Integritetsskydds myndigheten

Regionstyrelsen i Region Skåne
291 89 Kristianstad

Diarienummer:
IMY-2022-1290

Ert diarienummer:
2022-JUR000018

Datum:
2023-04-26

Beslut efter tillsyn enligt dataskyddsförordningen – Regionstyrelsen i Region Skåne

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) konstaterar att Regionstyrelsen i Region Skåne (regionen) i egenskap av personuppgiftsansvarig har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1] genom att regionen har lagrat okrypterade personuppgifter om patienter på ett usb-minne och den 1 november 2020 förlorat kontrollen över usb-minnet. Regionen har därigenom behandlat känsliga personuppgifter utan att ha säkerställt en lämplig säkerhetsnivå i förhållande till risken för förlust, obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

IMY beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen och 6 kap. 2 § dataskyddslagen[2] att regionen ska betala en administrativ sanktionsavgift för överträdelse av artikel 32.1 i dataskyddsförordningen på 200 000 (tvåhundratusen) kronor.

Redogörelse för tillsynsärendet

Utgångspunkt för tillsynen

IMY mottog från regionen den 18 november 2020 en anmälan om en personuppgiftsincident som skedde den 1 november 2020. Av anmälan framgår att ett usb-minne innehållande personnummer och känsliga personuppgifter om 1 934 registrerade glömdes bort av en medarbetare i fickan på kliniska kläder som lades i en tvättpåse för transport till regionalt tvätteri.

IMY har därefter mottagit två klagomål med anledning av personuppgiftsincidenten. Mot denna bakgrund beslutade IMY att inleda tillsyn.

IMY har granskat om behandlingen av personuppgifter på det aktuella usb-minnet uppfyller de krav på säkerhet som ställs i artikel 32 i dataskyddsförordningen.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

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

Uppgifter från regionen

Regionen har inkommit med två yttranden tillsammans med följande dokument.

- *Instruktion för Region Skånes behandling av personuppgifter,* version 2.0, upprättad den 20 juni 2018 och reviderad den 11 december 2020.
- *Riktlinjer för informationssäkerhet,* daterad den 7 december 2017.
- *Instruktion för tillämpning av riktlinjer för informationssäkerhet*, daterad den 22 maj 2020.
- *Skapa och förvara DIGITAL OCH ANALOG INFORMATION,* version 2.2, daterad den 22 april 2016.
- *Krav på systemstöd för hantering och förvaring av digitala dokument*, version 1.0, daterad den 18 december 2020.
- *Delegationsordning för regionstyrelsen,* daterad den 9 februari 2023.
- Delegationsbeslut om *Region Skånes yttrande gällande Integritetsskyddsmyndighetens tillsyn enligt dataskyddsförordningen IMY-2022-1290*, daterad den 21 februari 2023.
- *Ansökan om registeruppgifter, från kvalitetsregister, för forskningsändamål*, undertecknad den 26 maj 2020.
- *Beslut kring utlämnande*, undertecknad den 24 juni 2020.
- *Anvisning Årshjul för Region Skånes informationssäkerhetssamordnare,* angiven som bilaga 3 och odaterad.
- *Behandling av personuppgifter för forskning,* version 1.1, daterad den 20 maj 2018.

Av det första yttrandet från regionen framkommer i huvudsak följande. Personuppgiftsansvarig är den juridiska personen Region Skåne och regionstyrelsen är ytterst ansvarig för organisationen Region Skånes behandling av personuppgifter. På det försvunna usb-minnet finns två typer av personuppgifter; personnummer och särskilda kategorier av personuppgifter hänförliga till artikel 9.1 i dataskyddsförordningen i form av uppgifter om hälsa som rör 1 934 registrerade. Gällande de särskilda kategorierna av personuppgifter som räknas upp i artikel 9.1 i dataskyddsförordningen finns uppgifter om hälsa. Hälsouppgifterna är hänförliga till ett procedurrelaterat kvalitetsregister, SCAAR, gällande kranskärlssjukdom. Uppgifterna är uppgifter om hälsa av typ ”biodata”. Uppgifterna är okrypterade, men flertalet av värdena är inskrivna som ettor och nollor vilket representerar "ja" eller ”nej" och står därmed inte i klartext. Medarbetare i regionen tillåts att använda flyttbart medium i form av usb för behandling av personuppgifter om beslutade organisatoriska och tekniska skyddsåtgärder vidtas. Regionens styrdokument föreskrev som tekniska skydds-åtgärder vid förvaring och transport av lagringsmedia att skyddet ska motsvara det skyddsvärde som informationen har utifrån den informationsklassificering som genomförts samt att lagringsmedia som innehåller skyddsvärd information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport. Vid obligatorisk utbildning av de anställda upplyser regionen om att usb ska undvikas men att anställda vid användning av usb för lagring av känslig eller värdefull information ska använda krypterade usb. Dessa finns att beställa internt. Det försvunna usb-minnet har inte kommit tillrätta trots omfattande arbete med att återfinna det. Eftersökningen av usb-minnet har skett över en längre tid (november 2020 – mars 2021). Utredningen i ärendet talar inte för att uppgifterna har spridits eller att obehöriga fått del av informationen eftersom usb-minnet förkommit inom organisationen, men då det inte återfunnits är det rimligt säkert att anta att ett tillgänglighetsbrott har ägt rum.

