Timrå kommun:
Kommunstyrelsen
Barn- och utbildningsnämnden,
Socialnämnden,
Kultur- och tekniknämnden
Miljö- och byggnadsnämnden

För kännedom: Kommunfullmäktiges presidium

2020-06-16

Revisionsrapport ”Uppföljande granskning av IT-säkerhet samt införande av dataskyddsförordningen”

KPMG har på uppdrag av kommunens revisorer genomfört en granskning för att följa upp att åtgärder har vidtagits avseende iakttagelserna i revisionsrapporten ”uppföljning IT-säkerhet samt införande av dataskyddsförordningen”.

Revisionen önskar att styrelse och nämnder lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 30 oktober 2020. 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

DocuSigned by:
Sten Ekström
4F579758BB57480...
Sten Ekström
Ordförande

DocuSigned by:
1DF7A98627BA486...
Kenneth Norberg
Vice ordförande

Uppföljande granskning av IT-säkerhet samt införande av dataskyddsförordningen

Revisions rapport

Timrå kommun

KPMG AB

2020-06-16

Antal sidor 16

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

2020-06-16

Innehållsförteckning

1 Sammanfattning

Vi har av Timrå kommuns revisorer fått i uppdrag att följa upp att åtgärder har vidtagits avseende iakttagelserna i revisionsrapporten "Uppföljning IT-säkerhet samt införande av dataskyddsförordningen[1]". Uppdraget ingår i revisionsplanen för år 2020.

Granskningen syftar till att konstatera om tillräckliga åtgärder har vidtagits med anledning av iakttagelserna från den uppföljande granskningen av IT-säkerhet samt införande av dataskyddförordningen.

Vår sammanfattande bedömning utifrån granskningens syfte är att ett flertal åtgärder är vidtagna enligt lämnade rekommendationer men att det finns utrymme för ytterligare förbättringar. Några av dessa bland annat gällande behörigheter anser vi är ytterst väsentliga att dessa beaktas. Vi vill betona vikten av att kommunstyrelsen och nämnderna säkerställer att fattade beslut verkställs och att effekten av besluten följs upp.

Utifrån vår bedömning och slutsats rekommenderar vi att:

— kommunstyrelsen säkerställer att beslutade åtgärder genomförs, se avsnitt 3.1

— socialnämnden samt barn- och utbildningsnämnden regelbundet följer upp och säkerställer att förvaltningsplanerna innehåller aktuell och väsentlig information, se avsnitt 3.1.

— barn-och utbildningsnämnden samt socialnämnden att utifrån beslutade behörighetsrutiner regelbundet följer upp och säkerställer att rätt behörigheter har tilldelats och förhindrar obehörig åtkomst, se avsnitt 3.1 och 3.2.

— kultur- och tekniknämnden säkerställer att arbetet med förvaltningsplanen slutförs, se avsnitt 3.1.

— kommunstyrelsen regelbundet följer upp och säkerställer efterlevnaden av de vägledande råden och bestämmelser, däribland kravet på två systemförvaltare i berörda system, se avsnitt 3.2.

— styrelse och nämnder, fram till dess att den nya e-tjänsten är i bruk, regelbundet följer upp och säkrar rutiner i syfte att förebygga så att obehöriga inte får tillgång till kommunens system, se avsnitt 3.1 och 3.2.

— socialnämnden, barn och utbildningsnämnden samt kultur- och tekniknämnden vidtar åtgärder och säkerställer att hanteringen av avtal sker ändamålsenligt.

[1] 2018-10-10

2 Inledning/bakgrund

Vi har av Timrå kommuns revisorer fått i uppdrag att följa upp att åtgärder har vidtagits avseende iakttagelserna i revisionsrapporten "Uppföljning IT-säkerhet samt införande av dataskyddsförordningen[2]". Uppdraget ingår i revisionsplanen för år 2020.

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.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om tillräckliga åtgärder har vidtagits med anledning av iakttagelserna från den uppföljande granskningen av IT-säkerhet samt införande av dataskyddförordningen.

Granskningen ska besvara följande revisionsfrågor:

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

Granskningen avser kommunstyrelsen och samtliga nämnder.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Kommunallagen 6 kap § 6

— Gällande lagar och rekommendationer avseende

— Tillämpbara interna regelverk och policys

2.3 Metod

Granskningen har genomförts genom dokumentstudier och kompletterande avstämningar med berörda tjänstepersoner.

Rapporten är faktakontrollerad av förvaltningschef för: socialförvaltningen, barn- och utbildningsförvaltningen, miljö- och byggnadskontoret samt kultur- och teknikförvaltningen. Rapporten har även faktakontrollerats av kommunchef, IT-samordnare och dataskyddsombud.

