgett att vårdgivaren accepterar risken med att konfidentialiteten inte prioriteras lika högt som riktighet och tillgänglighet. Som Datainspektionen förstår det har Sahlgrenska Universitetssjukhuset aktivt tagit ställning till att bortprioritera att vidta åtgärder till skydd för den enskildes integritet, vilket gör agerandet allvarligare.

Dessa faktorer innebär sammantaget att överträdelserna inte är att bedöma som mindre överträdelser utan överträdelser som ska leda till en administrativ sanktionsavgift.

Datainspektionen anser att överträdelserna har en nära anknytning till varandra. Den bedömningen grundar sig på att behovs- och riskanalysen ska ligga till grund för tilldelningen av behörigheterna. Datainspektionen bedömer därför att dessa överträdelser har så nära anknytning till varandra att de utgör sammankopplade uppgiftsbehandlingar enligt artikel 83.3 i dataskyddsförordningen. Datainspektionen bestämmer därför en gemensam sanktionsavgift för överträdelserna.

Beträffande bristerna i loggarna kan Datainspektionen konstatera att inte alla uppgifter som ska ingå i loggarna gör det, men att loggning i huvudsak innehåller de uppgifter som krävs enligt Socialstyrelsens föreskrifter. Datainspektionen anser därför att det är tillräckligt att Sahlgrenska Universitetssjukhuset föreläggs att rätta bristen och bestämmer därför inte någon särskild sanktionsavgift för denna överträdelse.

Den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande. Det innebär att beloppet ska bestämmas så att den administrativa sanktionsavgiften leder till rättelse, att den ger en preventiv effekt och att den dessutom är proportionerlig i förhållande till såväl aktuella överträdelser som till tillsynsobjektets betalningsförmåga.

Det maximala beloppet för sanktionsavgiften i detta fall är 10 miljoner kronor enligt 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer Datainspektionen den administrativa sanktionsavgiften för Sahlgrenska Universitetssjukhuset till 3 500 000 (tre miljoner femhundra tusen) kronor.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av it-säkerhetsspecialisten Magnus Bergström. Vid den slutliga handläggningen har chefsjuristen Hans-Olof Lindblom samt enhetscheferna Malin Blixt och Katarina Tullstedt medverkat.

Lena Lindgren Schelin, 2020-12-02 (Det här är en elektronisk signatur)

Lena Lindgren Schelin, 2020-12-02 (Det här är en elektronisk signatur)

Bilagor: Bilaga 1 – Hur man betalar sanktionsavgift

Kopia för kännedom till:

Dataskyddsombud

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär.

Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Datainspektionen om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.



Hur man överklagar

FR-03

Vill du att beslutet ska ändras i någon del kan du överklaga. Här får du veta hur det går till.

Överklaga skriftligt inom 3 veckor

Tiden räknas oftast från den dag som du fick del av det skriftliga beslutet. I vissa fall räknas tiden i stället från beslutets datum. Det gäller om beslutet avkunnades vid en muntlig förhandling, eller om rätten vid förhandlingen gav besked om datum för beslutet.

För en part som företräder det allmänna (till exempel myndigheter) räknas tiden alltid från den dag domstolen meddelade beslutet.

Observera att överklagandet måste ha kommit in till domstolen när tiden går ut.

Vilken dag går tiden ut?

Sista dagen för överklagande är samma veckodag som tiden börjar räknas. Om du exempelvis fick del av beslutet måndagen den 2 mars går tiden ut måndagen den 23 mars.

Om sista dagen infaller på en lördag, söndag eller helgdag, midsommarafton, julafton eller nyårs-afton, räcker det att överklagandet kommer in nästa vardag.

Så här gör du

1. Skriv förvaltningsrättens namn och målnummer.
2. Förklara varför du tycker att beslutet ska ändras. Tala om vilken ändring du vill ha och varför du tycker att kammarrätten ska

ta upp ditt överklagande (läs mer om prövningstillstånd längre ner).

3. Tala om vilka bevis du vill hänvisa till. Förklara vad du vill visa med varje bevis. Skicka med skriftliga bevis som inte redan finns i målet.
4. Lämna namn och personnummer eller organisationsnummer.

Lämna aktuella och fullständiga uppgifter om var domstolen kan nå dig: postadresser, e-postadresser och telefonnummer.

Om du har ett ombud, lämna också ombudets kontaktuppgifter.
5. Skicka eller lämna in överklagandet till förvaltningsrätten. Du hittar adressen i beslutet.

Vad händer sedan?

Förvaltningsrätten kontrollerar att överklagandet kommit in i rätt tid. Har det kommit in för sent avvisar domstolen överklagandet. Det innebär att beslutet gäller.

Om överklagandet kommit in i tid, skickar förvaltningsrätten överklagandet och alla handlingar i målet vidare till kammarrätten.

Har du tidigare fått brev genom förenklad delgivning kan även kammarrätten skicka brev på detta sätt.

Prövningstillstånd i kammarrätten

När överklagandet kommer in till kammarrätten tar domstolen först ställning till om målet ska tas upp till prövning.

Kammarrätten ger prövningstillstånd i fyra olika fall.

- Domstolen bedömer att det finns anledning att tvivla på att förvaltningsrätten dömt rätt.
- Domstolen anser att det inte går att bedöma om förvaltningsrätten dömt rätt utan att ta upp målet.
- Domstolen behöver ta upp målet för att ge andra domstolar vägledning i rättstillämpningen.
- Domstolen bedömer att det finns synnerliga skäl att ta upp målet av någon annan anledning.

Om du *inte* får prövningstillstånd gäller det överklagade beslutet. Därför är det viktigt att i överklagandet ta med allt du vill föra fram.

Vill du veta mer?

Ta kontakt med förvaltningsrätten om du har frågor. Adress och telefonnummer hittar du på första sidan i beslutet.

Mer information finns på www.domstol.se.