Hälso- och sjukvårdsnämnden i Region Örebro län

Hälso-och sjukvårdsnämnden i Region Örebro län – tillsyn enligt dataskyddsförordningen

Datainspektionens beslut

Datainspektionen konstaterar att Hälso- och sjukvårdsnämnden i Region Örebro län mellan september 2019 och januari 2020 behandlade personuppgifter i strid med artikel 5, artikel 6 och artikel 9 i dataskyddsförordningen. Detta genom att ha publicerat känsliga personuppgifter på Region Örebro läns webbplats utan att det varit förenligt med principerna om ändamålsbegränsning och uppgiftsminimering, utan att det funnits laglig grund för det och i strid med förbudet mot att behandla känsliga personuppgifter. Hälso- och sjukvårdsnämnden i Region Örebro län har vid samma publicering även behandlat personuppgifter i strid med artikel 87 i dataskyddsförordningen och 3 kap. 10 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) genom att ha behandlat personnummer utan att ha stöd för det.

Datainspektionen konstaterar att Hälso- och sjukvårdsnämnden i Region Örebro län vid granskningen i februari 2020 befanns behandla personuppgifter i strid med artikel 32 i dataskyddsförordningen genom att inte ha vidtagit tillräckliga organisatoriska åtgärder för att se till att personuppgifter skyddas från otillåten publicering på regionens webbplats, såsom att upprätta skriftliga instruktioner och säkerställa att den som publicerar personuppgifter på webbplatsen gör detta i enlighet med instruktionerna.

Datainspektionen beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen och 6 kap. 2 § dataskyddslagen att Hälso- och sjukvårdsnämnden i Region Örebro län för överträdelserna av artikel 5, artikel 9 och artikel 32 i dataskyddsförordningen samt 3 kap. 10 § dataskyddslagen ska betala en administrativ sanktionsavgift på 120 000

kronor. Av detta belopp avser 80 000 kronor överträdelserna av artiklarna 5, 6 och 9 samt 3 kap. 10 § i dataskyddsförordningen och 40 000 kronor avser överträdelsen av artikel 32.

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Hälso- och sjukvårdsnämnden i Region Örebro län att upprätta skriftliga instruktioner och införa rutiner som säkerställer att den som publicerar personuppgifter på öppna webbplatser gör detta i enlighet med instruktionerna.

Redogörelse för tillsynsärendet

Datainspektionen tog emot ett klagomål mot Hälso- och sjukvårdsnämnden i Region Örebro län angående att en anmälan till JO mot rättspsykiatriska kliniken i Örebro hade publicerats i sin helhet på regionens öppna webbplats. Publiceringen hade skett inför ett nämndsammanträde den 25 september 2019. Anmälan innehöll anmälarens identitetsuppgifter (inklusive personnummer), kontaktuppgifter, uppgift om att anmälaren var inlagd på den rättspsykiatriska kliniken och uppgift om att anmälaren var föremål för urinprovtagning. Med anledning av detta beslutade Datainspektionen i slutet av januari 2020 att inleda en tillsyn mot Hälso- och sjukvårdsnämnden i Region Örebro län i syfte att undersöka nämndens hantering av personuppgifter vid webbpubliceringar. I samband med att tillsynen inleddes och Datainspektionen uppmärksammade nämnden om publiceringen tog nämnden bort den publicering som klagomålet rörde.

Hälso- och sjukvårdsnämnden i Region Örebro län har i huvudsak uppgett följande.

Den publicerade handlingen togs genast bort från den öppna webbplatsen. Vidare granskades alla publicerade kallelser och protokoll i syfte att kontrollera så att ytterligare röjande inte hade skett. Därefter gjordes en personuppgiftsincidentsanmälan till Datainspektionen, en intern avvikelseanmälan upprättades och det undersöktes vad som kunde göras för att något liknande inte skulle hända igen.

Region Örebro län publicerar normalt sett personuppgifter i kallelser och protokoll på sin webbplats som hänför sig till förtroendevalda politiker eller tjänstepersoner i deras tjänste-/förtroendeuppdrag. Vid webbpublicering

bedöms Region Örebro län kunna åberopa allmänt intresse för att publicera protokoll och kallelser, inklusive personuppgifter, utifrån artikel 6 i dataskyddsförordningen samt 2 kap. 2 § dataskyddslagen. Känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen och 3 kap. 3 § dataskyddslagen ska aldrig publiceras på regionens webbplats. I det aktuella fallet borde publicering inte ha skett.

Hälso- och sjukvårdsnämnden saknar skriftliga rutiner rörande publicering av handlingar och personuppgifter på webbplatsen. Det är ett fåtal personer som har som arbetsuppgift att publicera hälso- och sjukvårdsnämndens kallelser och protokoll på webbplatsen. Rutiner kring publiceringen delges muntligt. I detta fall har de muntliga rutinerna inte följts och handlingen publicerades av misstag.

