REVISIONSSKRIVELSE

Region Uppsala

	Datum	Dnr
Regionens revisorer	2023-04-14	REV2023-00005
	Till	Regionstyrelsen

Revisionsskrivelse gällande granskning av implementationen av Heroma

Regionens revisorer har anlitat Öhrlings PriceWaterhouseCooper (PwC) att som sakkunnigt biträde genomföra en granskning av implementationen av Heroma.

Bakgrund och syfte

Region Uppsala har under början av 2022 implementerat det nya personal- och lönesystemet Heroma. Systemet upphandlades 2018/2019 men implementerades inte förrän 2022 på grund av olika orsaker, bland annat pandemin. Det har varit problem i samband med implementeringen, exempelvis har medarbetare fått fel lön samt fel jour- och komptid. Även semesterdagar har inte stämt. Omständigheterna har även varit föremål för viss mediabevakning. Brister i lönesystemet innebär en stor risk för felaktig lönehantering och potentiell påverkan på de anställdas ersättning och förmåner. Revisorerna i Region Uppsala ser därför i sin risk- och väsentlighetsbedömning att implementationen av Heroma viktig att granska och utvärdera.

Syfte med granskningen är att granska och utvärdera implementationen av Heroma och om den skett med tillräcklig styrning och intern kontroll.

Den övergripande revisionsfrågan är:

- Har implementationen av systemet Heroma hanterats på ett sätt som skapar bra förutsättningar för en trygg och säker lönehantering?

Granskningens resultat

Den samlade bedömningen är att implementeringen av systemet delvis skett med tillräcklig styrning och intern kontroll. Man observerar att i det förberedande arbetet har inte kraven för vissa områden såsom schemaläggning varit tillräckligt genomarbetade. Utbildningsinsatserna har varit omfattande men mer utbildningsinsatser avseende schemaläggning och tolkning av lönespecifikationer borde ha genomförts. Medarbetare hade även svårt att få hjälp med problem som uppstod både inför och efter driftsättningen som främst berodde på hög belastning inom den upprättade supportfunktionen. Man bedömer att projektorganisationen och dess metodik har varit strukturerad samt att migrering av data genomförts på ett ändamålsenligt sätt. Applikationen i Heroma, ”Kom och Gå”, driftsattes utan att en ändamålsenlig lösenordshantering var etablerad.

Detta medförde att medarbetare kunde logga in på andra anställdas konton. En ändamålsenlig lösning för detta lanserades november 2022. Man noterar att anmälan om personuppgiftsincident till Integritetsskyddsmyndigheten (IMY) gjordes flera månader efter incidenten vilket indikerar på brister i rutinen inom regionen. Man bedömer vidare att det finns en ändamålsenlig behörighetsstruktur uppsatt i Heroma samt implementerade kontroller i lönehanteringsprocessen.

Revisorernas rekommendationer
Till Regionstyrelsen:

Gällande Heroma och kringliggande aktiviteter:

- Avsätt resurser för att utbilda organisationen i hur lönespecifikationerna i Heroma ska läsas och tolkas
- Säkerställ att det pågående arbetet med att bygga upp det nya organisationsträdet i Heroma fortsatt prioriteras och färdigställs.
- Etablera rutiner och arbetssätt för att följa upp loggade användaraktiviteter. Det bör exempelvis tydliggöras vad som är avvikande användaraktiviteter och hur avvikelserna ska hanteras.
- Se över om regionens register över personuppgiftsbehandlingar behöver uppdateras i och med genomförandet av detta projekt.

För kommande projekt:

- Säkerställ att supportfunktionen har förstärkt och adekvat bemanning vid driftstart av verksamhetskritiska system.
- Säkerställ att verksamheten avsätter tid för att genomföra utbildning vid lansering av verksamhetskritiska system.
- Säkerställ att det finns ändamålsenliga säkerhetsfunktioner (exempelvis för lösenordshantering) upprättade inför framtida lanseringar av IT-lösningar.
- Säkerställ att verksamheten avsätter ändamålsenliga resurser för att bedriva lokala anpassningsprojekt, bedriva verksamhetsspecifika utbildningar och för att tillsätta superanvändare vid genomförande av implementationer av större system. Det behöver även tydligt kommuniceras och förankras att verksamheten har detta ansvar. Det behöver även säkerställas att de medarbetare i verksamheten som deltar i projekt får möjlighet att avsätta tid för det.
- Se över om regionens medvetenhet och rutiner för att identifiera och hantera personuppgiftsincidenter behöver uppdateras. Detta för att säkerställa att personuppgiftsincidenter identifieras på ett ändamålsenligt sätt och att anmälan till IMY sker i linje med lagkraven.
- Vid tillämpliga fall bör det säkerställas att en konsekvensbedömning ur ett dataskyddsperspektiv genomförs redan innan införandet av IT-lösningar (i linje med artikel 35 i Dataskyddsförordningen) för att på så sätt förebygga risker innan de uppkommer.

Region Uppsala

	Datum	Dnr
Regionens revisorer	2023-04-14	REV2023-00005

- Tillse att det finns en projektekonom tillsatt för styrning och uppföljning av det ekonomiska utfallet i kommande projekt
- Säkerställ extra extern resurstilldelning vid stora projekt då dessa oftast inte kan drivas med enbart befintliga resurser

Regionens revisorer önskar svar från Regionstyrelsen avseende vilka åtgärder som planeras att vidtas med anledning av rapporten och revisorernas rekommendationer senast 2023-08-31.

För Regionens revisorer

Anders Toll
Ordförande