Integritetsskydds myndigheten

Sjukhusstyrelsen i Region Uppsala
751 85 Uppsala

Diarienummer:
DI-2021-5595

Datum:
2022-01-26

Beslut efter tillsyn enligt dataskyddsförordningen mot Sjukhusstyrelsen i Region Uppsala

Innehållsförteckning

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) konstaterar att Sjukhusstyrelsen i Region Uppsala (sjukhusstyrelsen) som personuppgiftsansvarig har, under tiden från den 25 maj 2018 till den 7 maj 2019, behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen[1] på följande sätt:

- Sjukhusstyrelsen har skickat känsliga personuppgifter som inte var krypterade via öppet nät till patienter och remittenter. Behandlingen har också skett i strid med Region Uppsalas egna riktlinjer. Det innebär att sjukhusstyrelsen inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen.

- Sjukhusstyrelsen har lagrat känsliga personuppgifter i e-postvärdtjänsten Outlook. Det innebär att sjukhusstyrelsen inte har vidtagit lämpliga tekniska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen.

IMY beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen och 6 kap. 2 § dataskyddslagen[2] att sjukhusstyrelsen, för överträdelse av artiklarna 5.1 f och 32.1 i dataskyddsförordningen, ska betala en administrativ sanktionsavgift på 1 600 000 (en miljon sexhundratusen) kronor.

Redogörelse för tillsynsärendet

Utgångspunkten för tillsynsärendet

IMY beslutade att inleda en tillsyn mot Region Uppsala med anledning av regionens anmälan den 7 maj 2019 om personuppgiftsincident.

IMY:s granskning omfattar den personuppgiftsbehandling som sjukhusstyrelsen utför i samband med att Akademiska sjukhuset skickar e-post med patientuppgifter till patienter och remittenter i tredjeland. IMY:s granskning omfattar även lagringen av patientuppgifter i e-postvärdtjänsten Outlook.

IMY har inom ramen för denna tillsyn granskat om den aktuella personuppgiftsbehandlingen uppfyller de krav på säkerhet som ställs i artiklarna 5.1 f och 32 i dataskyddsförordningen. IMY har inte granskat om personuppgiftsbehandlingen är förenlig med regleringen i dataskyddsförordningen i övrigt, till exempel bestämmelserna om överföring av personuppgifter till tredjeland.

Dataskyddsförordningen började tillämpas den 25 maj 2018. IMY:s tillsyn omfattar därför perioden från den 25 maj 2018 till den 7 maj 2019 (då anmälan kom in). IMY har

[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).
[2] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

inte granskat de åtgärder som sjukhusstyrelsen har uppgett att den vidtagit efter den 7 maj 2019.

Uppgifter från sjukhusstyrelsen

Regionstyrelsen i Region Uppsala har uppgett att den har rätt att företräda regionen utåt. Sjukhusstyrelsen har uppgett att den instämmer i det som regionstyrelsen anfört.

Sjukhusstyrelsen har, genom regionstyrelsen, uppgett bland annat följande.

Personuppgiftsansvar
Sjukhusstyrelsen är personuppgiftsansvarig för den personuppgiftsbehandling som sker när e-post skickas från och till patienter eller remittenter i utlandet. Behandlingen sker på förvaltningen, Akademiska sjukhuset, som är placerad under nämnden sjukhusstyrelsen. Denna bedömning görs mot bakgrund av att sjukhusstyrelsen är en självständig förvaltningsmyndighet som bestämmer ändamål och medel med personuppgiftsbehandlingen.

E-post som skickas okrypterad över öppet nät till tredjeland

Behandling av personuppgifter i e-post

Akademiska sjukhuset skickar e-post till patienter och remittenter (det vill säga hemsjukhuset) i utlandet på patientens eller remittentens initiativ. Det är upp till patienten alternativt remittenten att välja hur uppgifterna ska skickas in. Dialogen mellan patienten eller remittenten och Akademiska sjukhuset sker huvudsakligen via e-post.

