Timrå kommun
Kommunstyrelsen
Barn- och utbildningsnämnden
Socialnämnden
Kultur- och tekniknämnden
Bygg- och miljönämnden

För kännedom: Kommunfullmäktiges presidium

2018-10-10

Revisionsrapport ”Uppföljning av IT-säkerhet och granskning av införandet av dataskyddsförordningen”

KPMG har på uppdrag av kommunens revisorer genomfört en uppföljning av tidigare granskning av IT-säkerhet samt granskning av införandet av dataskyddsförordningen.

Revisionen önskar att kommunstyrelsen och berörda nämnder lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 21 januari 2019. Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

Svaret skickas till Lena Medin, KPMG (mailadress lena.medin@kpmg.se) för vidarebefordran till revisorerna.

För Timrå kommuns revisorer

Sten Ekström
Ordförande

Kenneth Norberg
Vice ordförande

Uppföljning av IT-säkerhet samt granskning av införande av dataskyddsförordningen

Rapport

Timrå kommun

KPMG AB

2018-10-10

Antal sidor 12

Timrå kommun
Uppföljning av IT-säkerhet samt granskning av införande av dataskyddsförordningen

2018-10-10

Innehållsförteckning

1 Sammanfattning

Vi har av Timrå kommuns revisorer fått i uppdrag att uppdrag att följa upp att åtgärder har vidtagits avseende iakttagelserna i revisionsrapporten ”Hantering av IT-säkerhet[1]”. Vidare har vi fått uppdrag att översiktligt granska om kommunen har vidtagit tillräckliga åtgärder för att klara kraven i dataskyddsförordningen (GDPR). Uppdraget ingår i revisionsplanen för år 2018.

Granskningen syftar till att konstatera om tillräckliga åtgärder har vidtagits med anledning av iakttagelserna från granskning av IT-säkerhet samt för att klara kraven i dataskyddsförordningen.

Vår sammanfattande bedömning utifrån granskningens syfte är att tillräckliga åtgärder inte har vidtagits med anledning av iakttagelserna från den tidigare granskningen av IT-säkerhet samt för att klara kraven i dataskyddsförordningen.

Mot bakgrund av vår granskning rekommenderar vi att:

— Kommunstyrelsen och berörda nämnder generellt säkerställer att beslutade åtgärder vidtas.

— Kommunstyrelsen och berörda nämnder fattar beslut om åtgärder med anledning av resultatet i GAP- och riskanalyser (se avsnitt 3.2).

— Kommunstyrelsen följer upp att styrdokumenten, bl.a. vägledande råden, efterlevs (se avsnitt 3.3). I vår rapport har vi särskilt tagit upp följande punkter, men rekommendationen gäller styrdokumenten som innehåller en mängd krav generellt:
  - Behovet av två systemförvaltare (se avsnitt 3.4).
  - Att riktlinjer för behörighetstilldelning upprättas och att blankett/ e-tjänst ger mer stöd för tilldelning vad gäller nivåer (se avsnitt 3.5).
  - Att regelbundna interna kontroller genomförs och att resultatet rapporteras till centrala IT (se avsnitt 3.6).

— Kommunstyrelsen tillser att styrdokumenten omprövas regelbundet, gärna årligen (se avsnitt 3.3).

— Kommunstyrelsen och övriga nämnder säkerställer att Dataskyddsförordningen efterlevs. Vi rekommenderar att samtliga nämnder inhämtar en statusrapport med tillhörande plan för åtgärder samt följer upp denna (se avsnitt 4).

[1] Rapporten daterad februari 2016

2 Inledning/bakgrund

Vi har av Timrå kommuns revisorer fått i uppdrag att följa upp att åtgärder har vidtagits avseende iakttagelserna i revisionsrapporten ”Hantering av IT-säkerhet”. Vidare har vi fått uppdrag att översiktligt granska om kommunen har vidtagit tillräckliga åtgärder för att klara kraven i dataskyddsförordningen. Uppdraget ingår i revisionsplanen för år 2018.

Av 2016 års revisionsrapport gällande IT-säkerhet framgår att den interna kontrollen avseende kommunens IT-säkerhet inte är tillräcklig och bör förbättras. Av svaret från kommunstyrelsen framgår att ett flertal åtgärder kommer att vidtas.