Av det andra yttrandet från regionen framkommer i huvudsak följande. Personuppgifterna på det förkomna usb-minnet härrörde från ett nationellt kvalitetsregister, SCAAR. Begäran om uttag ur kvalitetsregistret ombesörjs av Uppsala kliniska forskningscentrum, UCR. Den av Region Skåne anställde forskaren hade ansökt om uttag och fått beslut om utlämnande av registeruppgifter från kvalitetsregister SCAAR för forskningsändamål. UCR beskriver i ansökan att överlämnat material ska förvaras på ett betryggande sätt, i krypterad form så att obehöriga inte kan få tillgång till det. Ansvarig forskare, anställd hos forskningshuvudmannen Region Skåne har accepterat och förbundit sig till de säkerhetsåtgärder som den centralt personuppgiftsansvarige har uppställt för utlämnandet av de aktuella personuppgifterna.

Region Skånes användning av lagringsmedia följs upp årligen i enlighet med anvisning Årshjul för Region Skånes informationssäkerhetssamordnare. En teknisk säkerhetsåtgärd som driftsattes år 2021 sedan den aktuella händelsen är 7-zip. 7-zip är ett komprimeringsprogram som även kan användas för att kryptera filer. En ytterligare teknisk säkerhetsåtgärd som vidtagits är utvecklandet av en lagringsyta, Säker lagring extern, för hantering av känsliga personuppgifter, sekretessbelagda uppgifter eller annan information som bedöms integritetskänslig och skyddsvärd och som avses att delas med parter utanför Region Skåne. Organisatoriska säkerhetsåtgärder har också vidtagits med anledning av personuppgiftsincidenten. Region Skåne genomför en pågående översyn av instruktion Behandling av personuppgifter för forskning och avser bland annat att uppdatera instruktionen med förtydligande hänvisningar till beslutade befintliga tekniska säkerhetsåtgärder.

Förvaltningen Regionservice har även infört skärpta rutiner för enheterna Tvätt och textil och Kundcenter gällande hantering av upphittade föremål på tvätteriet. För att ytterligare stärka följsamheten av de beslutade tekniska och organisatoriska säkerhetsåtgärderna, utöver de aktiviteter som redogjorts för ovan och i tidigare yttrande, har förvaltningen Skånes Universitetssjukvård intensifierat den dataskyddsrättsliga stöttningen till forskningsorganisationen.

Region Skåne medger förvisso att personuppgiftsincidenten inneburit en överträdelse av dataskyddsförordningen och har därför beslutat om ersättning till de drabbade registrerade som begärt det, i enlighet med skyldigheten i artikel 82.1 i dataskyddsförordningen. Överträdelsen av dataskyddsförordningen i detta avseende innebär dock inte att Region Skåne har vare sig brustit i sin ansvarsskyldighet som personuppgiftsansvarig eller i de vidtagna säkerhetsåtgärderna, utan överträdelsen beror uteslutande på en enskild anställds oaktsamhet.

Motivering av beslutet

Gällande regler m.m.

Personuppgifter och personuppgiftsansvariges ansvar
Artikel 4.1 i dataskyddsförordningen definierar begreppet personuppgifter som varje upplysning som avser en identifierad eller identifierbar fysisk person.