En patient från utlandet som får vård vid Akademiska sjukhuset registreras i huvudjournalsystemet Cosmic. Journalhandlingar som erhålls från patienten om hens hälsotillstånd scannas in i Cosmic. Även den vård som utförs vid Akademiska sjukhuset dokumenteras i Cosmic. När vården avslutas skriver ansvarig läkare en sammanställning av vården i en så kallad Medical report i Cosmic. Medical report skickas till patienten eller remittenten per post, men om det är brådskande skickas den via e-post.

Syftet med behandlingen är att bedriva högspecialiserad hälso- och sjukvård vid Akademiska sjukhuset.

Akademiska sjukhuset skickar uppskattningsvis 500–1 000 dylika e-postmeddelanden per månad. E-postmeddelandena skickades under 2018 till patienter alternativt remittenter i Libanon, Marocko, Nepal, Pakistan, Peru, Ryssland, Saudiarabien, Schweiz, Thailand, Turkiet, USA, Argentina, Australien, Indien, Irak, Iran, Israel, Kanada, Kenya och Kina.

E-postmeddelandena innehåller oftast journalhandlingar och vidarebefordras till berörd verksamhetschef, specialist och i vissa fall annan personal inom Akademiska sjukhuset. Två personer har tillgång till personuppgifterna. Det är administrativ personal med vårdbakgrund som har tillgång till personuppgifterna och personalen omfattas av sekretess.

Personuppgifterna som behandlas är uppgifter om hälsa samt uppgifter om patientens namn, reservpersonnummer, hemadress, e-postadress, telefonnummer, remittent,

berört verksamhetsområde och tidpunkt för inbokad vård. De registrerade är anställda, patienter och barn. Vad gäller anställda förekommer uppgifter om dem endast i sändande och mottagande e-postadresser.

Personuppgiftsbehandlingen rörde cirka 300 registrerade per år räknat från 2014 till maj 2019. Antalet gäller både personer som kommit in med förfrågningar om vård och de som behandlats på Akademiska sjukhuset.

Personuppgiftsbehandlingen har pågått sedan 2014 och pågår fortfarande. Det framgår av en skrivelse från sjukhusstyrelsen daterad den 2 juni 2021.

Kryptering

Personuppgifterna skickas okrypterade över öppet nät. Det innebär att överföringen av e-posten och informationen i e-postmeddelandena inte är skyddad av kryptering.

Sjukhusstyrelsen har sedan införandet av Outlook använt Microsofts standardinställningar, vilket innebär att överföringen av e-posten sker med det opportunistiska kryptografiska kommunikationsprotokollet, OTLS[3]. Sjukhusstyrelsen använder versionen 1.2 av det kryptografiska kommunikationsprotokollet (TLS 1.2). Det innebär att om mottagarens e-postleverantör inte har denna version av TLS, väljs en föregående version av TLS.

Om det saknas stöd för TLS hos mottagarens e-postleverantör skickas e-postmeddelandena okrypterade vid överföringen. Det rör enligt sjukhusstyrelsen cirka 1 av 9 000 e-postmeddelanden. Sjukhusstyrelsen har dock inte verifierat exakt hur många av dessa e-postmeddelanden per dag som skickas okrypterade i denna personuppgiftsbehandling.

Sjukhusstyrelsen har inte uppfyllt kraven på att överföring av personuppgifter i öppna nät ska göras på ett sådant sätt att inte obehöriga kan ta del av dem. Detta då överföringen gjordes okrypterad via Outlook.

Styrdokument

Enligt Region Uppsalas styrdokument om hantering av e-post får känsliga personuppgifter inte kommuniceras via e-post.

Vidtagna åtgärder efter incidenten

Sjukhusstyrelsen införde i september 2019 en krypteringslösning för filer, vilket möjliggjorde en säker överföring via e-post.

Det pågår ett systematiskt förbättringsarbete och sjukhusstyrelsen har arbetat med en riskanalys och en konsekvensbedömning.

Lagring i e-postvärdtjänsten Outlook
I Outlook lagras e-postmeddelandena mellan patient eller remittent och Akademiska sjukhuset. Journalhandlingarna lagras också i Outlook.

[3] Opportunistic Transport Layer Security.

Motivering av beslutet

Gällande regler

Den personuppgiftsansvariges ansvar
Den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter är personuppgiftsansvarig. Det framgår av artikel 4.7 i dataskyddsförordningen.

