Mottagare
Till Region Hallands revisorer

Datum
2025-08-13

Diarienummer
RS250570

Yttrande - Revisionsrapport Granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten

Regionens revisorer har behandlat och godkänt revisionsrapport om granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten. Granskningens syfte är att bedöma om regionstyrelsen har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt. Revisorerna har i granskningen biträtts av sakkunniga från PWC.

Utifrån genomförd granskning har revisorerna lämnat följande rekommendationer

Regionstyrelsen rekommenderas att:

- Säkerställa att riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL snarast genomförs,
- Säkerställa att lämplighetsbedömningar dokumenteras på ett sätt som innebär att det är tydligt att bedömningar har skett innan utlämning (det vill säga innan en tjänst tagits i bruk), och att OSL därmed efterlevs,
- Säkerställa att de brister och oklarheter avseende främst tjänsteavtal och dess koppling till PUB-avtal åtgärdas vid liknande anskaffningar framgent,
- Säkerställa att uppföljning av leverantörer och avtal initieras snarast, samt att ett systematiskt arbetssätt avseende uppföljning inom området etableras,
- Säkerställa att ett systematiskt arbetssätt etableras (kan med fördel göras genom användning av utvecklad teknik), som innebär att registerförteckningarna regelbundet uppdateras och kvalitetssäkras,
- Säkerställa att ändamålsenliga rutiner finns även på systemspecifik nivå,
- Säkerställa att väl anpassad information om personuppgiftsbehandling sker på ett lättillgängligt sätt vid digitala vårdmöten.

Revisionsrapporten har tillsänts Regionstyrelsen för yttrande och redogörelse om vilka åtgärder som regionstyrelsen avser att vidta med anledning av resultatet i granskningen. Regionstyrelsen har tagit del av den genomförda granskningen och avger nedanstående yttrande.

Adress: Region Halland, Box 517, 301 80 Halmstad
Besöksadress: Södra vägen 9
Telefon: 035-13 48 00 Fax: 035-13 54 44

E-post: regionen@regionhalland.se
Webb: regionhalland.se
Org. Nr: 232100–0015

Regionstyrelsen yttrande

Regionstyrelsen och regionkontoret arbetar kontinuerligt med att säkerställa efterlevnad till gällande lagstiftning. Omfattningen av dokumentationen är ofta en bedömning i förhållande till resursåtgång där gränsdragning ibland är svår, dock måste alltid nivå för att säkerställa laglig efterlevnad uppnås. Regionkontoret vill dock påtala att ingen av de leverantörer som nämns i granskningen har bedömts olämpliga att behandla de uppgifter som är aktuella. Regionstyrelsen delar revisorernas uppfattning om att det kan vara svårt att följa nuvarande riskanalyser och dokumentation och avser göra förtydligande och förbättringar. Vidare delas inte revisorernas uppfattning om tjänsteavtal och PUB-avtal tydligare kan kopplas samman där licenspartneravtal används som anskaffningsform eftersom licenspartnern inte behandlar några personuppgifter.

- Säkerställa att riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL snarast genomförs,
- Säkerställa att lämplighetsbedömningar dokumenteras på ett sätt som innebär att det är tydligt att bedömningar har skett innan utlämning (det vill säga innan en tjänst tagits i bruk), och att OSL därmed efterlevs,

Regionkontoret har under hösten 2024 arbetat med att förstärka juridisk kompetens för att ytterligare systematisera arbetet för att säkerställa att bl. a GDPR och OSL efterlevs på det sätt som förväntas. Under våren 2025 har det skett förtydligande i befintliga anskaffningsprocesser och kompletteringar i riskanalyser. Revisionsrapporten förtydligar ytterligare vad som behöver säkerställas.

Enligt revisorerna finns det synpunkter på att bestämmelsen i 10 kap 2a§ OSL inte har efterlevts och här vill vi göra ett förtydligande. De granskade systemen har anskaffats vid en tidpunkt som var före 1 juli 2023. I samtliga fall har leverantörens lämplighet granskats av Region Halland och inte funnits olämplig för utlämnande av aktuella uppgifter. 10 kap 2a§ OSL anger att bedömningen ska utgå ifrån huruvida leverantören inte anses olämplig vilket anses vara en mindre omfattande bedömning än om att lagen hade varit formulerad som att en lämplighetsbedömning skulle genomföras. Därför måste också insatsen för riskanalys och dokumentationskrav stå i proportion till detta. Lagen anger inte uttryckligen att dokumentationen ska vara skriftlig. Regionkontoret har i enighet med detta ansett att olämplighetsbedömningar finns och att de utlämnade uppgifter som aktuella leverantörer behandlar INTE är utsatta för risk. Dock ser vi att dokumentationen för riskanalys i vissa delar kan förbättras med utgångspunkt att bevisa att en olämplighetsbedömning har utförts. Regionkontoret har påbörjat en systematisk översyn hur riskanalyser och dokumentationen ska förtydligas och kompletteras.

- Säkerställa att de brister och oklarheter avseende främst tjänsteavtal och dess koppling till PUB-avtal åtgärdas vid liknande anskaffningar framgent,

Att en leverantör som upphandlas kan behandla avsedda uppgifter måste vara ett grundläggande kriterium för en god genomförd anskaffning. Regionkontoret säkerställer att det finns avtal som reglerar affärsförhållande och personuppgiftsbehandling med våra leverantörer. Dock är det inte alltid att ett affärsförhållande innefattar någon behandling av personuppgifter utan en leverantör kan vara ombud av en licens för en tjänst som tredje part tillhandahåller. Regionkontoret bedömt det som komplicerat att involvera en leverantör som endast är ombud, bedömningen har gjorts utifrån att leverantören inte har någon kännedom om de personuppgifter som tredjeparts leverantören behandlar och har därmed inte möjlighet att redogöra för behandlingens art och tillvägagångssätt. Vi har uppmärksammat att bedömning huruvida ett PUB-avtal alltid ska knytas ett affärsavtal kan bedömas olika. I dialog med jurister vid SKR finns bedömningen att PUB-avtal alltid följer behandlingen av personuppgifter och kan således också tecknas direkt med den part som behandlar personuppgifterna utan gällande affärsavtal.

- Säkerställa att uppföljning av leverantörer och avtal initieras snarast, samt att ett systematiskt arbetssätt avseende uppföljning inom området etableras,
- Säkerställa att ett systematiskt arbetssätt etableras (kan med fördel göras genom användning av utvecklad teknik), som innebär att registerförteckningarna regelbundet uppdateras och kvalitetssäkras,
- Säkerställa att ändamålsenliga rutiner finns även på systemspecifik nivå,
- Säkerställa att väl anpassad information om personuppgiftsbehandling sker på ett lättillgängligt sätt vid digitala vårdmöten.

Revisorerna föreslår en systematisk återkommande uppföljning av leverantörerna och regionstyrelsen delar uppfattningen att det ska vara enklare att följa och förstår vikten av detta, men vill samtidigt påtala att detta är ett omfattande arbete då regionen i dagsläget innehar ca 700 olika IT-system. I en återkommande uppföljning måste resursåtgång vägas in i förhållande till riskexponering av regionens uppgifter i det aktuella IT-systemet. Regionkontoret ska undersöka på vilket sätt som en systematiskuppföljning kan genomföras så snart som möjligt.

Regionstyrelsen

Mikaela Waltersson
Regionstyrelsens ordförande

Krister Björkegren
Regiondirektör