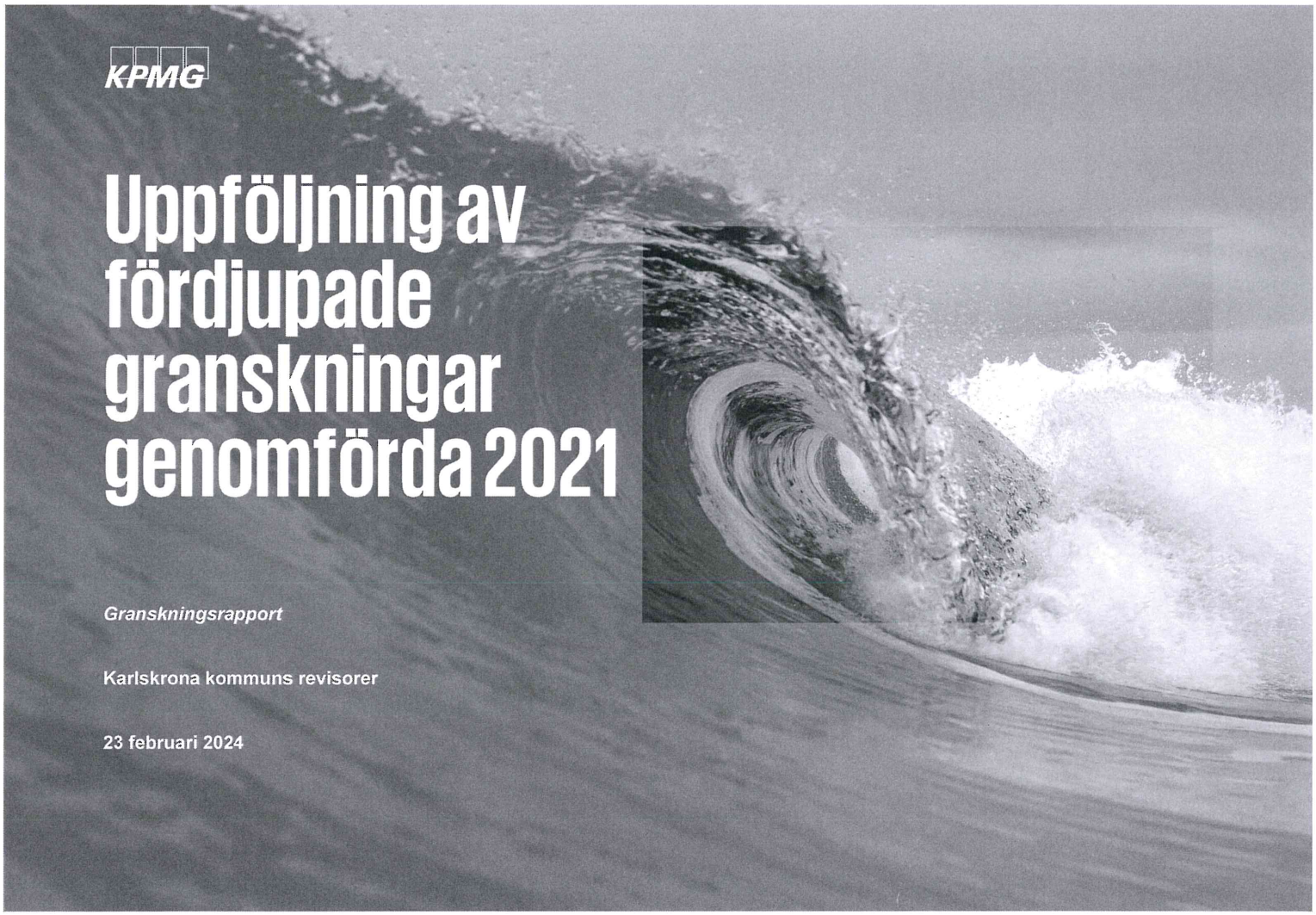

KPMG

Uppföljning av fördjupade granskningar genomförda 2021

Granskningsrapport

Karlskrona kommuns revisorer

23 februari 2024

Innehåll

Bakgrund, syfte och metod

Bakgrund

KPMG har av Karlskrona kommuns revisorer fått i uppdrag att utifrån de fördjupade granskningar som genomfördes under 2021 undersöka vilka åtgärder som berörda nämnder och styrelse har vidtagit med hänsyn till granskningsresultatet för respektive granskning.