EU har i april 2016 beslutat om ett nytt regelverk för behandling av personuppgifter som ska börja tillämpas i medlemsstaterna i maj 2018. Den nya dataskydds-förordningen kommer att gälla som lag i samtliga medlemsstaterna och ersätter då tidigare nationell lagstiftning. Vid tidpunkten för vår granskning har den nya lagstiftningen trätt i kraft och arbetet med att anpassning till den nya lagstiftningen bör vara klart.

Revisorerna bedömer att det finns en risk att beslutade åtgärder inte genomförts fullt ut i enlighet med svar på revisionsrapporten. Det finns också en risk att vidtagna åtgärder inte har fått avsedd effekt. Revisionen anser att det är väsentligt att fattade beslut genomförs samt att det finns rutiner för att säkra att så sker.

Vad gäller dataskyddsförordningen bedömer revisionen att det finns en risk för att tillräckliga förberedelser inte har genomförts för att lagstiftningen ska kunna följas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om tillräckliga åtgärder har vidtagits med anledning av iakttagelserna från granskning av IT-säkerhet samt för att klara kraven i dataskyddsförordningen.

Granskningen har besvarat följande revisionsfrågor:

— om åtgärder har vidtagits i enlighet med svaren på granskning av IT-säkerhet samt om styrelsen har följt upp att vidtagna åtgärder efterlevs och fått avsedd effekt.

— om tillräckliga åtgärder har vidtagits för att säkerställa efterlevnad av dataskyddsförordningen.

Granskningen gällande IT-säkerhet omfattar endast uppföljning av tidigare granskning. Vad gäller dataskyddsförordningen är granskningen översiktlig.

Granskningen avser främst kommunstyrelsen men samtliga nämnder omfattas av regelverket.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Kommunallagen 6 kap. 6 §

— Tillämpbara interna regelverk, policys och beslut

2.3 Metod

Granskningen har genomförts genom:

— Dokumentstudier

- Vägledande råd och bestämmelser (främst Förvaltning & Drift av IT inom Timrå kommun)
- GAP-analys Timrå kommun informationssäkerhet
- Timrå kommun riskutvärdering IT-system
- Blanketter för bl.a. behörighetstilldelning
- Handlingsplan GDPR – ett stöd i det fortsatta arbetet.

— Intervjuer med berörda tjänstemän

Rapporten är faktakontrollerad av IT-samordnare och IT-chef.

3 Uppföljning av tidigare granskning

3.1 Rekommendationer och kommunstyrelsens svar

Följande rekommendationer lämnades med anledning av tidigare granskning. Under respektive punkt finns kommunstyrelsens svar:

— *Färdigställ riskanalyser av prioriterade system och förtydliga vid vilka tillfällen riskanalyser ska göras.*

  Som bekant pågår riskanalyser (GAP), som kommer att vara färdigställda under kvartal 3 2016. Det påpekas att systemförvaltarna behöver stöd i detta arbete, vilket de har. En konsult på driften samt en samordnare på Centrala IT har stått till förfogande sedan starten för snart ett år sedan.

— *Se till att de vägledande råden är aktuella.*

  Efter riskanalysernas färdigställande ska aktualisering av styrdokumenten ske. Det planeras till kvartal 3 – 4 2016. I nya versioner kommer att framgå var, när och hur riskanalyser ska göras. Enligt tidigare gjord revision så är det denna ordning som ska gälla.

— *Utred om ansvarsfördelningen är ändamålsenlig, exempelvis genom att se till att minst två personer har kännedom om system och rutiner vid varje förvaltning.*

  Som framgår är ansvaret systemägarens (enskild förvaltning) för att det till exempel ska finnas dubbla funktioner för systemförvaltning. Det ska påpekas att behovet av sådana dubbla funktioner poängteras i befintliga styrdokument. Centrala IT har i dagsläget inget mandat för att kräva att förvaltningarna t.ex. ska ha dubbla systemförvaltare för respektive system. Detta är en verksamhetsfråga.

— *Säkerställ att det finns skriftliga rutiner för exempelvis behörighetshantering och att de rutinerna är ändamålsenliga.*

  Skriftliga rutiner för behörighetshantering gällande kommunens nät, finns och bedöms vara ändamålsenliga. Dock krävs det även behörighetsbeställningar från respektive systemförvaltare i respektive system. Där har Centrala IT inga mandat att bestämma hur eller när ett lösenord ska ges. Det är en verksamhetsfråga och även i många fall en leverantörsfråga. I många system kan vi inte välja vilka regler vi vill ha utan de finns redan inbyggda i systemet.