Region Örebro län har påbörjat arbetet med att skapa skriftliga riktlinjer och rutiner för delgivning av kallelser och protokoll till förtroendevalda samt för publicering på webbplatsen.

Övrigt som framkommit i ärendet

Datainspektionen har gått igenom den information som nämnden lämnat om händelsen i en personuppgiftsanmälan (dnr PUI-2020-339). Nämnden uppger i denna handling bland annat att incidenten inträffade på grund av ”Mänskliga faktorn: fel i det enskilda fallet” (ett förtryckt svarsalternativ), att handlingen tagits bort från den externa webben, att borttagning av handlingen åtföljdes av en omedelbar granskning av alla publicerade kallelser och protokoll för att säkerställa att röjande inte har förekommit på annat sätt eller i andra handlingar, att ett datum bestämts för information och genomgång till berörd personalgrupp kring regler för publicering på webben, samt att den registrerade informerats om incidenten.

I en bilaga till anmälan om personuppgiftsincident skrev regionen följande. ”Region Örebro län anser det vara mycket viktigt att personuppgifter behandlas korrekt och i enlighet med vid varje tidpunkt gällande regler. Därför strävar Region Örebro län efter att i de olika stegen i beredningen av ärenden, uppmärksamma förekomsten av personuppgifter i olika typer av handlingar, och att om det inte är nödvändigt att de finns där, antingen ta bort dem eller presentera dem i en sådan form att de inte kan härledas till enskild person. Detta arbete sker systematiskt och igenom ett antal beredningssteg./…/I förevarande fall har det emellertid varit så att de

aktuella uppgifterna till följd av ett misstag, som inte på sedvanligt sätt har uppmärksammats i beredningsgången, har följt med ut i publiceringen på den publika webben.”

Motivering av beslut

Datainspektionen konstaterar att det bland de personuppgifter som publicerades på Region Örebro läns öppna webbplats funnits uppgifter som varit känsliga enligt artikel 9 i dataskyddsförordningen. Detta gäller för uppgiften om att den registrerade är intagen på den rättspsykiatriska kliniken och att hen är föremål för urinprovstagning. Detta då den förstnämnda uppgiften avslöjar att personen kan lida av en allvarlig psykisk störning och den sistnämnda uppgiften att personen har eller har haft en drogproblematik. Därmed utgör de uppgifter om hälsa. Vidare har personnummer omfattats av publiceringen.

Rättslig reglering

Personuppgifter får endast behandlas om det finns en rättslig grund för det som framgår av artikel 6 i dataskyddsförordningen. Ett sådant rättsligt stöd kan till exempel bestå i att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse, till exempel att ge allmänheten insyn i den kommunala verksamheten. Behandling av känsliga personuppgifter är som huvudregel förbjuden och sådana personuppgifter får endast behandlas om behandlingen omfattas av ett undantag i artikel 9 i dataskyddsförordningen. Personnummer får endast behandlas med stöd av 3 kap. 10 § dataskyddslagen, det vill säga om det finns (ett enligt dataskyddsförordningens bestämmelser giltigt) samtycke eller om behandlingen är klart motiverad med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

De som behandlar personuppgifter måste förutom att ha en rättslig grund alltid uppfylla de grundläggande principer som framgår av artikel 5 i dataskyddsförordningen. Bland annat får personuppgifter endast användas för särskilda, uttryckligt angivna och berättigade ändamål (principen om ändamålsbegränsning) och det får inte behandlas fler personuppgifter än nödvändigt för ändamålen (uppgiftsminimeringsprincipen). Av artikel 32

följer att den personuppgiftsansvarige har att vidta lämpliga tekniska och organisatoriska åtgärder för personuppgifter för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter. Vidare ska den personuppgiftsansvarige, enligt artikel 32.4, vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige.

Datainspektionens bedömning av publiceringen

Datainspektionen bedömer att publiceringen av en privatpersons korrespondens till en myndighet gått utöver ett tänkbart ändamål med att publicera delar av det aktuella ärendet på webben (att ge allmänheten insyn i den kommunala verksamheten). Därmed har det inte funnits något särskilt, uttryckligt angivet och berättigat ändamål med publiceringen av de aktuella personuppgifterna. Vidare har det inte funnits någon laglig grund för att publicera personuppgifterna och publiceringen har inte omfattats av något undantag mot förbudet att behandla känsliga personuppgifter. Personnummer har publicerats utan att de villkor som framgår av 3 kap. 10 § dataskyddslagen varit uppfyllda.

