Stockholms läns landsting

3

Tillsättning av dataskyddsombud för hälso- och sjukvårdsnämndens personuppgiftsbehandlingar

HSN 2018-0456

Hälso- och sjukvårdsnämnden
Hälso- och sjukvårdsförvaltningen
Styrning och ekonomi
Lenah Hedberg

TJÄNSTEUTLÅTANDE
2018-04-26

HSN 2018-0456

Hälso- och sjukvårdsnämnden

Tillsättning av dataskyddsombud för hälso- och sjukvårdsnämndens personuppgiftsbehandlingar

Ärendebeskrivning

Den 25 maj 2018 kommer Personuppgiftslagen att ersättas av det EU-gemensamma Dataskyddsdirektivet (GDPR). I och med detta ställs krav på bland annat myndigheter att ersätta dagens personuppgiftsombud (PUO) med dataskyddsombud (DSO).

Beslutsunderlag

Hälso- och sjukvårdsdirektörens tjänsteutlåtande
PM Beslutsunderlag Dataskyddsombud 2018-03-15

Förslag till beslut

Hälso- och sjukvårdsnämndenHälso- och sjukvårdsnämnden beslutar

att tillsätta Dan Billtorp och Lenah Hedberg som dataskyddsombud med särskilt ansvar för de personuppgiftsbehandlingar som hör till hälso- och sjukvårdsförvaltningen

att tillsätta Peter Gröön som dataskyddsombud med särskilt ansvar för de personuppgiftsbehandlingar som hör till smittskyddsverksamheten

att uppdra till hälso- och sjukvårdsdirektören att anmäla dessa till Datainspektionen

att omedelbart justera beslutet.

Förvaltningens motivering till förslaget

Hälso- och sjukvårdsförvaltningen har över 150 personuppgiftsregister varav cirka 130 stöds av IT-systemlösningar. Dataskyddsombudet ska bland annat övervaka att förvaltningen efterlever förordningen, informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda om deras skyldigheter enligt förordningen. Dataskyddsombudet ansvarar också för att hålla en uppdaterad förteckning av

personuppgiftsbehandlingarna och ska vara kontaktperson till Datainspektionen som är tillsynsmyndighet.

För att kunna uppfylla alla de krav som den nya dataskyddsförordningen ställer på förvaltningen avseende informationssäkerhet vid behandling av personuppgifter och att tillgodose de registrerades rättigheter avseende registerutdrag och annan information krävs att ett antal personer i organisationen samverkar. Ett förslag till virtuell organisation för att sköta uppdraget finns preciserat och motiverat i dokumentet ”Beslutsunderlag Dataskyddsombud 2018-03-15 ”. För att på bästa sätt säkerställa att personuppgiftsbehandling är korrekt och laglig föreslår förvaltningen att nämnden enligt Europaparlamentets och rådets förordning (EU) 2016/679 artikel 37 pkt 1 utser tre dataskyddsombud.

Ekonomiska konsekvenser
Beslutet i sig medför inga ekonomiska konsekvenser men underlåtenhet att följa och tillämpa den nya dataskyddsförordningen kan medföra att förvaltningen kan tilldömas viten.

Konsekvenser för patientsäkerhet
Förslaget till beslut medför oförändrade konsekvenser för patientsäkerheten.

Konsekvenser för jämlik och jämställd vård
Förslaget till beslut medför oförändrade konsekvenser för jämlik och jämställd vård.

Miljökonsekvenser
Förslaget medför oförändrade konsekvenser för miljön.

Barbro Naroskyin
Hälso- och sjukvårdsdirektör

Margareta Tufvesson
Avdelningschef

Beslutet ska skickas till
Datainspektionen

Godkänd av Barbro Naroskyin, 2018-04-26

Verksamhetsstyrning och stöd
Styrning och ekonomi

PM
2018-03-15

Handläggare Lenah Hedberg
Telefon 08-123 131 68
E-post lenah.hedberg@sll.se

Beslutsunderlag Dataskyddsombud DSO

Bakgrund

Datalagen infördes 1973 i Sverige. Syftet med lagen var att säkerställa medborgarnas personliga integritet. Samtliga personuppgiftsbehandlingar skulle därmed anmälas och godkännas hos Datainspektionen.
PUL - personuppgiftslagen började gälla den 24 oktober 1998. Lagen infördes i EU. s samtliga medlemsstater men gav utrymme för lokala anpassningar. Detta har inneburit att den svenska lagstiftningen som exempelvis patientdatalagen har haft företräde vid tolkning av lagens tillämpning.
I och med att PUL infördes fanns möjlighet för myndigheter att utse en eller flera PuO (personuppgiftsombud). PuO. s uppgift var och är att föra register över myndighetens samtliga personuppgiftsbehandlingar, samt se till att det finns rutiner för att ta ut information ur myndighetens register efter förfrågningar från allmänheten. Uppgifter skall också lämnas till andra myndigheter som har rätt att få ut information ur systemen exempelvis Rättsmedicinalverket och Polisen. PuO.s uppgift är också att i möjligaste mån minimera upplägg av och uppgifter i register.