— *Se till att det genomförs regelbundna kontroller med avseende på IT-säkerhet och att de kontrollerna baseras på en riskbedömning. Kommunstyrelsen som är övergripande ansvarig för IT säkerheten bör regelbundet inhämta information om vilket arbete som bedrivs vid förvaltningarna.*

  Centrala IT kommer att utreda och överväga om det är ändamålsenligt att föreslå att det ska göras en årlig rapportering av de kontroller av IT-säkerhet som genomförts vid förvaltningarna. Dock har Centrala IT inga mandat att kräva att förvaltningarna ska göra detta.

  Det framgår också av svaret att centrala IT inte har någon egen makt över internkontrollen. Centrala IT avser att lägga önskemål om att alltid ha med några punkter. Det poängteras att det utförs ständig övervakning och kontroller i våra system.

— *Utred om det finns något sätt att automatiskt få en överblick över de anställdas samtliga behörigheter. I dagsläget hålls en manuell förteckning av systemförvaltarna.*

  Vad till sist gäller att med automatik få överblick över anställdas samtliga behörigheter pågår det arbetet. Det har pågått en under en längre tid, vilket vi tidigare informerat om. Arbetet innebär att när en medarbetare inte längre får lön så stängs man automatiskt av från inloggning i kommunens nät. I och med att den inloggningen tas bort, så kommer man inte längre in i andra system heller. Det krävs fortfarande att respektive systemförvaltare löpande håller ordning på sina egna inloggningar till sitt eget system.

3.2 Riskanalyser

Av ”Vägledande råd och bestämmelser – Förvaltning & Drift av IT inom Timrå kommun” framgår att krav på och åtgärder för ett enskilt IT-system ska dokumenteras i en verksamhets/riskanalys. Kravet gäller för kommunens tio prioriterade system, d.v.s. sådana som är viktiga för verksamheten. Analysen ska kontrolleras varje år och uppdateras vart tredje år.

En GAP-analys genomfördes hösten 2016[2] av en extern konsult.

En intern riskanalys har därefter genomförts två gånger. Vi har tagit del av rapport daterad 2017-10-10.

Analyser visar på ett antal brister. Kommunstyrelsen som enligt uppgift har behandlat rapporterna, har däremot inte fattat några beslut om åtgärder för att komma till rätta med bristerna.

Enligt kommunledningsförvaltningen har dock vissa åtgärder vidtagits. Socialförvaltningen uppger att åtgärder är vidtagna. Barn- och utbildningsförvaltningen uppger att en tjänst har inrättas och att ett arbete kommer att påbörjas under hösten 2018. Kultur- och teknikförvaltningen och miljö- och byggnadsnämnden anser att iakttagelserna inte berör förvaltningarnas respektive system.

[2] GAP analys Informationssäkerhet 2016-11-23 ver 0.9

Kommentar

Vi anser att det är väsentligt att de brister som konstateras i analyserna åtgärdas. Vi anser att kommunstyrelsen som övergripande IT-ansvarig har ansvaret för att åtgärder vidtas samt genom sin uppsiktsplikt följa upp nämndernas åtgärder.

Vi noterar att kravet på riskanalys gäller kommunens tio prioriterade system. Vi anser att det rimligtvis finns fler system inom kommunen som är verksamhetskritiska, även om inte lika många anställda berörs. Vi anser att det behöver övervägas om riskanalyser behöver genomföras för dessa i någon form.

3.3 Vägledande råd

De vägledande råden, för närvarande sex dokument exklusive tillägg, har uppdateras och fastställts av kommunstyrelsen, senast år 2016. Ytterligare ett antal förändringar har skett därefter. Enligt uppgift ryms dessa inom tidigare mandat om att göra smärre justeringar.

Enligt uppgift kommer råden att uppdateras under hösten 2018 med anledning av dataskyddsförordningen och i samband med det kommer även kommunstyrelsen att fastställa råden.

Kommentar

Vi ser positivt på att vägledande råden har uppdaterats. Vi anser att styrdokument, såsom vägledande råd, regelbundet, gärna årligen, omprövas.