Hälso- och sjukvårdsnämnden har enbart arbetat med muntliga instruktioner till de medarbetare som ansvarat för publicering av nämndens handlingar på webben. Publiceringen borde ha föregåtts av en bedömning av om den var tillåten enligt dataskyddsförordningen. Att så inte har skett tyder på att nämnden brustit i instruktionerna till de som arbetar under nämndens överinseende. Det innebär att nämnden inte vidtagit lämpliga organisatoriska säkerhetsåtgärder för att skydda mot otillåten publicering av personuppgifter på webben.

Datainspektionen har i en rad beslut om kommuners webbpubliceringar enligt personuppgiftslagen[1] uttalat att en lämplig organisatorisk åtgärd för att skydda personuppgifter från otillbörlig publicering är skriftliga rutiner för webbpublicering. Sådana rutiner ska användas av personalen och bör fastställa när personuppgifter får publiceras, vem som ska göra

[1] Personuppgiftslagen (1998:204), PuL, trädde i kraft den 24 oktober 1998 och upphörde att gälla den 24 maj 2018. Datainspektionen var tillsynsmyndighet enligt PuL fram till att Dataskyddsförordningen började tillämpas den 25 maj 2018.

bedömningen, hur länge uppgifterna ska bevaras på webben, arbetsrutin för maskering av känsliga eller sekretessbelagda uppgifter, hantering av länkade dokument samt angivande av vem som ansvarar för publicering och eventuell borttagning av uppgifter.[2] Andra lämpliga åtgärder kan vara att se till att personalen får tillräcklig utbildning i dataskyddsförordningen och hur den ska arbeta så att personuppgifter inte hanteras i strid med regelverket. Sådan utbildning kan säkerställa att den som publicerar personuppgifter på webbplatsen gör detta i enlighet med instruktionerna från den personuppgiftsansvarige.

De rutiner som hälso- och sjukvårdsnämnden haft har inte räckt till för att skydda personuppgifter från publicering i strid med dataskyddsförordningen. Tillräckliga åtgärder har inte vidtagits för att säkerställa att de som publicerar personuppgifter under nämndens överinseende gör det i enlighet med nämndens instruktioner för publiceringen.

Datainspektionen konstaterar därför att Hälso- och sjukvårdsnämnden i Region Örebro län har överträtt artiklarna 5, 6, 9 och 32 i dataskyddsförordningen, samt 3 kap. 10 § dataskyddslagen.

Val av ingripande

Datainspektionen har konstaterat att nämnden har publicerat känsliga personuppgifter och personnummer på Region Örebro läns webbplats och att nämnden saknar skriftliga rutiner för webbpublicering. Den publicering som har skett har saknat berättigat ändamål och laglig grund. Publiceringen har inte omfattats av något av undantagen till förbudet mot att behandla känsliga personuppgifter. Detta innebär att nämnden har behandlat personuppgifter i strid med principerna om ändamålsbegränsning och uppgiftsminimering i artikel 5 i dataskyddsförordningen, bestämmelsen om laglig behandling i artikel 6 och förbudet mot behandling av känsliga personuppgifter i artikel 9. Publiceringen av personnummer uppfyller inte villkoren i 3 kap. 10 § dataskyddslagen och strider därför mot den bestämmelsen.

I artikel 58 i dataskyddsförordningen anges Datainspektionens samtliga befogenheter. Datainspektionen har vid överträdelser av

[2] Se till exempel DI-1309-2011, DI-1787-2011 och DI-1057-2016.

dataskyddsförordningen ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a -j, bland annat reprimand, föreläggande och sanktionsavgifter.

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. 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.

Sanktionsavgift ska utgå
Datainspektionen har bedömt att nämnden har överträtt artiklarna 5, 6, 9 och 32 i dataskyddsförordningen samt 3 kap. 10 § dataskyddslagen, antagen på grundval av artikel 87 i dataskyddsförordningen. Dessa artiklar omfattas av artiklarna 83.4 och 83.5. Vid en överträdelse av dessa ska tillsynsmyndigheten överväga att påföra administrativa sanktionsavgifter utöver, eller istället för, andra korrigerande åtgärder.

Datainspektionen bedömer att det inte är fråga om en mindre överträdelse. Detta mot bakgrund av att de personuppgifter som publicerades var känsliga och rörde en patient. Vidare kunde personen inte rimligen förvänta sig att dennes korrespondens gjordes tillgänglig för en stor krets. Dessutom var personuppgifterna publicerade under en längre tid utan att det upptäcktes av nämnden. Det finns inte skäl att ersätta sanktionsavgiften med någon annan korrigerande åtgärd. Hälso- och sjukvårdsnämnden ska således påföras en administrativ sanktionsavgift.

Bestämmande av sanktionsbeloppets storlek
Enligt artikel 83.1 i dataskyddsförordningen ska varje tillsynsmyndighet säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande.

