Integritetsskydds myndigheten

Regionstyrelsen i Region Uppsala
751 85 Uppsala

Diarienummer:
DI-2019-9457

Datum:
2022-01-26

Beslut efter tillsyn enligt dataskyddsförordningen mot Regionstyrelsen 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 Regionstyrelsen i Region Uppsala (regionstyrelsen) som personuppgiftsansvarig har, under tiden från den 25 maj 2018 till den 7 maj 2019, behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1]. Det har skett genom att regionstyrelsen inom regionen skickat känsliga personuppgifter och personnummer via e-post. Överföringen av e-posten var krypterad men inte informationen i e-postmeddelandena. Behandlingen har också skett i strid med Region Uppsalas egna riktlinjer. Det innebär att regionstyrelsen inte har vidtagit lämpliga tekniska och organisatoriska 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 regionstyrelsen, för överträdelse av artikel 32.1 i dataskyddsförordningen, ska betala en administrativ sanktionsavgift på 300 000 (trehundratusen) kronor.

Redogörelse för tillsynsärendet

Utgångspunkten för tillsynen

IMY beslutade att inleda en tillsyn mot regionstyrelsen efter en anmälan om personuppgiftsincident från regionstyrelsen den 7 maj 2019.

IMY:s granskning omfattar två kategorier av personuppgiftsbehandlingar.

Den första kategorin avser e-postmeddelanden med patientuppgifter som skickades automatiserat till berörda vårdförvaltningar inom Region Uppsala för bland annat administration och kvalitetssäkring.

Den andra kategorin avser e-postmeddelanden med patientuppgifter som skickades manuellt till forskare och läkare inom Region Uppsala för bland annat forskning och kvalitetsuppföljning.

IMY har granskat om personuppgiftsbehandlingarna i e-posten uppfyller de krav på säkerhet som ställs i artikel 32 i dataskyddsförordningen.

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

Uppgifter från regionstyrelsen

Regionstyrelsen har uppgett bland annat följande.

[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.

Den första kategorin av personuppgiftsbehandling – e-post som skickades automatiserat
Statistikdatabasen Cosmic Intelligence hämtade personuppgifter från huvudjournalsystemet Cosmic. Personuppgifterna hämtades sedan av Business Objects som lade informationen i en excelfil. Överföringarna skedde automatiskt varje månad. Business Objects skickade därefter excelfilerna till berörda vårdförvaltningar inom Region Uppsala, såsom Akademiska sjukhuset och Lasarettet i Enköping. E-postmeddelandena skickades automatiserat varje månad till Region Uppsalas e-postdomäner. E-postmeddelandena skickades enbart till behöriga personer inom den förvaltning som var berörd inom Region Uppsala.

De aktuella excelfilerna kunde innehålla samtliga uppgifter från patientjournalen, förutom den löpande texten från patientjournalens fritextfält. Beroende på typ av rapport kunde även andra uppgifter ingå, såsom väntetider och patientkategori. Excelfilerna innehöll även uppgifter om personnummer, namn, vårdande enhet och kontaktdatum.

Cirka 25 e-postmeddelanden skickades varje månad till ett hundratal mottagare inom Akademiska sjukhusets verksamhetsområde. Hundratals sändare och mottagare inom Region Uppsala hade tillgång till personuppgifterna.

Det övergripande syftet med personuppgiftsbehandlingen har varit administration, exempelvis att korrigera fel i verksamheterna och att åtgärda dem. Dessutom har syftet varit att utveckla och säkra kvaliteten i verksamheten.

Personuppgiftsbehandlingen har pågått sedan 2015 och fram till regionstyrelsens anmälan om incidenten till IMY den 7 maj 2019. Behandlingen stoppades helt i samband med att incidenten upptäcktes.

Den andra kategorin av personuppgiftsbehandling – e-post som skickades manuellt
Statistikdatabasen Cosmic Intelligence hämtade personuppgifter från huvudjournalsystemet Cosmic. Utdatasystemet Diver hämtade sedan personuppgifter från Cosmic Intelligence samt de patientadministrativa systemen IMX och PAS. Uttag av personuppgifter gjordes sedan manuellt från Diver till excelfiler. De manuella uttagen gjordes av bland annat systemutvecklare och administratören på regionkontoret. Dessa excelfiler skickades sedan till läkare när de hade begärt uppgifter i kvalitetsuppföljningssyfte och till forskare när de hade begärt forskningsunderlag. E-postmeddelandena skickades enbart till mottagare som var anställda inom Region Uppsala, det vill säga endast till Region Uppsalas e-postdomäner. Det innebär att e-postmeddelandena inte skickades till e-postadresser knutna till Uppsala universitet.