Vi noterar att råden innehåller en mängd riktlinjer, för att säkerställa att dessa efterlevs behöver kommunstyrelsen följa upp efterlevnaden. Av svaret på föregående rapport framgår att Centrala IT inte anser att det finns något sådant mandat och enligt våra intervjuer hänvisas också till bristande resurser. Det är en fråga som kommunstyrelsen måste lösa.

3.4 Systemförvaltare

Av kommunstyrelsen fastställda ”Vägledande råd och bestämmelser – Förvaltning & Drift av IT inom Timrå kommun” framgår att det för mellan och stora system ska finnas två systemförvaltare.

Såsom framgår av svaret anses det vara en verksamhetsfråga. Vi har i vår granskning noterat att det verkar finnas i varje fall för några system, däribland vid socialförvaltningen, som numera har två systemförvaltare.

Kommentar

Vi anser att kommunstyrelsen och övriga nämnder systematiskt behöver gå igenom behovet av två systemförvaltare för de system som berörs.

3.5 Behörigheter

Av ”Vägledande råd och bestämmelser – Förvaltning & Drift av IT inom Timrå kommun” framgår att

- endast behörig användare anställd i kommunen, ges åtkomst till kommunens IT-system. Undantagsfall kan behörighet ges tillfälligt till leverantörer
- användares behörighet ska styras utifrån dennas arbetsuppgifter och efter beslut av chefen
- varje användare ska ha en personlig identitet bestående av login-id och lösenord. Lösenord ska bytas vid uppmaning efter 180 dagar.
- den som är tjänstledig eller av annan orsak har längre frånvaro skall ha sin identitet spärrad
- uppföljning och revidering av tilldelade behörigheter ska ske regelbundet av respektive systemförvaltare.

En blankett för att begära behörighet finns framtagen. Blanketten som ska sparas i respektive personalakt skrivs under av ansvarig chef och behörighetsbeställaren. Enligt personalavdelningen sker ingen formell kontroll att blanketten kommer till dem för arkivering. En e-tjänst är under utveckling då blanketten innebär ett betydande administrativt arbete.

Behörigheten till centrala IT-systemet avslutas enligt uppgift senast tre månader efter sista lönen. Det ska enligt ansvariga därefter vara omöjligt att få tillgång även till övriga system. Ändring av behörigheter på systemnivå, t.ex. med anledning av ändringar av tjänst, arbetsplats, sker per system.

Kommentar

Vi bedömer att kommunstyrelsen i det vägledande rådet angett grundläggande krav för tilldelning av behörigheter. Av vägledande rådet framgår att regler för behörighetstilldelning ska vara fastlagda och kända. Varken kommunstyrelsen eller nämnderna har upprättat några egna riktlinjer för tilldelning av behörigheter. Vi anser att sådana är väsentliga vid behörighetstilldelning samt för att möjliggöra uppföljning av att rätt behörighet har tilldelats. Kommunstyrelsen bör även i kommungemensamma riktlinjer utifrån en övergripande riskbedömning reglera vilka kombinationer av behörigheter mellan olika system som är olämpliga.

Av den blankett som används för tilldelning av behörighet saknas för flera system möjlighet att ge olika nivåer på behörighet. Det gäller bl.a. lönesystemet och ekonomisystemet där rimligen inte alla användare ska ha samma behörighet.

Det är bra att behörigheten till inloggningen till centrala IT-systemet stängs ner med automatik när tjänstepersonen inte längre erhåller lön. Vi vill däremot lyfta risken om behörigheten inte blir förändras vid till exempel vid byte av tjänst.

3.6 Regelbundna kontroller

Enligt ”Vägledande råd och bestämmelser – Förvaltning & Drift av IT inom Timrå kommun” ska systemägaren årligen rapportera till Centrala IT om interna kontroller som genomförts vid förvaltningen och vilka som planeras till nästa år.

Några sådana rapporter har inte lämnats till Centrala IT.

Vi kan i några av planerna för uppföljning av intern kontroll se att vissa IT-relaterade risker har bedömts och ska ingå i uppföljning. Av den sammanfattande rapporten som lämnats till styrelsen eller nämnden är det dock svårt att bedöma vilken kontroll som följts upp.

Kommentar

Timrå kommun är beroende av fungerande IT-baserade verksamhetsstöd. Vi konstaterar att trots det ingår inte risken i någon högre grad ingår i styrelsens och nämndernas riskbedömningar. Antalet uppföljda kontroller är begränsade. Resultatet har inte lämnats till Centrala IT.