Syfte och revisionsfrågor

Syftet med granskningen är att följa upp vilka åtgärder som vidtagits utifrån identifierade förbättringsområden/rekommendationer avseende följande granskningar:

- Granskning om direktupphandling
- Granskning av informationssäkerhet

Avgränsning

Granskningen omfattar genomförda granskningar under 2021.

Metod

De två för uppföljningen aktuella granskningsrapporterna med tillhörande missiv samt nämndernas svar på respektive granskning har granskats. Utifrån detta underlag har ett antal uppföljande frågor upprättats. Ansvariga tjänstemän har tillställts frågor rörande vilka åtgärder som vidtagits med anledning av tidigare granskning.

Granskning av direktupphandling (Kommunstyrelsen)

Tidigare granskningens syfte: *Granskningen syftar till att bedöma om kommunstyrelsens uppsiktplikt av nämndernas efterlevnad av reglerna kring direktupphandling samt att utvalda nämnders interna kontroll avseende direktupphandling är tillräcklig..*

Tidigare rekommendationer	Kommunstyrelsens svar 21-11-30	Iakttagelser från uppföljningen
1. **Kommunstyrelsen** stärker upp den interna kontrollen avseende dokumentationsplikten vid direktupphandling	Arbete med Riktlinjer för Inköp och upphandling pågår av upphandlingsenheten och planeras bli klar under 2021, de tidigare riktlinjerna gäller tills ny antas av kommunstyrelsen. Riktlinjerna kommer att förtydligas ytterligare avseende både dokumentationsplikten och hur rutinerna, som finns dokumenterade i direktupphandlingsvertyg, ska tillämpas. Upphandlingsenheten har även fått i uppdrag av kommundirektören att hantera förvaltningarnas behov av ytterligare stöd inom området. Detta innebär att Karlskrona kommun centraliserar direktupphandlingsprocessen för direktupphandlingar över 100 000 kr exkl. moms, vilket ökar kontrollen och säkerställer dokumentationsplikten. Denna förändring sker under år 2022.	❖ Upphandlingsenheten har tagit fram riktlinjer enligt uppdraget och Kommunstyrelsen beslutade om nya riktlinjer 2022-09-06 § 219. ❖ Av riktlinjerna framgår ett förtydligande av dokumentationsplikten samt en förändring i ansvarsfördelningen som innebär att samtliga direktupphandling överstigande 100 000 kronor hanteras av upphandlingsenheten. ❖ För att möta det centraliserade uppdraget att hantera direktupphandlingar över 100 000 kronor har upphandlingsenheten stärkts med en heltidstjänst från och med våren 2022. ❖ Utöver detta har upphandlingsenheten reviderat certifieringsutbildningen för inköpsansvariga samt uppdaterat befintliga mallar för upphandling.

Granskning av direktupphandling (Drift- och servicenämnden)