Den personuppgiftsansvarige ansvarar för och ska kunna visa att de grundläggande principerna i artikel 5 i dataskyddsförordningen följs (artikel 5.2).

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. Det framgår av artikel 24.1 i dataskyddsförordningen.

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

Uppgifter om hälsa utgör så kallade känsliga personuppgifter. Det är förbjudet att behandla sådana personuppgifter enligt artikel 9.1 i dataskyddsförordningen, såvida behandlingen inte omfattas av något av undantagen i artikel 9.2 i förordningen.

Av artikel 32.1 i dataskyddsförordningen följer att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Det ska ske 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.

Vid bedömningen av lämplig säkerhetsnivå ska 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. Det framgår av artikel 32.2 i dataskyddsförordningen.

I skäl 75 i dataskyddsförordningen anges de faktorer som ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter som kan uppkomma vid behandling av personuppgifter. Bland annat ska beaktas om behandlingen gäller personuppgifter om hälsa eller om sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

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

IMY:s bedömning

Personuppgiftsansvar
Sjukhusstyrelsen har uppgett att den är personuppgiftsansvarig för den personuppgiftsbehandling som sker när e-post skickas från Akademiska sjukhuset till patienter och remittenter i utlandet. Detta stöds av den övriga utredningen i ärendet. IMY bedömer därför att sjukhusstyrelsen är personuppgiftsansvarig för de e-postöverföringar som det är fråga om i ärendet. Vidare bedömer IMY att sjukhusstyrelsen också är personuppgiftsansvarig för den personuppgiftsbehandling som sker vid lagringen i e-postvärdtjänsten Outlook eftersom e-postöverföringarna sker därifrån.

Känsliga personuppgifter har skickats okrypterat via öppet nät
Som personuppgiftsansvarig ska sjukhusstyrelsen vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna (artikel 32 i dataskyddsförordningen). Personuppgifterna som behandlas måste till exempel skyddas mot obehörigt röjande eller obehörig åtkomst.

Vad som är lämplig säkerhetsnivå varierar i förhållande till bland annat de risker för fysiska personers rättigheter som behandlingen medför samt behandlingens art, omfattning, sammanhang och ändamål. Vid bedömningen måste det exempelvis beaktas vad det är för typ av personuppgifter som behandlas, till exempel uppgifter om hälsa.[4]

Sjukhusstyrelsen har skickat ett stort antal personuppgifter via e-post till patienter och remittenter i utlandet. Det rör sig om uppskattningsvis 500–1 000 skickade e-postmeddelanden per månad. De aktuella e-postmeddelandena innehöll personuppgifter om hälsa som är känsliga personuppgifter. Behandling av känsliga personuppgifter kan innebära betydande risker för den personliga integriteten och därför krävs ett starkt skydd vid behandling av sådana uppgifter. Det innebär att om sådana personuppgifter skickas via e-post måste de skyddas på ett sådant sätt att obehöriga inte kan ta del av dem. Personuppgifterna kan till exempel skyddas genom kryptering.

Av sjukhusstyrelsens uppgifter framgår att sjukhusstyrelsen använde en teknik, så kallad OTLS, som innebär att överföringen av e-posten krypteras för det fall mottagande e-postserver stödjer TLS. Om mottagande e-postserver inte har stöd för TLS, blir överföringen av e-posten okrypterad. Det innebär att sjukhusstyrelsen använder en teknik som är avhängig mottagarens tekniska inställningar, vilket innebär att sjukhusstyrelsen inte kan säkerställa att överföringen av e-posten är krypterad. E-posten har skickats externt (det vill säga utanför Region Uppsala), vilket har medfört att det inte gått att säkerställa att e-posten som skickas från Akademiska sjukhuset mottas med en kryptering som är lämplig i förhållande till risken med behandlingen. Sjukhusstyrelsen har själv uppgett att den inte har verifierat hur många av e-postmeddelandena som skickades okrypterade via öppet nät per dag.