I och med att det inom ramen för PUL funnits möjligheter för EU:s medlemsstater att göra lokala anpassningar, har man upplevt att det är svårt med olika lagstiftning i olika länder. PUL är heller inte anpassad till dagens databehandlingar och kräver en modernisering. Därför togs ett förslag till en allmän dataskyddsförordning fram i januari 2012. Ett nytt dataskyddsdirektiv antogs 27 april 2016. En följd av detta är att all lagstiftning inom tillämpningsområdet, för Hälso- och sjukvårdsförvaltningens del exempelvis patientdatalagen, måste ses över och anpassas.

Den 25 maj 2018 kommer EU:s gemensamma dataskyddsdirektiv GDPR (General Data Protection Regulation) att träda i kraft. I samband med detta kommer också Datainspektionen att få en ny roll.

Krav i GDPR (Dataskyddsförordningen)

- Skarpare krav kommer att ställas på ansvariga myndigheter och företag på att leva upp till de krav som ställs i och med införandet av den nya GDPR.
- Personuppgiftsansvarig ska vidta lämpliga åtgärder för att till den registrerade kunna tillhandahålla all information och all kommunikation vilket avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med klart och tydligt språk
- Säkerhet för uppgifterna inkl. skydd mot förlust förstöring/skada genom olyckshändelse ska säkerställas med lämpliga tekniska/organisatoriska åtgärder
- Lämpliga åtgärder och strategier ska genomföras för dataskydd
- Information ska inte lagras längre än nödvändigt och inte i en form som möjliggör identifiering längre än nödvändigt
- Information ska tillhandahålla skriftligt och när så är lämpligt i elektronisk form.
- Den registrerade har rätt att av den personuppgiftsansvarige få information rättad utan onödigt dröjsmål och den personuppgiftsansvarige ska meddela samtliga som kan beröras av rättelsen och därefter underrätta den registrerade om vilka åtgärder som vidtagits.
- Den registrerade har rätt att komplettera ofullständiga personuppgifter bl. a genom att tillhandahålla kompletterande information
- Om den registrerade lämnar begäran i elektronisk form ska informationen om möjligt tillhandahållas i elektronisk form
- Uppgifter ska lämnas utan dröjsmål och senast en månad efter att begäran mottagits
- Rätt till överföring direkt från en personuppgiftsansvarig till en annan när detta är tekniska möjligt
- Personuppgiftsincidenter ska utan dröjsmål eller senast inom 72 timmar meddelas tillsynsmyndigheten, görs inte anmälan inom 72 timmar måste det motiveras

- Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs enligt GDPR.
- Tillsynsmyndigheten kan besluta om korrigerande befogenheter
- Administrativa sanktionsavgifter upp till 20 Milj Euro eller 4% av den globala omsättningen (för myndigheter föreslås max 20 miljoner kr)
- Skadestånd ska kunna utdömas

De flesta personuppgiftsbehandlingar i HSF:s verksamhet stödjer sig i första hand på kraven i patientdatalagen. (PDL)

Nedanstående texter är hämtade ur:
Europaparlamentets och rådets förordning (EU) 2016/679

Definition av dataskyddsombud

Dataskyddsombud ska i ramlagen definieras som en fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.

Krav på dataskyddsombud

Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Skälen för utredningens förslag

Den personuppgiftsansvarige ska utnämna ett eller flera data-skyddsombud, offentliggöra ombudens kontaktuppgifter och meddela tillsynsmyndigheten vem/vilka meddela tillsynsmyndigheten personen/personernas kontaktuppgifter.

Dataskyddsombud ska utnämnas på grundval av sina yrkesmässiga kvalifikationer, sin sakkunskap om lagstiftning och praxis rörande dataskydd och sin förmåga att fullgöra de uppgifter som åläggs dataskyddsombud.

Alla personuppgiftsansvariga ska utse dataskyddsombud

I dataskyddsförordningen föreskrivs ingen allmän skyldighet för personuppgiftsansvariga att utse dataskyddsombud. Däremot gäller enligt artikel 37.1 sådan skyldighet för myndigheter och andra offentliga organ. Dataskyddsombud ska också utses av personuppgiftsansvariga eller

personuppgiftsbiträden vilkas kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning. Detsamma gäller om kärnverksamheten består av behandling i stor omfattning av känsliga personuppgifter.

Ett eller flera dataskyddsombud ska utses

I större myndighetsorganisationer kan det vara svårt för en enda person att ensam utföra de uppgifter som ett dataskyddsombud ska ha i framtiden. Flera dataskyddsombud bör därmed kunna utses för en behörig myndighet.