För myndigheter gäller enligt 6 kap. 2 § andra stycket dataskyddslagen att sanktionsavgiften ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen och högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5. Överträdelser av artikel 5, 6, 9 och 3 kap. 10 § dataskyddslagen (som antagits på grundval av artikel 87) omfattas av de högre sanktionsavgifterna enligt artikel 83.5 och

överträdelser av artikel 32 omfattas av det lägre maxbeloppet enligt artikel 83.4.

I artikel 83.2 i dataskyddsförordningen anges faktorer som ska beaktas vid bestämmande av sanktionsavgiftens storlek. Dessa faktorer är bland annat a) överträdelsens karaktär, svårighetsgrad och varaktighet, b) om överträdelsen skett med uppsåt eller genom oaktsamhet, c) de åtgärder som den personuppgiftsansvarige har vidtagit för att lindra den skada som de registrerade lidit, d) graden av ansvar hos den personuppgiftsansvarige med beaktande av de tekniska åtgärder som genomförts i enlighet med artikel 32, g) de kategorier av personuppgifter som omfattas av överträdelsen, h) det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige anmälde överträdelsen.

Vid Datainspektionens bedömning av sanktionsavgiftens storlek har hänsyn tagits till följande.

Överträdelsen har avsett känsliga personuppgifter avseende en person i beroendeställning för vilken publiceringen av uppgifterna kan ha fått allvarliga följder. Vidare har uppgifterna legat publicerade öppet på regionens webbplats under en längre tid. Att det saknats lämpliga tekniska och organisatoriska åtgärder för att se till sådana personuppgifter inte publiceras utgör en risk för att liknande händelser ska inträffa igen. Avsaknaden av lämpliga säkerhetsåtgärder avspeglar sig i att nämnden inte själv upptäckt den felaktiga publiceringen. Emellertid har publiceringen inte skett avsiktligt och det finns inte något som tyder på att fler än en person i realiteten skulle ha drabbats av felaktiga publiceringar av känsliga personuppgifter. Till detta kommer att nämnden så fort den fått kännedom om händelsen agerat genom att ta bort den publicerade handlingen, informera den registrerade och informera den berörda personalen samt att det påbörjats ett arbete med att ta fram skriftliga rutiner. Datainspektionen konstaterar även att regionen har gjort en personuppgiftsincidentsanmälan för nämndens räkning till Datainspektionen och följt de föreskrifter som finns i det avseendet.

Publiceringen av personuppgifter på nämndens öppna webbplats avser ett och samma agerande och omfattar överträdelse av artiklarna 5, 6 och 9 i dataskyddsförordningen samt 3 kap. 10 § dataskyddslagen.

Sanktionsavgiften för överträdelsen av artikel 32 avser nämndens organisatoriska säkerhetsåtgärder vid publicering på öppna webbplatser och fastställs därmed separat.

Datainspektionen bestämmer utifrån en samlad bedömning att Hälso- och sjukvårdsnämnden i Region Örebro län ska betala en administrativ sanktionsavgift på 120 000 kronor för överträdelserna av artiklarna 5, 6, 9 och 32 i dataskyddsförordningen och 3 kap. 10 § dataskyddslagen. Av detta belopp avser 80 000 kronor överträdelserna av artiklarna 5, 6 och 9 i dataskyddsförordningen samt 3 kap. 10 § i dataskyddslagen och 40 000 kronor avser överträdelsen av artikel 32 i dataskyddsförordningen.

Föreläggande om ytterligare organisatoriska åtgärder
Enligt artikel 58.2 d har Datainspektionen befogenhet att förelägga en personuppgiftsansvarig att se till att en behandling sker i enlighet med dataskyddsförordningens bestämmelser. Det framgår av artikel 58.2 att administrativa sanktionsavgifter kan kombineras med förelägganden. Hälso- och sjukvårdsnämnden har inte vidtagit tillräckliga organisatoriska åtgärder enligt artikel 32 i dataskyddsförordningen för att se till att personuppgifter skyddas från otillåten publicering på regionens webbplats, såsom att upprätta skriftliga instruktioner och säkerställa att den som publicerar personuppgifter på webbplatsen gör detta i enlighet med instruktionerna.

Hälso- och sjukvårdsnämnden i Region Örebro län ska därför föreläggas att upprätta skriftliga instruktioner och införa rutiner som säkerställer att den som publicerar personuppgifter på öppna webbplatser gör detta i enlighet med instruktionerna.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av [juristen] Elin Hallström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Malin Blixt och enhetschefen Katarina Tullstedt medverkat. It-säkerhetsspecialisten Magnus Bergström har deltagit i de bedömningar som rör informationssäkerhet.

Lena Lindgren Schelin, 2020-05-11 (Det här är en elektronisk signatur)

Bilaga
Hur man betalar sanktionsavgift

Kopia för kännedom till:
Dataskyddsombudet

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.