I det aktuella fallet skickas informationen i e-postmeddelandena utan kryptering, det vill säga uppgifterna har kunnat läsas i klartext via öppet nät (internet). Det innebär att

[4] Se skälen 75 och 76 i dataskyddsförordningen.

obehöriga har kunnat få åtkomst till personuppgifterna i e-postmeddelandena och att andra än avsedda mottagare har kunnat ta del av uppgifterna både under överföringen, i de fall då mottagarens e-postserver inte haft stöd för TLS, och efter överföringen av e-posten. Enligt IMY finns det en risk för att uppgifterna kommer i orätta händer efter överföringen, eftersom personen som skickar uppgifterna skulle kunna skriva en felaktig mottagaradress [1].

IMY finner att informationen i e-postmeddelandena borde ha skyddats mot obehörigt röjande eller obehörig åtkomst, och detta alldeles oavsett om överföringen av e-posten varit krypterad eller inte. Sjukhusstyrelsen borde ha vidtagit tekniska åtgärder, till exempel i form av kryptering, för att skydda personuppgifterna och därigenom säkerställa en lämplig skyddsnivå för uppgifterna.

Att ett stort antal känsliga personuppgifter under en längre tid har exponerats mot internet utan skydd mot obehörigt röjande eller obehörig åtkomst, innebär enligt IMY att bristen i säkerheten varit av sådant allvarligt slag att den även innebär en överträdelse av artikel 5.1 f i dataskyddsförordningen.

Enligt sjukhusstyrelsen anges i Region Uppsalas styrdokument om hantering av post och e-post att känsliga personuppgifter inte får kommuniceras via e-post. Sjukhusstyrelsen har således identifierat de risker som behandlingen av känsliga personuppgifter i e-post medför men inte vidtagit tillräckliga åtgärder för att följa riktlinjerna. IMY finner därmed att sjukhusstyrelsen inte har vidtagit de lämpliga organisatoriska åtgärder som krävs för att säkerställa behandlingens säkerhet.

Sammantaget finner IMY att sjukhusstyrelsen, genom att inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen, har behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen.

Känsliga personuppgifter har lagrats i Outlook
Sjukhusstyrelsen har uppgett att journalhandlingarna även lagras i Outlook utöver lagringen i huvudjournalsystemet Cosmic.

Journalhandlingarna innehåller personuppgifter om hälsa som är känsliga personuppgifter. Behandling av känsliga personuppgifter kan innebära betydande risker för den personliga integriteten och därför krävs ett starkt skydd vid behandling av sådana uppgifter. Det innebär bland annat att dessa personuppgifter måste skyddas på ett sådant sätt att obehöriga inte kan ta del av dem.

Syftet med ett e-postsystem (i detta fall Outlook) är att sprida och kommunicera information. Ett e-postsystem är exponerat mot internet vilket innebär att uppgifterna i systemet riskerar att bli åtkomliga för obehöriga. Outlook är därför generellt sett en olämplig lagringsplats för känsliga personuppgifter.

Genom att lagra journalhandlingar i Outlook, har de aktuella uppgifterna utsatts för en hög risk att de röjs eller att obehöriga får åtkomst till dem. Det innebär att sjukhusstyrelsen inte har vidtagit de tekniska åtgärder som krävs enligt artikel 32 i dataskyddsförordningen för att säkerställa ett lämpligt skydd för uppgifterna.

Att ett stort antal känsliga personuppgifter under en längre tid har exponerats mot internet utan skydd mot obehörigt röjande eller obehörig åtkomst, innebär enligt IMY

[1] Se Datainspektionens rapport Anmälda personuppgiftsincidenter 2019 (rapport 2020:2).

att bristen i säkerheten varit av sådant allvarligt slag att den även innebär en överträdelse av artikel 5.1 f i dataskyddsförordningen.

Sammanfattningsvis anser IMY att sjukhusstyrelsen inte har vidtagit lämpliga tekniska åtgärder för att förhindra obehörigt röjande av eller obehörig åtkomst till personuppgifterna som lagrats i Outlook. Sjukhusstyrelsen har därigenom inte säkerställt en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Sjukhusstyrelsen har därmed behandlat personuppgifterna i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen.

Val av ingripande

Rättslig reglering
IMY har vid överträdelser av dataskyddsförordningen ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen, bland annat reprimand, föreläggande och sanktionsavgifter.

