BLENDOW LEXNOVA

LEXNOVA NYHETER

Fem sjukhus döms till mångmiljonavgifter för GDPR-brister

Publicerad
26 MAY 2021

Förvaltningsrätten dömer fem sjukhus att betala över 20 miljoner kronor i sanktionsavgifter sedan de överträtt GDPR. Bristen består i att sjukhusen tilldelat varje användare behörighet för åtkomst till personuppgifter utan att genomföra behovs- och riskanalyser.

Sjukhusen har låtit anställda få full tillgång till patientuppgifter utan att göra en behovs- och riskanalys. Vårdgivaren ska enligt 4 kap. 2 § i Socialstyrelsens föreskrift HSLF-FS 2016:40 göra en behovs-och riskanalys, innan tilldelning av behörigheter i systemet sker.

I fallet med exempelvis Sahlgrenska Universitetssjukhuset har de ansvariga 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, numera enligt Integritetsskyddsmyndigheten, IMY, kunde konstatera att Sahlgrenska Universitetssjukhuset inte har genomfört en analys som avser verksamhetens, olika processers och personalkategoriers behov av att behandla uppgifter. Det som beskrivs är i stället 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.

Myndigheten hänvisade till förarbetena till patientdatalagen enligt vilka vissa uppgifter kan 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 anställde 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.

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

Förvaltningsrätten i Stockholm finner att sjukhusen överträtt GDPR och att IMY därmed haft fog för att ingripa dels genom en administrativ sanktionsavgift, dels ett föreläggande. Förvaltningsrätten bedömer att sjukhusens underlåtenhet att genomföra behovs- och riskanalyser innebär inte bara en överträdelse av nationella bestämmelser utan också av de grundläggande principerna för personuppgiftsbehandling i GDPR.

I domarna där domskälen i princip är identiska skriver förvaltningsrätten att 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.

Och 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.

Capio tog upp legalitetsprincipen och pekade på att den i grunden en straffrättslig princip men den tillämpas också inom förvaltningsrätten när det är fråga om att ålägga administrativa sanktioner eller böter. Detta innebär ett krav på klarhet i tillämpningen av normer vilket saknas här.

Förvaltningsrättens uppfattning är att förarbetsuttalandena till patientdatalagen inte gör anspråk på att vara en uttömmande uppräkning av vad en behovs- och riskanalys alltid måste innehålla för att anses vara godtagbar. Enligt förvaltningsrättens mening får det dock anses framgå redan av ordalydelsen i nämnda bestämmelse att den personuppgiftsansvarige måste göra en analys av såväl behov som risker angående åtkomst till patientuppgifter innan behörighetstilldelning. Förvaltningsrätten bedömer mot denna bakgrund att det överklagade beslutet inte strider mot legalitetsprincipen

De aktuella sjukhusen är Sahlgrenska Universitetssjukhuset som får betala 3,5 miljoner kronor, Capio S:t Görans sjukhus som måste betala 10 miljoner kronor, Karolinska Universitetssjukhuset som döms att betala 4 miljoner kronor och slutligen Region Östergötland och Region Västerbotten som ska betala 2,5 miljoner kronor vardera. Totalt alltså 22,5 miljoner kronor i administrativa sanktionsavgifter med andra ord.

Mikael Kindbom

Instans: Förvaltningsrätterna

Rättsområden: Personuppgifter och integritet, Hälso- och sjukvårdsrätt, Fri rörlighet, Övrig arbetsrätt, IT-rätt