[2] 2018-10-10

3 Resultat av granskningen

Granskningen bygger på de rekommendationer som lämnades vid vår tidigare genomförda uppföljande granskning samt de svar på revisionsrapporten som kommunstyrelsen och nämnderna lämnade i samband med denna.

Vår sammanfattade bedömning av vår tidigare genomförda uppföljande granskning var att det inte vidtagits tillräckliga åtgärder med anledning av iakttagelserna samt för att klara kraven i dataskyddsförordningen.

Mot bakgrund av granskningen lämnades som en övergripande rekommendationen till kommunstyrelsen och berörda nämnder att säkerställa att beslutade åtgärder vidtas.

3.1 GAP- och riskanalyser

Den andra rekommendationen riktade sig till kommunstyrelsen och berörda nämnder och handlade om att fatta beslut om åtgärder med anledning av resultatet i de GAP-och riskanalyser som genomfördes under perioden 2016 - 2017.

3.1.1 Kommunstyrelsens åtgärder med anledning av GAP- och riskanalys

Kommunstyrelsen meddelade i sitt svar att den GAP-analys som genomfördes hösten 2016 och den riskutvärderingen som genomfördes år 2017 visar på brister i olika system. I tabellen nedan framgår de identifierade bristerna från GAP-analysen med styrelsens svar samt en nulägesbeskrivning över det aktuella läget.

Identifierade brister i GAP-analys och styrelsens svar	Aktuellt läge
• **Avsaknad av handlingsplaner för analys och hantering av risker för verksamhetssystemen** *Svar:* Planerna saknas fortfarande. Centrala IT har fyra gånger per år förvaltningsmöten där kommande arbeten tas upp för respektive verksamhetssystem. I de uppdaterade riktlinjerna står även att en systemplan årligen ska göras.	Handlingsplan antogs december år 2018 och är enligt uppgift under revidering som beräknas fastställas hösten år 2020.
• **LIS-system** *Svar:* LIS-system har införts. Systemet har däremot inte varit så enkelt som utlovats. Två analyser gjorda år 2017 och 2018. Mall för enklare riskanalys har tagits fram och kommer att spridas/informeras om till systemförvaltarna.	Enligt uppgift har systemet sagts upp i och med byte av driftleverantör. Framtagna mallar tillämpas för riskanalyser och systemförvaltningsplanen. I och med byte av leverantör görs även en genomgång av samtliga system tillsammans med systemförvaltarna.

Identifierade brister i GAP-analys och styrelsens svar	Aktuellt läge
• **Uppdragsbeskrivning av Centrala IT** *Svar:* Omorganisation med ny chef som rekryterats tillträder 1 januari 2019.	Ny chef tillträdde januari 2019 samt att en ny organisation har trätt i kraft. Den nya organisationen bygger på en sammanslagning av två medarbetare från skolenhetens IT och Centrala IT. Enligt uppgift finns planer på att två ytterligare medarbetare ska arbeta med verksamhetsutveckling.
• **Avsaknad av strategi, t.ex. processdokumentation** *Svar:* En IT-arkitekt genomför en dokumentation av kommande nätverk under år 2018. Utöver detta arbete måste varje systemägare ta sitt ansvar och dokumentera hur just deras system är uppsatt och med vilka kopplingar.	Processer har tidigare genomförts av den tidigare IT-leverantörens IT-arkitekt. Enligt uppgift blev resultatet inte enligt förväntan och förhoppningar finns på bättre dokumentation av den nya driftleverantören.
• **Utbildning i informationssäkerhet** *Svar:* Både informationssäkerhet samt GDPR/dataskyddsförordningen har pågått i flera omgångar, under 2017–18 till alla medarbetare.	Nanoutbildningar har löpande skickats ut till samtliga medarbetare med en kommunmail. Detta både i Informationssäkerhet och Dataskydd.
• **IT-infrastruktur - kraftförsörjning** *Svar:* Ansvaret internt på kultur- och teknikförvaltningen. Centrala IT har säkerställt viss säkerhet i kommunhuset under år 2017–18 genom ny UPS. *Kommunikationsnivåer till prioriterade arbetsplatser* - Ingen brist i dagsläget. Inga synpunkter har heller kommit från verksamheten att det ska vara någon brist någonstans.	Enligt uppgift anses tillräckliga åtgärder vidtagits. De åtgärder som bl.a. vidtagits är regelbundna kontroller av dieselaggregat
• **Kommunens telefonväxel** *Svar:* Tillgänglighet och test regelbundet. Huvudansvaret ligger på leverantören Sundsvalls kommun. Gemensamma möten fyra gånger per år. • **www.Timra.se: tillgänglighet prioritet ett vid kris.** *Svar:* Omfattande arbete genomförts för att säkra upp tillgängligheten under 2017–18. Servrar har flyttats och uppgraderats. Samt att under 2018 driftsätts en helt ny webbportal.	• Kommunens telefonväxel: Upphandling av Sundsvalls kommun för tjänsten pågår • www.timra.se – Ny webb driftsatt december 2019 på nya servrar. Inget stopp på den sedan uppgraderingen.