Tidigare rekommendationer	Drift- och servicenämndens svar 21-12-14 §172	Iakttagelser från uppföljningen
2. **Drift- och servicenämnden** bör stärka sin interna kontroll	Efter tillstyrkan från arbetsutskottet beslutar drift- och servicenämnden att komplettera nämndens internkontrollplan för 2022 avseende granskning av rutiner för dokumentation.	❖ I internkontrollplanen för 2022 ingick: *Risk att otillåten direktupphandling sker på grund av oklara direktiv/oaktsamhet vilket kan leda till bland annat ekonomisk skada och förtroendeskada.* Förvaltningen valde för 2022 att gå igenom samtliga fakturor där det fanns oklarheter, utifrån sammanställt i lista från upphandlingsenheten. Upphandlingsenheten sammanställning visade: • Antal fakturor totalt utan anmärkning: 27278 st. • Antal fakturor där oklarhet råder: 438 st. ❖ Motsvarande internkontrollpunkt finns i internkontrollplanen för 2023 & 2024 där ett urval av fakturor kontrolleras. ❖ Förvaltningen har även granskat avtalstroheten vilken är hög, drygt 80 % för 2022 och 92% för 2023. Orsaker till att direktupphandlingar behöver genomföras är således extraordinär händelse, specifika engångsinköp till projekt, direktupphandling av utbildningsinsatser eller engångsinköp vid prov av utrustning, tjänster och varor. ❖ Drift- och serviceförvaltningen har också stärkt rutiner vad gäller utbildning. Samtliga medarbetare med inköpsrätt har genomfört utbildningen från upphandlingsenheten och närmsta chef har utpekat ansvar för att utbildning genomförs vid nyanställning. ❖ Mandat för att ta beslut om att upphandling ska genomföras har också förtydligats. Ansvarig inom området där direktupphandlingen ska ske är den som har mandat att ta beslutet. ❖ Stabsavdelningen gör stickprov och uppföljning av handlingar/ärenden i kommunens ärendehanteringssystem. Kontakt tas med handläggare vid brister i diarieföring för varje enskilt ärende.

Granskning av direktupphandling (Drift- och servicenämnden forts.)

Tidigare rekommendationer	Drift- och servicenämndens svar 21-12-14 §172	Iakttagelser från uppföljningen
3. **Drift- och servicenämnden** tillser att det finns dokumenterade nämndspecifika rutiner för direktupphandling.	Efter tillstyrkan från arbetsutskottet beslutar drift- och servicenämnden att ge förvaltningen i uppdrag att ta fram nämndspecifika fastställda dokumenterade rutiner.	❖ Förvaltningen ansåg efter genomlysning av verksamheten att det inte fanns behov av att ta fram nämndspecifika rutiner för direktupphandling ❖ I och med upphandlingsenhetens ökade hantering av och kontroll över upphandlingar ansågs detta inte behöva kompletteras med nämndspecifika rutiner.

Granskning av direktupphandling (Äldrenämnden)

Tidigare rekommendationer	Äldrenämndens svar 22-03-01 §6	Iakttagelser från uppföljningen
2. **Äldrenämnden** bör stärka sin interna kontroll	Kommer genomföras kontroll av att samtlig personal med inköpsrätt genomgått certifieringsutbildning för beställare med inköpsrätt, samt överväga om denna utbildning bör repeteras med visst tidsintervall. Under år 2022 kommer förvaltningen bjuda in upphandlingsenheten till förvaltningens ledningsgrupp för övergripande genomgång av upphandlingslagstiftning, policy och riktlinje samt vikt av avtals-/leverantörstrohet.	❖ I äldreförvaltningens kompetensutvecklingsplan ingår att samtliga medarbetare med chefsbefattning samt medarbetare med beställningsrätt ska genomföra "Certifieringsutbildning av personal med beställningsrätt" som löpande anordnats genom upphandlingsenheten. ❖ I introduktionsutbildningen för nya medarbetare ingår krav på chef att tillse att samtliga nya medarbetare med beställningsrätt genomgår certifieringsutbildningen. Genomgången certifieringsutbildning läggs in i kompetensverktyget Heroma kompetens, vilket möjliggöra för chefer att säkerställa att medarbetare har aktuell utbildning. ❖ Upphandlingsenheten har under år 2022 medverkat vid en av äldreförvaltningens chefsdagar för att ge grundläggande kunskap till samtliga chefer avseende upphandling, inköp, avtalstrohet med mera.. Detta avses genomföras vartannat till vart tredje år.
3. **Äldrenämnden** tillser att det finns dokumenterade nämndspecifika rutiner för direktupphandling.	Under år 2022 kommer förvaltningen ta fram och fastställa nämndspecifik rutin för inköp och direktupphandlingar.	❖ Nämndspecifik rutin för direktupphandling är inte framtagen. ❖ Förvaltningen har inväntat upphandlingsenhetens riktlinje som innebär att förvaltningen inte längre ansvarar för att genomföra och dokumentera direktupphandlingar över 100 000 kronor. Den nya riktlinjen innebär också att direktinköp har införts för ett värde upp till 15 tkr. ❖ Efter övervägande har äldreförvaltningen beslutat att framta en riktlinje för direktupphandlingar under 100 000 kronor och direktinköp. Riktlinjen planeras vara klar under kvartal 2.