Excelfilerna kunde bland annat innehålla uppgifter om personnummer, diagnoskoder, kontaktdatum, verksamhetsområde, ålder, län, åtgärdskod och avdelning. Excelfilerna innehöll inte uppgifter om namn. Excelfilerna rörde enbart patienter som behandlades på Akademiska sjukhuset.

Cirka 200−250 e-postmeddelanden skickades per år. Hundratals sändare och mottagare inom Region Uppsala hade tillgång till personuppgifterna.

Personuppgifterna behandlades för administrativa syften och för att utveckla och säkra kvaliteten i verksamheten samt för forskningsändamål.

Personuppgiftsbehandlingen pågick från september 2014 till regionstyrelsens anmälan om incidenten till IMY den 7 maj 2019. Behandlingen stoppades helt i samband med att incidenten upptäcktes och ett arbete påbörjades för att ta fram en lösning för kryptering av e-post.

Information som rör båda personuppgiftsbehandlingarna
Personuppgiftsansvar

Regionstyrelsen är personuppgiftsansvarig för den personuppgiftsbehandling som rör sammanställning av data i Business Objects och för den behandling som sker vid automatisk överföring via e-post. Behandlingen sker på förvaltningen regionkontoret, som är placerad under nämnden regionstyrelsen. Denna bedömning görs mot bakgrund av att regionstyrelsen är en självständig förvaltningsmyndighet som bestämmer ändamål och medel med personuppgiftsbehandlingen.

Regionstyrelsen är även personuppgiftsansvarig för den behandling som sker i Diver och för den behandling som sker via den manuella överföringen via e-post.

Regionstyrelsen har bifogat dokumenten *Reglemente för styrelser och nämnder i Region Uppsala* samt *Regionstyrelsens delegationsordning*.

Styrdokument

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

Kategorier av registrerade

Kategorier av registrerade är anställda, patienter, barn och personer med skyddad identitet. Vad gäller anställda förekommer uppgifter om dem endast i sändande och mottagande e-postadresser.

Personuppgiftsbehandlingarna rör sammantaget mellan 100 000 och 500 000 individer för perioden 2015−2019.

Kategorier av användare

De kategorier av användare som har tillgång till personuppgifterna är administrativ personal med access till källsystem och lagringsytor.

Kryptering

Transporten (överföringen) av e-posten inom regionen var krypterad men informationen i excelfilerna var inte skyddad genom kryptering.

Transporten av e-posten skickades krypterad med det kryptografiska kommunikationsprotokollet TLS1.2 till mottagare inom Region Uppsala. Regionstyrelsen använde i den första personuppgiftsbehandlingen en lokal e-postserver vid transporten av e-posten mellan Business Objects och mottagare inom regionen. I den andra behandlingen använde regionstyrelsen Microsofts Outlook för e-posten.

Det saknades tekniska skyddsåtgärder för att förhindra läsning och ändring av informationen i excelfilerna. Det saknades också skyddsåtgärder för att förhindra att obehöriga tog del av informationen.

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 i förordningen).

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.
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 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 faktorer som ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter. Bland annat nämns förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt samt om behandlingen avser uppgifter om hälsa eller sexualliv. Vidare ska beaktas om behandlingen gäller personuppgifter 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
Regionstyrelsen har uppgett att den är personuppgiftsansvarig för de e-postöverföringar som beskrivs i ärendet, vilket stöds av utredningen i ärendet. IMY bedömer därför att regionstyrelsen är personuppgiftsansvarig för de aktuella behandlingarna.

Känsliga personuppgifter har skickats okrypterat inom regionen
Regionstyrelsen har skickat excelfiler med patientuppgifter inom regionen via e-post. När det gäller den första kategorin av personuppgiftsbehandling skickades cirka 25 e-postmeddelanden automatiskt varje månad och när det gäller den andra kategorin skickades cirka 200-250 e-postmeddelanden manuellt per år. Överföringen av e-posten inom regionen var krypterad men inte informationen i excelfilerna.

Regionstyrelsen har uppgett att känsliga personuppgifter inte får kommuniceras via e-post enligt Region Uppsalas styrdokument om hantering av post och e-post.

Som personuppgiftsansvarig ska regionstyrelsen 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 och friheter 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 om det är fråga om uppgifter om hälsa.[3]

De aktuella excelfilerna innehöll personuppgifter om hälsa som är känsliga personuppgifter. Behandling av känsliga personuppgifter kan innebära betydande risker för den personliga integriteten. Dessutom innehöll excelfilerna personnummer som anses vara särskilt skyddsvärda personuppgifter[4]. Uppgifterna i e-postmeddelandena var därför av en sådan art att de krävde ett starkt skydd.