Uppgifter om hälsa definieras i artikel 4.15 i dataskyddsförordningen som person-uppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus.

Uppgifter om hälsa utgör så kallade känsliga personuppgifter.[3] Även uppgifter som indirekt kan röja känsliga personuppgifter utgör en behandling av känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen.[4] Europeiska dataskyddsstyrelsen (EDPB) har uttalat att begreppet uppgifter om hälsa enligt dataskyddsförordningen måste tolkas brett mot bakgrund av bland annat EU-domstolens dom i målet Lindqvist och då det framgår av skäl 53 till dataskyddsförordningen att uppgifter om hälsa förtjänar ett omfattande skydd.[5]

Personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. Den personuppgiftsansvarige ansvarar för och ska kunna visa att de grundläggande principerna i artikel 5 i dataskyddsförordningen följs, det framgår av artikel 5.2 i dataskyddsförordningen.

Enligt artikel 5.1 f i dataskyddsförordningen ska personuppgifterna 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.

Vidare framgår det av artikel 24.1 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.

Av skäl 74 till dataskyddsförordningen framgår att personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med dataskyddsförordningen, även vad gäller åtgärdernas effektivitet. Den personuppgiftsansvariga bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

EDPB har anfört att i princip all behandling av personuppgifter av anställda som sker inom ramen för en organisations verksamhet kan betraktas som att den sker under den organisationens kontroll. Anställda som exempelvis har tillgång till personuppgifter inom en organisation betraktas i allmänhet inte som ”personuppgiftsansvariga” eller ”personuppgiftsbiträden”, utan snarare som ”personer som agerar under den personuppgiftsansvariges eller personuppgiftsbiträdets befogenhet” i den mening som avses i artikel 29 i dataskyddsförordningen. I undantagsfall kan det dock hända att en anställd beslutar att använda personuppgifter för sina egna ändamål och därigenom

---

[3] EU-domstolens mål C-101/01, Lindqvist, EU:C:2003:596, punkt 51.
[4] EU-domstolens mål C-184/20, Vyriausioji tarnybinės etikos komisija, EU:C:2022:601, punkt 128.
[5] EDPB:s riktlinjer 03/2020 om behandling av uppgifter om hälsa för vetenskapliga forskningsändamål i samband med covid-19-utbrottet, s. 5.

olagligt överskrider de befogenheter som han eller hon fick (till exempel för att starta sitt eget företag eller liknande).[6]

Kravet på säkerhet vid behandling av personuppgifter m.m.
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. Lämpliga säkerhetsåtgärder kan bland annat inbegripa pseudonymisering och kryptering av personuppgifter.

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 39 till dataskyddsförordningen anges bland annat att personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

I skäl 75 till dataskyddsförordningen anges faktorer som bör 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.

Skäl 83 till dataskyddsförordningen ger ytterligare vägledning om den närmare innebörden av dataskyddsförordningens krav på säkerhet vid behandling av personuppgifter, bland annat att personuppgiftsansvariga bör utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Vid bedömningen av datasäkerhetsrisken bör man även beakta de risker som personuppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.

IMY:s bedömning

Utredningen i ärendet visar att regionen har tappat bort ett usb-minne. Usb-minnet lagrar okrypterade personuppgifter om hälsa och personnummer om 1 934 registrerade. Usb-minnet har inte återfunnits.

Personuppgiftsansvar
Regionen har angett att de är personuppgiftsansvariga för den aktuella behandlingen men menar samtidigt att de inte brustit i sin ansvarsskyldighet då överträdelsen beror på en anställds oaktsamhet.

---

[6] Se Europeiska dataskyddsstyrelsens (EDPB) riktlinje 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.0, antaget den 7 juli 2021, punkt 19 och artikel 24.1 i dataskyddsförordningen.

IMY konstaterar följande. Av artikel 4.7 i dataskyddsförordningen framgår bland annat att en personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Personuppgiftsansvariga ska enligt artikel 5.2 i dataskyddsförordningen ansvara för och kunna visa att principerna i artikel 5.1 efterlevs (principen om ansvarsskyldighet). Vidare framgår det av artikel 24.1 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.

