Tobias Lindbergh, utredare Systemförvaltning
Nils Ahlberg, Objekt- och tjänsteägare FO Lab

2018-05-31

Dnr: -

Hantering av Personuppgiftsbiträdesavtal inom SÖR

Inledning

Allmänt

Dataskyddsförordningen är en EU-lag som ersätter den nuvarande svenska personuppgiftslagen (PuL). Dataskyddsförordningen innehåller regler om hur man får behandla personuppgifter och syftar till att skydda de personer vars uppgifter man behandlar. Dataskyddsförordningen kallas oftast GDPR som är förkortningen av det engelska namnet general data protection regulation. I och med att dataskyddsförordningen är en EU-lag kommer alla länder i EU att ha samma lagstiftning.

Personuppgift

I princip alla tänkbara typer av **personuppgifter** som direkt eller indirekt kan kopplas till en person som är i livet omfattas av lagen. På samma sätt omfattas i princip nästan all typ av hantering av dessa personuppgifter, så kallad **personuppgiftsbehandling**. Alltså allt vi kan tänkas göra med personuppgifterna, exempelvis insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning och läsning. Personuppgiftsansvarig är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till.

Personuppgiftsansvarig

I Region Östergötland är det regionstyrelsen som är personuppgiftsansvarig. Den personuppgiftsansvarige måste se till att behandlingen sker i enlighet med dataskyddsförordningens samtliga bestämmelser. Inför införandet av GDPR har Region Östergötland framför allt arbetat med att tolka den nya lagen och omvandla det till riktlinjer och vägledning. Ett antal nya riktlinjer har skapats och finns tillgängliga i Dokumenta. Ett antal större, strategiska system har inventerats och kartlagts utifrån det nya regelverket. Den som är personuppgiftsansvarig kan överlåta ansvaret för den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

Personuppgiftsbiträde

Den personuppgiftsansvarige måste se till att behandlingen sker i enlighet med dataskyddsförordningens samtliga bestämmelser. Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ. Det ska tecknas ett

personuppgiftsbiträdesavtal mellan personuppgiftsansvarig och personuppgiftsbiträde. I Region Östergötland är det dataskyddsombudet som skriver under personuppgiftsbiträdesavtal.

Nuläge

Region Östergötland tecknar i dagsläget ett personuppgiftsbiträdesavtal *per ärende/system och/eller vårdenhet* och extern aktör (fysisk eller juridisk person, offentlig myndighet, institution eller annat organ) som utför personuppgiftsbehandling för Region Östergötlands räkning. Inom Sydöstra sjukvårdsregionen (SÖR) sker ett kraftigt ökat samarbete avseende flera vårddiscipliner, bl.a. genetik, Next-Generation DNA Sequencing (NGS), digital patologi, radiologi etc. Då både den IT-nära och den verksamhetsnära utvecklingen inom ovanstående områden går snabbt framåt; t.ex. datainsamling utanför Region Östergötlands IT-infrastruktur, molnlagring och –analys av mätdata, distribuerad analys av prover, app- och webdirektåtkomst till patientdata etc., förväntas antalet personuppgiftsbiträdesavtal att öka lavinartat.

Rekommendation

Juristfunkionerna vid resp. part i SÖR (Landstinget i Kalmar, Region Östergötland, Region Jönköpings Län) ta fram ett tydligt regelverk avseende hantering av personuppgiftsbiträdesavtal (i enlighet med GDPR) inom vårt samarbetsavtal i sydöstra sjukvårdsregionen för att hantera personuppgiftsbiträdesavtal på aggregerad nivå (ett avtal som reglerar personuppgiftsbehandlingen inom flera ärenden7system och/eller vårdenheter). Juridisk kompentens behöver samverka inom SÖR för att hantera frågan.