Överföringen av e-posten från regionstyrelsen var krypterad men inte informationen i e-postmeddelandena. Det innebar att informationen i excelfilerna inte kunde avlyssnas (läsas) under själva överföringen. Däremot kunde informationen läsas i klartext av såväl behöriga som obehöriga mottagare efter överföringen. Vid en automatiserad överföring finns en viss risk för att uppgifter kommer i orätta händer ifall systemet skulle uppdateras felaktigt. Vid en manuell överföring av personuppgifter finns en ännu högre risk för att uppgifterna kommer i orätta händer jämfört med en automatiserad överföring. Detta eftersom personen som skickar uppgifterna skulle kunna skriva en felaktig mottagaradress[5]. Enligt IMY:s bedömning borde regionstyrelsen ha vidtagit tekniska åtgärder, till exempel i form av kryptering, för att skydda informationen i de automatiserade och de manuella e-postmeddelandena mot obehörigt röjande eller obehörig åtkomst och därigenom säkerställa en lämplig skyddsnivå.

Enligt regionstyrelsen anges i Region Uppsalas styrdokument om hantering av post och e-post att känsliga personuppgifter inte får kommuniceras via e-post.

[3] Se skälen 75 och 76 i dataskyddsförordningen.
[4] Se artikel 87 i dataskyddsförordningen och 3 kap. 10 § dataskyddslagen.
[5] Se Datainspektionens rapport Anmälda personuppgiftsincidenter 2019 (rapport 2020:2).

Regionstyrelsen 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 regionstyrelsen inte har vidtagit de lämpliga organisatoriska åtgärder som krävs för att säkerställa behandlingens säkerhet.

Sammantaget finner IMY att regionstyrelsen inte vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Regionstyrelsen har därför behandlat personuppgifter i strid med artikel 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 i dataskyddsförordningen, 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. Det framgår av 6 kap. 2 § dataskyddslagen samt artikel 83.4 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 regionstyrelsen har överträtt artikel 32.1 i dataskyddsförordningen. Överträdelser av den bestämmelsen kan, som framgår ovan, föranleda sanktionsavgifter.

Överträdelserna har skett genom att regionstyrelsen har skickat en stor mängd okrypterade patientuppgifter inom regionen genom krypterad e-post. Personuppgifterna i e-posten var bland annat känsliga personuppgifter och personnummer, vilket innebar en hög risk för de registrerades fri- och rättigheter. Behandlingarna har skett systematiskt och under en längre tid. Behandlingarna har också skett i strid med Region Uppsalas egna riktlinjer. Dessa faktorer innebär sammantaget att en sanktionsavgift bör påföras.

IMY konstaterar att den manuella respektive den automatiska överföringen av e-post utgör sammankopplade uppgiftsbehandlingar enligt artikel 83.3 i dataskyddsförordningen. Detta eftersom behandlingarna rör patientuppgifter som hämtades från huvudjournalsystemet Cosmic för liknande ändamål såsom administration och kvalitetssäkring. Dessutom är det frågan om överträdelse av samma bestämmelse det vill säga artikel 32.1 i förordningen.

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 under en längre tid, det vill säga under den granskade perioden från den 25 maj 2018 till den 7 maj 2019, och att de har skett systematiskt. Det är även försvårande att behandlingarna omfattat en stor mängd hälsouppgifter som obehöriga kunnat få åtkomst till efter överföringen. När det gäller den första kategorin av personuppgiftsbehandling, har det rört sig om cirka 25 e-postmeddelanden per månad som obehöriga har kunnat få åtkomst till och när det gäller den andra kategorin har det rört sig om cirka 200−250 e-postmeddelanden per år. Regionstyrelsen uppskattar att personuppgiftsbehandlingarna sammantaget har rört mellan 100 000 och 500 000 individer för perioden 2015−2019. Det är således frågan om ett stort antal registrerade under ett år. Genom de uppgifter som behandlas kan de registrerade identifieras direkt genom till exempel namn, personnummer och uppgifter om hälsa. IMY anser därför att uppgifternas karaktär, omfattning och de registrerades beroendeställning ger regionstyrelsen ett särskilt ansvar att säkerställa ett lämpligt skydd för personuppgifterna, vilket inte skett.

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

Som förmildrande omständigheter beaktar IMY att överföringen av e-posten var krypterad och att e-posten skickades internt inom regionen. Det innebär att regionstyrelsen har vidtagit vissa åtgärder i syfte att efterleva kraven och minska riskerna med behandlingarna. IMY beaktar också att regionstyrelsen stoppade behandlingarna i samband med anmälan om personuppgiftsincident till IMY den 7 maj 2019.

IMY bestämmer utifrån en samlad bedömning att regionstyrelsen ska betala en administrativ sanktionsavgift på 300 000 (trehundratusen) 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.