IMY ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

Medlemsstaterna får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter. Det framgår av artikel 83.7 i förordningen. Sverige har i enlighet med detta beslutat att tillsynsmyndigheten ska få ta ut sanktionsavgifter av myndigheter. För överträdelser av bland annat artikel 32 ska avgiften uppgå till högst 5 000 000 kronor. För överträdelser av bland annat artikel 5 i förordningen ska avgiften uppgå till högst 10 000 000 kronor. Det framgår av 6 kap. 2 § dataskyddslagen samt artikel 83.4 och 83.5 i dataskyddsförordningen.

Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen. Det framgår av artikel 83.3 i dataskyddsförordningen.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 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 vid bestämmandet av sanktionsavgiftens storlek. Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i förordningen. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Påförande av sanktionsavgift
IMY har ovan bedömt att sjukhusstyrelsen har överträtt artiklarna 5.1 f och 32.1 i dataskyddsförordningen. Överträdelser av dessa bestämmelser kan, som framgår ovan, föranleda sanktionsavgifter.

Överträdelserna har skett genom att sjukhusstyrelsen har skickat en stor mängd patientuppgifter genom okrypterad e-post via öppet nät till patienter och remittenter i tredjeland samt genom att patientuppgifterna har lagrats i Outlook. Personuppgifterna som behandlades var känsliga personuppgifter, vilket innebär en hög risk för de registrerades fri- och rättigheter. Behandlingarna som beskrivs i ärendet har skett systematiskt och under en längre tid. Behandlingarna via e-post har också skett i strid med Region Uppsalas egna riktlinjer. Dessa faktorer innebär sammantaget att en sanktionsavgift bör påföras.

IMY bedömer att behandlingarna via e-post och lagringen avser två sammankopplade uppgiftsbehandlingar enligt artikel 83.3 i dataskyddsförordningen. Detta eftersom behandlingarna rör hantering av samma personuppgifter i Outlook och avser överträdelse av samma bestämmelser.

Vid bestämmande av sanktionsavgiftens storlek ska IMY beakta både försvårande och förmildrande omständigheter samt att den administrativa sanktionsavgiften ska vara effektiv, proportionell och avskräckande.

Det är försvårande att personuppgiftsbehandlingarna har pågått en längre tid, det vill säga under den granskade perioden från den 25 maj 2018 till den 7 maj 2019, och att sjukhusstyrelsen inte skyndsamt vidtog åtgärder för att skydda personuppgifterna trots att sjukhusstyrelsen var medveten om bristerna i säkerheten. Det är även försvårande att behandlingarna omfattat en stor mängd hälsouppgifter som okrypterade skickats via öppet nät och som lagrats i Outlook. Det har rört sig om uppskattningsvis mellan 500 och 1 000 e-postmeddelanden per månad som obehöriga har kunnat få åtkomst till via internet och omfattat cirka 300 registrerade per år. Genom de uppgifter som behandlas kan de registrerade identifieras direkt genom namn, kontaktuppgifter och uppgifter om hälsa. IMY anser därför att uppgifternas karaktär, omfattning och de registrerades beroendeställning ger sjukhusstyrelsen ett särskilt ansvar att säkerställa ett lämpligt skydd för personuppgifterna, vilket inte skett.

Det är vidare försvårande att behandlingarna har skett systematiskt och att de skett i strid med Region Uppsalas egna riktlinjer om att känsliga personuppgifter inte ska skickas via e-post.

Som förmildrande omständighet beaktas att sjukhusstyrelsen i september 2019 införde tekniska åtgärder i form av en krypteringslösning för filer.

IMY bestämmer utifrån en samlad bedömning att sjukhusstyrelsen ska påföras en administrativ sanktionsavgift på 1 600 000 (en miljon sexhundratusen) kronor.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Linda Hamidi. Vid den slutliga handläggningen har även rättschefen David Törngren, enhetschefen Malin Blixt och it-säkerhetsspecialisten Ulrika Sundling medverkat.

Lena Lindgren Schelin, 2022-01-26 (Det här är en elektronisk signatur)

Bilaga
Information om betalning av sanktionsavgift.

Kopia till
Dataskyddsombudet.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

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