Identifierade brister i GAP-analys och styrelsens svar	Aktuellt läge
• **Mailsystem** Flera mailsystem används inom kommunen vilket också bör tydliggöras. De höga SLA nivåer som finns på Outlook omfattas inte Firstclass inom skolan av. Förslaget i rapporten var att enas om ett system med lika hög tillgänglighet. *Svar:* Under 2018 har projekt inletts för att försöka lösa den frågan. Dessutom genomförs en sammanslagning av de två olika IT-enheterna under 2019. Det föreslogs en utbildning för medarbetarna om hur man hanterar mail och klickar på länkar. *Svar:* Det har gjorts 2017 i en omgång, och görs löpande just nu i en annan omgång, november 2018. Det föreslogs en handlingsplan när kommunen skulle byta mailsystem och uppgradera. *Svar:* När det gäller systemet för adminnätet har detta redan gjorts under 2017–18 till nyaste versionen, och arbetet fortsätter som sagt under 2019 med att försöka lösa ett gemensamt system för alla medarbetare.	Enligt uppgift har Timrå kommun sedan maj 2019 tillämpat samma mailsystem, den nyaste versionen av Exchange. Vad gäller krypterad mail ingår Timrå kommun i utvecklingsprojekt med SKR och Inera. Det beräknas vara helt i drift hösten 2020. Enligt uppgift har även genom nanoutbildningar för informationssäkerhet tagit del av utbildning vad gäller mail. I de vägledande råd och bestämmelser finns även information vad gäller gallring i e-post.
• **Teis** Saknas en bedömning om vad som ska övervakas. Och vilka kriterier och larm som ska kräva åtgärd. *Svar:* Här krävs det insatser från alla håll. Först från systemägare som är de som ska sätta nivåerna för just sitt system. Sedan måste Centrala IT dokumentera detta på ett pedagogiskt sätt. Det har under flera års tid gått larm via mail, till två ansvariga på Centrala IT och till vissa systemförvaltare. Detta måste tydliggöras under 2019 till systemförvaltarna vad dessa mail innebär.	Enligt uppgift går ett SMS larm ut till en utvald grupp vid samtliga störningar.

Identifierade brister i GAP-analys och styrelsens svar	Aktuellt läge
• **LEX** Inför framtiden med integration mot e-tjänster bör en godkänd process för varje integration göras, så att hänsyn tas till alla säkerhetsrisker. *Svar:* Detta görs i varje projekt för varje enskild e-tjänst. Detta har löpande pågått under 2018 och fortsätter under 2019.	Integration med e-tjänsteportalen är i drift i liten skala
• **eCompanion/Besched** Här planeras upphandling och införande av nytt system. Detta system agerar master för all personal och alla behörigheter i nätet. Eftersom detta system har särskilt höga krav just vid utbetalningstillfällena föreslås att kommunen har goda rutiner för ett eventuellt bortfall de dagarna i månaden. *Svar:* Det finns reservrutin med banken och har funnit sedan start 2004. Detta måste också säkerställas inför ett nytt system att rutinerna funkar.	Enligt uppgift kommer ett nytt system införas hösten år 2020 vilket kommer innehålla båda dessa två tidigare system. Reservrutin med banken vid utbetalningar har funnits implementerat sedan år 2007.
• **Aditro (Visma) ekonomisystem** *Svar:* Här pågår införandet av helt nytt system. Planeras vara färdigt kring årsskiftet 2018–19.	Ekonomisystemet heter numera UBW och implementerades helt under år 2019.

3.1.2 Övriga nämnders åtgärder med anledning av GAP- och riskanalys

Socialnämnden och barn- och utbildningsnämnden har i sitt svar angett att förvaltningarna har fått i uppdrag att utarbeta en förvaltningsplan gällande system och budget som beräknas färdigställas under år 2019. Av svaren framgår också att respektive förvaltning fått i uppdrag att utarbeta riktlinjer för olika behörigheter i systemet ProCapita vilket ska färdigställas under år 2019.