Granskning av informationssäkerhet (Kommunstyrelsen)

Tidigare gransknings syfte: *Det övergripande syftet med granskningen är att bedöma om kommunstyrelsen säkerställt en ändamålsenlig styrning, uppföljning och intern kontroll för kommunens arbete med informationssäkerhet.*

Tidigare rekommendationer till kommunstyrelsen	Kommunstyrelsens svar 21-11-30 §280	Iakttagelser från uppföljningen
1. Upprätta regleringar inom nedanstående områden inom bestämmelser för informationssäkerhet: - **Organisation –** Ansvar/ansvarsfördelning såväl centralt som inom de olika förvaltningarna. - **Målsättning –** Mål (KPI:er) inom nyckelområden som underlag vid regelbunden uppföljning/rapportering - **Identifiering/kartläggning/dokumentation –** Av känslig information, såväl digitala som fysiska. Inkluderar dess koppling till arbetsmoment/behandling där dessa används. - **Informationssäkerhetsklassificering –** Metod, klassificeringsnivå mm. - **Riskanalys –** metod, risknivå mm. - **Skyddsåtgärder –** Kommungemensamt underlag för bestämmande av skyddsmetod. Bör ha koppling till klassificeringsnivåer/risknivåer. - **Uppföljning/rapportering –** Oberoende uppföljning/rapportering ger förtroende samt underlag för åtgärder.	De brister som revisorerna överlag pekar på i sin rapport bejakas. Inga specifika svar för respektive brist finns i svaret. Arbetet pågår inom såväl kommunledningsförvaltningen som inom drift- och serviceförvaltningens IT-avdelning med att åtgärda påpekade brister	❖ Policy för informationssäkerhet är beslutad av kommunfullmäktige (2022/44186) samt ett regelverk för informationssäkerhet (2022/45829) är beslutat av kommundirektören. ❖ Bestämmelserna inkluderar beskrivningar av organisation, målsättningar, identifiering, klassificiering, riskanalys, skyddsåtgärder och uppföljning.

Granskning av informationssäkerhet (forts.)

Tidigare rekommendationer	Kommunstyrelsens svar 21-11-30 §280	Iakttagelser från uppföljningen
2. Gemensamma bestämmelser för området åtkomst bör framtas.	.	❖ Gemensamma bestämmelser för området åtkomst framgår av regelverk för informationssäkerhet, kap. 5.15.
3. Spårbarhet för användarkonton i granskade system bör finnas	.	❖ Samtliga händelser loggas i samtliga system utom EDP Future där endast förändringar i systemet loggas. En stor rensning av anonyma användarkonton har också genomförts som också innebär bättre spårbarhet.
4. Regler bör tillämpas som säkerställer inaktivitet på användarkonton efter en viss tid i granskade system		❖ Inaktiva konton har rensats. För ProCapita och LifeCare inaktiveras konto efter 90 dagar inaktivitet och måste återaktiveras av systemadministratör. En automatiserad process inaktiverar användarkonton i AD för anställda 14 dagar efter anställningens slut och raderas efter 365 dagar. Användarkonton ej knutna till anställda avslutas ej per automatik utan kräver manuell hantering. För EDP Future finns ingen inaktivitetstid utan det krävs manuellt avslut av systemförvaltare.
5. Krav på bytesfrekvens av lösenord bör finnas för granskade system (exkluderat servicekonton)	.	❖ Lösenord till Procapita och Lifecare går ut efter 90 dagar och måste då bytas. Administrativa konton 120 dagar, elevkonton 1095 dagar. Dessa regelbestämmelser är idag en del av policy. En utfasning av lösenordshantering på AD är nära förestående där det i stället blir tvåfaktorsinloggning. För EDP Future saknas krav på bytesfrekvens av lösenord.

Granskning av informationssäkerhet (forts.)