IMY konstaterar att regionen bestämt ändamål och medel med behandlingen av personuppgifterna i förevarande fall, det vill säga hur och varför personuppgifterna ska behandlas. Det är således regionen som är personuppgiftsansvarig för behandlingen av personuppgifter.[7] Att regionen är personuppgiftsansvarig innebär att de ansvarar för att följa dataskyddsförordningen vid behandlingen av personuppgifterna. Det ansvaret omfattar även kraven på säkerheten för uppgifterna. Den behandling som sker inom verksamheten ansvarar den personuppgiftsansvarige för även om det är frågan om misstag eller felbedömning som skett av exempelvis en anställd. Det är först om den anställde agerar för andra ändamål som inte omfattas av arbetsgivarens ändamål som det kan bli frågan om att den anställde eller någon annan är personuppgiftsansvarig för behandlingen. I detta fall har både lagringen av känsliga personuppgifter på ett okrypterat usb och förlusten av usb-minnet skett inom ramen för den anställdes tjänst. Regionen är således ansvarig för att behandlingen av personuppgifterna skett i enlighet med dataskyddsförordningens krav på säkerhet.

Behandlingen har inneburit en hög risk

Som personuppgiftsansvarig ska regionen vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna med behandlingen, se artikel 32 i dataskyddsförordningen. Personuppgifterna som behandlas måste till exempel skyddas mot förlust, 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.[8]

Patienter får anses ha en hög förväntan på att obehöriga inte ska kunna ta del av de uppgifter som framkommer i kontakten med vården. Det eftersom patienter har rätt till en konfidentiell kontakt med vården.[9] Behandling av personuppgifter inom hälso- och sjukvården innebär generellt en hög risk för de registrerades fri- och rättigheter.

På det aktuella usb-minnet lagrar regionen uppgifter om hälsa som är känsliga personuppgifter. Behandling av känsliga personuppgifter kan innebära betydande risker för den personliga integriteten. Dessutom innehåller usb-minnet personnummer som anses vara särskilt skyddsvärda personuppgifter.[10] Behandlingen av uppgifterna på usb-minnet är därför av en sådan art att uppgifterna kräver ett starkt skydd.

---

[7] Jfr EDPB:s riktlinje 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.0, antaget den 7 juli 2021, punkt 19 och 27.
[8] Se skälen 75 och 76 till dataskyddsförordningen.
[9] Inom både enskild som allmän hälso- och sjukvårdsverksamhet skyddas uppgifter om en enskilds hälsotillstånd eller andra personliga förhållanden av tystnadsplikt, se 6 kap. 12 § patientsäkerhetslagen (2010:659) och 25 kap. 1 § offentlighets- och sekretesslagen (2009:400).
[10] Jfr artikel 87 i dataskyddsförordningen och 3 kap. 10 § dataskyddslagen.

Regionen har inte vidtagit tillräckliga säkerhetsåtgärder
IMY konstaterar att den aktuella behandlingen innebär att lagring skett av personuppgifter på ett usb-minne utan att dessa skyddats av lämpliga säkerhetsåtgärder som till exempel kryptering. Kryptering innebär att den skyddsvärda informationen omvandlas från ett läsbart till ett kodat format med hjälp av en krypteringsnyckel. Informationen blir då oläslig för alla som inte har tillgång till krypteringsnyckeln. Detta innebär att den skyddsvärda informationen inte kan utläsas direkt där denna lagras utan en krypteringsnyckel.

Av utredningen framgår att det direkt och ensamt av uppgifterna på det förlorade usb-minnet går att utläsa att det rör uppgifter om hälsa kopplade till patienters personnummer, det vill säga det går att identifiera att de registrerade varit föremål för vård och behandling. IMY konstaterar vidare att även om vissa av värdena är inskrivna som ettor och nollor som ska representera ja eller nej, så fråntar inte det att det rör sig om uppgifter om hälsa och som kan kopplas till en identifierbar person.

När personuppgifter behandlas på flyttbar lagringsmedia, till exempel usb, finns betydande risker att personuppgifter sprids på ett oavsiktligt sätt. De säkerhetsåtgärder som ska vidtas utifrån bedömning enligt artikel 32 i dataskyddsförordningen innebär att behandling av integritetskänsliga personuppgifter inte ska kunna gå förlorade, röjas obehörigen eller spridas på oavsiktligt sätt.