4 Dataskyddsförordningen

Vi har genom intervjuer konstaterat att det har genomförts ett arbete för att införa dataskyddsförordningen.

Det har centralt funnits en plan för införandet av GDPR. Vi har inte tagit del av planen i dess ursprungliga form utan enbart som ”Handlingsplan för dataskydd – ett stöd för det fortsatta arbetet” (fortsättningsvis benämnd handlingsplan).

Av handlingsplanen som lämnades till kommunchefen för kännedom i slutet av juli framgår att ansvaret är utdelat till olika tjänstepersoner. Av planen framgår att information/utbildning har genomförts, det finns vissa rutiner framtagna och att dataskyddsombud finns på plats. Av några punkter framgår att arbetet inte är avslutat. Av våra intervjuer framgår också att det fortfarande kvarstår ett arbete för anpassning till lagstiftningen, främst för kommunstyrelsen, barn- och utbildningsnämnden och socialnämnden. Bland det som återstår kan nämnas att säkerställa att förteckningen över personuppgiftsbehandlingar är komplett och att säkerställa att avtal finns med externa leverantörer.

Såsom vi uppfattat har kommunstyrelsen och nämnderna fått information om lagstiftningen men däremot inte något om införandeprocessen, d.v.s. att allt är klart eller om något återstår.

5 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att tillräckliga åtgärder inte har vidtagits med anledning av iakttagelserna från den tidigare granskningen av IT-säkerhet samt för att klara kraven i dataskyddsförordningen.

5.1 Svar på revisionsfrågorna

— Har åtgärder vidtagits i enlighet med svaret på granskning av IT-säkerhet samt om styrelsens har följt upp att vidtagna åtgärder efterlevs och fått avsedd effekt?

Vad gäller regelverk har kommunstyrelsen, som är övergripande ansvarig för kommunens IT-verksamhet, antagit och reviderat ett antal vägledande råd och bestämmelser i enlighet med tidigare rapport. Av dessa framgår ett antal bestämmelser, varav några framgår av vår rapport, som såväl kommunstyrelsen som övriga nämnder har att följa. Vi konstaterar i vår granskning att bestämmelserna inte alltid efterlevs. Vår bedömning är att kommunstyrelsen inte har följt upp och säkrat efterlevnaden av bestämmelserna i tillräcklig omfattning.

— Har tillräckliga åtgärder vidtagits för att säkerställa efterlevande av dataskyddsförordningen?

Dataskyddsförordningen började gälla som lag den 25 maj 2018. Vår granskning visar att det kvarstår åtgärder för att säkerställa efterlevnad. Vi anser vidare att kommunstyrelsen och ansvariga nämnder inte har informerat sig tillräckligt om statusen för införandet.

5.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi att:

— Kommunstyrelsen och berörda nämnder generellt säkerställer att beslutade åtgärder vidtas.

— Kommunstyrelsen och berörda nämnder fattar beslut om åtgärder med anledning av resultatet i GAP- och riskanalyser (se avsnitt 3.2).

— Kommunstyrelsen följer upp att styrdokumenten, bl.a. vägledande råden, efterlevs (se avsnitt 3.3). I vår rapport har vi särskilt tagit upp följande punkter, men rekommendationen gäller styrdokumenten som innehåller en mängd krav generellt:
  - Behovet av två systemförvaltare (se avsnitt 3.4).
  - Att riktlinjer för behörighetstilldelning upprättas och att blankett/ e-tjänst ger mer stöd för tilldelning vad gäller nivåer (se avsnitt 3.5).
  - Att regelbundna interna kontroller genomförs och att resultatet rapporteras till centrala IT (se avsnitt 3.6).

— Kommunstyrelsen tillser att styrdokumenten omprövas regelbundet, gärna årligen (se avsnitt 3.3).

— Kommunstyrelsen och övriga nämnder säkerställer att Dataskyddsförordningen efterlevs. Vi rekommenderar att kommunstyrelsen och samtliga nämnder inhämtar en statusrapport med tillhörande plan för åtgärder samt följer upp denna, (se avsnitt 4).

Timrå kommun
Uppföljning av IT-säkerhet samt granskning av införande av dataskyddsförordningen

2018-10-10

Datum som ovan

KPMG AB

Lena Medin
Certifierad kommunal revisor