Dataskyddsombudens kvalifikationer

Vilka kvalifikationer och vilken kunskap en person bör ha för att kunna utses till dataskyddsombud varierar naturligtvis. Den nödvändiga nivån på sakkunskap fastställas med utgångspunkt i den personuppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas. Det kan således krävas mer av ett dataskyddsombud i en stor organisation som behandlar många känsliga personuppgifter och för olika ändamål än av ett ombud i en mindre organisation där en begränsad mängd uppgifter behandlas. Det ska ligga i varje personuppgiftsansvarigs intresse att dataskyddsombudet har tillräcklig kunskap, erfarenhet och förmåga att utföra sina uppgifter.

Dataskyddsombud vara fysiska personer. Det kan vara en av den personuppgiftsansvariges medarbetare som fått särskild utbildning beträffande lagstiftning och praxis i fråga om dataskydd. Ett dataskyddsombud måste få relativt omfattande insyn i den behöriga myndighetens verksamhet. Det medför att dataskyddsombud i de allra flesta fall kommer att utses bland den personuppgiftsansvariges anställda. Det bör dock inte införas något förbud mot att anlita dataskyddsombud utanför den egna organisationen.

Information om dataskyddsombuden

Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten vem som har utsetts till dataskyddsombud och när ombudet entledigas. Det är viktigt att tillsynsmyndigheten får information om det, eftersom ombuden bl.a. ska ha till uppgift att samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den i vissa fall.

Dataskyddsombudets arbetsuppgifter

Dataskyddsombud ska informera och ge råd till den personuppgiftsansvarige och de anställda som utför personuppgiftsbehandling om deras skyldigheter enligt direktivet och annan unionsrätt eller medlemsstaternas bestämmelser om dataskydd. Ombuden ska också övervaka efterlevnaden av dessa regler och av den personuppgiftsansvariges strategier för skyddet av

personuppgifter. I dataskyddsombudens arbetsuppgifter ingår vidare att på begäran ge råd beträffande konsekvensbedömningar och att övervaka genom-förandet av dem. Dataskyddsombud ska samarbeta med tillsyns-myndigheten och fungera som kontaktpunkt för den i frågor som rör behandling av personuppgifter

Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Den personuppgiftsansvarige ska stödja dataskyddsombudet i utförandet av de arbetsuppgifter som ingår i ombudets ansvarsområde. Det ska göras genom att den personuppgiftsansvarige tillhandahåller de resurser som krävs för att ombudet ska kunna fullgöra uppgifterna och ger ombudet tillgång till personuppgifter och IT-system. Den personuppgiftsansvarige ska också se till att dataskyddsombudets kunskaper upprätthålls. Dataskyddsombudet bör kunna utföra sina uppdrag och uppgifter på ett oberoende sätt.

Ombudens arbetsuppgifter enligt direktivet

Dataskyddsombudens roll påminner i stora delar om personupp-giftsombudens. Dataskyddsombuden har genom direktivet delvis fått nya arbetsuppgifter och en något förändrad roll i förhållande till personuppgiftsombudet. Flertalet av de arbetsuppgifter som ska anförtros dataskyddsombud har t.ex. karaktären av intern rådgivning. Dataskyddsombuden har också fått ett tydligare uppdrag att bistå tillsynsmyndigheten.
Dataskyddsombud ska självständigt kontrollera att de personuppgiftsansvariga behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör de skyldigheter som åligger personuppgiftsansvariga. Kravet på självständighet infördes i personuppgiftslagen eftersom det nu gällande dataskyddsdirektivet anger att ombudet ”på ett oberoende sätt” ska kunna kontrollera den personuppgiftsansvarige. Självständighetskravet innebär att den personuppgiftsansvarige inte bör utse ett ombud som har en alltför underordnad ställning i organisationen. För att ombuden ska vara oberoende på det sätt som direktivet förutsätter måste han eller hon också ha tillräckliga kvalifikationer och kunskaper för att kunna utföra sina arbetsuppgifter på ett självständigt sätt.

Dataskyddsombudens kontroll ska omfatta ansvarstilldelning, information till och utbildning av personal som deltar i behandlingen och tillhörande granskning. Ombuden bör också påpeka eventuella brister för de personuppgiftsansvariga så att de blir medvetna om dem och har möjlighet att vidta lämpliga åtgärder.