Tidigare rekommendationer	Kommunstyrelsens svar 21-11-30 §280	Iakttagelser från uppföljningen
6. Åtkomst till information i system bör kontrolleras i granskade system		❖ För konton knutna till AD finns fem domänadministratörer för förändring och åtkomst av data. För Procapita och Lifecare gör systemadministratörer kontroller av aktivitet på användarkonton och kontrollerar även löpande att användare har rätt behörigheter. I EDP Future saknas det möjlighet att kontrollera vad användare har tittat på, kontroll över åtkomst till information är således begränsad till behörighetsstyrningen och förändringar i systemet.
7. Enhetliga rutiner för åtkomst bör finnas i granskade system	.	❖ Process för skapande av användarkonto till AD finns automatiserade och genereras via personalsystemet. För skapande av övriga konton sker manuell hantering via Abou och formulär. För övriga system är det upp till närmaste chef att anmäla till systemadministratör när förändring av behörigheter behövs för anställd. ❖ Kommunen använder även specifika dataurval, för att användaren enbart ska ha åtkomst till den information som användaren behöver.
8. Automatisk hantering för användarkonton i Heroma bör finnas	.	❖ För anställda finns det en automatisk process där konton inaktiveras efter 14 dagar efter anställningens slut. Konsulters konton hanteras manuellt efter start och slutdatum. Automatisk hantering för samtliga konton saknas således.
9. Rutin för monitorering av användare och behörigheter bör finnas för granskade system	.	❖ Rutin för monitorering finns för AD, Procapita och Lifecare. EDP Future saknar en rutin för monitorering. .

Sammanfattande bedömning

Granskning av direktupphandling

Vår sammanfattande i bedömning är att kommunstyrelsen har vidtagit åtgärder med anledning av rekommendationen i den tidigare granskningen

- Vår bedömning baserar på att att kommunstyrelsen har stärkt upp den interna kontrollen avseende dokumentationsplikten vid direktupphandlingar genom att ta framta riktlinjer för direktupphandling, centralisera direktupphandlingar över 100 000 kronor, förtydliga dokumentationsplikten och genomföra utbildningsinsatser för förvaltningarna.

Vår sammanfattande bedömning är att drift- och servicenämnden i allt väsentligt har vidtagit åtgärder med anledning av rekommendationerna i den tidigare granskningen.

- Vår bedömning baseras på att drift- och servicenämnden har stärkt sin interna kontroll genom att återkommande inkludera direktupphandlingar i internkontrollplanen. Förvaltningen har också stärkt andra rutiner som stärker kontrollen kring direktupphandlingar. Vi kan dock konstatera att nämndspecifika rutiner för direktupphandlingar under 100 000 kronor inte framtagits.

Vår sammanfattande bedömning är att äldrenämnden till viss del har vidtagit åtgärder med anledning av rekommendationerna i den tidigare granskningen.

- Vår bedömning baseras på att förvaltningen har genomfört kunskapshöjande insatser för personalen, men i övrigt har inga åtgärder vidtagits för att stärka den interna kontrollen. Nämndspecifika rutiner för direktupphandling har inte framtagits men vi kan konstatera att det är under framtagande.

Granskning av informationssäkerhet

Vår sammanfattande bedömning är att kommunstyrelsen i allt väsentligt har vidtagit åtgärder med anledning av rekommendationerna i den tidigare granskningen

- Vår bedömning baseras på att gemensamma bestämmelser för informationssäkerhet i form av policy och regelverk finns framtagna. Vi bedömer att detta innebär en tydligare kravställning på systemets funktioner och en större enhetlighet. Vi kan också se att åtgärder i systemen med en del kritiska faktorer så som anonyma användarkonton, inaktiva konton och enhetliga rutiner för åtkomst har genomförts. I vissa delar finns fortsatt ett utvecklingsarbete kvar i enskilda system kopplat till automatisk hantering av användarkonton, bytesfrekvens av lösenord och rutin för monitorerin

Datum som ovan

KPMG AB

Simon Homander
Verksamhetsrevisor

Lars Jönsson
Certifierad kommunal yrkesrevisor

kpmg.com/socialmedia