Regionen ansvarar som personuppgiftsansvarig för att dessa personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet, vilket inbegriper skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Att regionen lagrat hälsouppgifter på ett okrypterat usb-minne som de också tappat bort innebär att en påtaglig risk för att någon som inte har rätt att ta del av dem kan komma att få åtkomst till uppgifterna. Det innebär i sin tur att det även finns risk för att uppgifterna kan komma att spridas vidare. Regionen har därmed inte säkerställt en lämplig säkerhetsnivå i förhållande till risken för förlust, obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Sammantaget finner IMY att regionen inte vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen genom att regionen har använt ett flyttbart medium för lagring av känsliga personuppgifter utan att säkerställa att obehöriga inte kan ta del av dem och därefter förlorat kontrollen över usb-minnet. Regionen har därför behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Val av ingripande

Tillämpliga bestämmelser
Av artikel 58.2 och artikel 83.2 i dataskyddsförordningen framgår att IMY har befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83. Beroende på omständigheterna i det enskilda fallet ska administrativa sanktionsavgifter påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2, som till exempel föreläggande och förbud. Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om administrativa sanktionsavgifter ska påföras och vid bestämmande av avgiftens storlek. Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 istället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Medlemsstaterna får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter. Det framgår av artikel 83.7 i dataskyddsförordningen. 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 och artikel 83.4 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.

Sanktionsavgift ska påföras
IMY har ovan bedömt att regionen har överträtt artikel 32.1 i dataskyddsförordningen. Överträdelser av den bestämmelsen kan, som framgår ovan, föranleda sanktionsavgifter. IMY finner vid en samlad bedömning av de omständigheter som beskrivs under rubriken Sanktionsavgiftens storlek att det finns skäl att påföra nämnden en sanktionsavgift och att det därmed inte är fråga om en sådan mindre överträdelse att det finns skäl att i stället utfärda en reprimand.

Sanktionsavgiftens storlek
För överträdelser av bland annat artikel 32 i dataskyddsförordningen får sanktionsavgiften för offentliga myndigheter uppgå till högst 5 000 000 kronor. Det framgår av 6 kap. 2 § dataskyddslagen och artikel 83.4 i dataskyddsförordningen. I bedömningen av överträdelsens allvarlighet beaktar IMY i enlighet med artikel 83.2 g i dataskyddsförordningen att behandlingen har omfattat känsliga personuppgifter om hälsa.

Vidare beaktar IMY vad som framkommit om överträdelsens karaktär, svårighetsgrad och varaktighet utifrån vad som anges i artikel 83.2 a i dataskyddsförordningen. Överträdelsen har skett genom att regionen har lagrat okrypterade personuppgifter om patienter på ett usb-minne och förlorat kontrollen över usb-minnet. Det har inneburit att regionen inte har säkerställt en lämplig säkerhetsnivå i förhållande till risken för förlust, obehörigt röjande av eller obehörig åtkomst till personuppgifterna. Behandlingen har inneburit att ett större antal patienter kan identifieras direkt genom personnummer tillsammans med uppgifter om hälsa, vilket innebär en hög risk för de registrerades fri- och rättigheter. Att regionen inte har uppfyllt säkerhetskraven är allvarligt eftersom det är frågan om personuppgifter av sådan typ att uppgifterna kräver ett starkt skydd utifrån behandlingens art.

Det avser dessutom personuppgifter som skyddas av sekretess. Mot bakgrund av att regionen uppgett att det rör sig om 1 934 registrerade kan det även konstateras att överträdelsen berör ett stort antal registrerade.

IMY anser att det är en försvårande omständighet att usb-minnet inte återfunnits och det är oklart vilken spridning personuppgifterna har fått.

IMY bestämmer utifrån en samlad bedömning att regionen ska betala en administrativ sanktionsavgift på 200 000 (tvåhundratusen) kronor.

Detta beslut har fattats av den tillförordnade enhetschefen Linn Sandmark efter föredragning av juristen Anna Hellgren Westerlund. Vid den slutliga handläggningen av ärendet har enhetschefen Katarina Tullstedt medverkat. Vid handläggningen av ärendet har it- och informationssäkerhetsspecialisten Joyce Wong medverkat.

Linn Sandmark, 2023-04-26 (Det här är en elektronisk signatur)

Bilaga
Information om betalning av sanktionsavgift

Kopia till
Dataskyddsombudet
Klaganden

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.