Dataskyddsombud bör informera och ge råd till personuppgiftsansvariga och de som behandlar personuppgifter under dennes ledning om deras skyldigheter enligt ramlagen och andra författningar som rör personuppgiftsbehandling. Det handlar främst om att göra den

personuppgiftsansvarige och medarbetarna medvetna om vad de i olika situationer är skyldiga att göra, t.ex. att informera registrerade, att ha säkerhetsrutiner och att dokumentera personuppgiftsbehandlingen. Om den personuppgiftsansvarige begär det ska ombudet ge råd vid en konsekvensbedömning och kontrollera att bedömningen genomförs på rätt sätt. Dataskyddsombud ska även samarbeta med och fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling av personuppgifter. Samarbetet innebär också att ombuden, när det är lämpligt, ska samråda med tillsynsmyndigheten även i andra frågor som rör personuppgiftsbehandling.

Dataskyddsombudens roll påminner om internrevisorers. För att ombuden ska kunna utöva intern kontroll bör de inte ges arbetsuppgifter som kan komma i konflikt med kontrolluppgiften. Det kan t.ex. vara olämpligt att låta dataskyddsombud utbilda personalen eller ansvara för att den får annan information, eftersom det är åtgärder som omfattas av den interna granskningen. Av samma skäl är det inte lämpligt att dataskyddsombud ges i uppdrag att föra det register över personuppgiftsbehandlingar som den personuppgiftsansvarige ska föra.

Bör dataskyddsombud även ges andra arbetsuppgifter?

Dataskyddsombuden fungerar som kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter på samma sätt som personuppgiftsombuden. Den personuppgiftsansvarige ska göra dataskyddsombudens kontaktuppgifter tillgängliga för registrerade, vilket talar för att dataskyddsombuden bör ha samma roll i förhållande till enskilda som personuppgiftsombud har i dag.

Enligt personuppgiftslagen ska ett personuppgiftsombud anmäla till tillsynsmyndigheten om han eller hon misstänker att den personuppgiftsansvarige bryter mot gällande bestämmelser och inte vidtar rättelse. Någon sådan skyldighet föreskrivs inte i direktivet. Det är viktigt att dataskyddsombud uppmärksammar tillsynsmyndigheten på eventuella problem och brister, särskilt om den personuppgiftsansvarige inte rättar sig efter ombudets påpekanden. Dataskyddsombuden bör därför, som personuppgiftsombuden i dag, ha i uppdrag att anmäla eventuella överträdelser till tillsynsmyndigheten.

Dataskyddsombudens verksamhet ska underlättas

För att dataskyddsombuden ska kunna utföra sina arbetsuppgifter krävs det att de personuppgiftsansvariga gör det möjligt och tillhandahåller de resurser som ombuden behöver. Den personuppgiftsansvarige ska t.ex. göra ombudet delaktig i frågor och beslut som rör behandling av personuppgifter. Ombuden bör också få tillgång till all dokumentation gällande personuppgiftsbehandlingen och, i den utsträckning det behövs, tillgång till de

personuppgifter som behandlas. Den personuppgiftsansvarige bör även se till att ombudet ges utrymme för vidareutbildning och annan kunskapsinhämtning.

Registerutdrag

I nuläget kommer förfrågningar från allmänheten, från andra myndigheter som exempelvis polisen, socialtjänsten, andra landsting, rättsmedicinalverket mm. Registerutdragen tas i dagsläget ut från Liston, GVR, ARV och Tand och systemen som handhas av Smittskyddsenheten. I och med att GDPR träder i kraft så kan man misstänka att fler personer kommer att kontakta förvaltningen för att få information om vilka system de finns registrerade i.

Innan registerutdrag skickas ska dels en bedömning göras om personen som begär utdraget har rätt till det och menprövning av innehållet i informationen ska ibland göras innan informationen skickas ut. Registerutdrag till rättsmedicinalverket ska expedieras inom 24 timmar. Förfrågan från polismyndigheten skall besvaras skyndsamt, men uppgifter får endast lämnas ut om misstankar finns att brott begåtts som kan ge fängelse i minst ett år. Information till de registrerade (patienterna) ska ske utan dröjsmål och under alla omständigheter senast inom en månad efter det att begäran inkommit.

För att förvaltningen ska kunna leva upp till ovan angivna krav bör det finnas ett antal personer som kan samarbeta för att ta ut underlag och också kunna vara back-up vid sjukdom, kurser och semester.

För de system som kan bli aktuella att ta ut registerutdrag ifrån ansvarar objektägaren eller motsvarande för att adekvata resurser avsätts för att möta befolkningens rättigheter till information och har ett uttalat ansvar för att sköta uttagen och utskick av registerutdrag.

Förslag på virtuell arbetsorganisation

Dataskyddsombud 3 personer
Informationssäkerhetssamordnare 1 person
Arkivansvarig 1 person
IT-arkitekt (IT-arkitektgrupp)
Jurist 1 person
Förvaltningsledare verksamhet (eller motsvarande om objektet inte är PM3-etablerat)
Personer som handhar uttag och utskick av registerutdrag på uppdrag av objektägaren eller motsvarande