Enligt uppgift antog socialnämnden förvaltningsplan för system och budget den 19 maj 2020[3]. Syftet att ge möjlighet till planering och utveckling av IT-stödet utifrån ekonomi, säkerhet, verksamhetsnytta och arbetsmiljö. Av förvaltningsplanen framgår bl.a. information vad gäller definition av system, organisation samt ansvar och säkerhet.

Barn- och utbildningsnämnden antog förvaltningsplanen för system och budget den 22 april 2020[4]. Av förvaltningsplanen framgår att den ska fungera som stöd till administratörer vad gäller arbete i ProCapita, felanmälan till Tietos support och behörigheter.

[3] SN 2020-05-19 § 72
[4] 2020-04-22 § 16

Vi har även tagit del av socialnämndens samt barn och- utbildningsnämndens rutiner vad gäller behörigheter inom systemet ProCapita som fastställdes under våren 2019. Av rutinerna framgår bl.a. att det är behörig chef som beställer behörigheter till ProCapita, att det för nya och för ändrade behörigheter ska fyllas i en beställningsblankett som skickas till systemansvarig. Systemansvarig ska även regelbundet kontrollera användare i systemet. Av rutinerna framgår att det för personal som inte längre ska ha behörighet ska fylla i en blankett som skickas till servicedesk och som kopia till systemansvarig. Beställningsblanketterna ska därefter alltid skickas till löneenheten för förvaring tillsammans med den anställdes personakt.

Vid avstämning framgår att barn- och utbildningsnämnden inte följt upp behörigheter till systemet ProCapita vilket beskrivs vara en följd av att förvaltningen endast beställt tre nya behörigheter till systemet under de senaste 1,5 åren vilket bidragit till att de känner att de har kontroll över behörigheterna.

Inte heller socialnämnden har följt upp behörigheter till systemet ProCapita. Enligt uppgift planeras ett förfarande för kontroll av behörigheter.

Vi har tagit del av Centrala ITs/informationssäkerhetssamordnarens sammanställning av interna kontroller för år 2019 där det bl.a. konstaterats brister i socialförvaltningens verksamhetssystem. Orsaken uppges vara att ansvarig chef inte meddelat systemförvaltarna vid avslutad anställning så behörigheterna i systemet inte har avslutats.

Kultur- och tekniknämnden meddelade i deras svar att åtgärder vidtagits och att dessa finns upptagna i det reviderade dokumentet för ”beskrivning av behörigheter för kultur- och teknikförvaltningens verksamhetssystem samt rutiner för behörighetstilldelning”. Av svaret framgår att dokumentet beskriver systemen med bl.a. uppgifter om behörighetstilldelning, utförande av riskanalys, antal systemförvaltare och interna kontroller.

Vi har tagit del av kultur- och tekniknämndens dokument för ”beskrivning av behörigheter för kultur- och teknikförvaltningens verksamhetssystem samt rutiner för behörighetstilldelning”. Vad gäller rutiner för behörighetsbeställning framgår av dokumentet att behörigheter till Centrala IT system beslutas av verksamhetsansvarig chef som därefter beställs av utsedd behörighetsbeställare eller av förvaltningschef. Vad gäller kultur och teknikförvaltningens egna system beslutas behörigheter av verksamhetsansvarigchef som systemförvaltaren/systemadministratören därefter ansvarar för.

Av rutinerna för kultur- och tekniknämnden framgår även att kontroll av behörigheter ska genomföras minst en gång per år av systemförvaltaren/systemadministratören som därefter ansvarar för att rapportera till Centrala IT enligt deras rutiner.

Vid avstämning framgår att kultur- och tekniknämnden kommer vid nämndsammanträdet den 17 juni 2020 redovisas en genomförd kontroll av behörigheter till nämndens verksamhetssystem utan anmärkningar.

Vad gäller systemförvaltningsplaner inom kultur- och tekniknämnden har förvaltningen påbörjat ett arbete som beräknas fortskrida under år 2020.

3.1.3 Bedömning

Vi konstaterar att kommunstyrelsen utifrån den genomförda GAP-analysen har vidtagit antal åtgärder enligt lämnade rekommendationer samtidigt som vissa åtgärder fortfarande pågår, däribland införandet av LIS-system och processdokumentation. Vi anser att det är väsentligt att kommunstyrelsen som övergripande IT-ansvarig säkerställer att de brister som konstateras i analyserna åtgärdas.

Vi rekommenderar kommunstyrelsen att säkerställa att beslutade åtgärder genomförs.

Vi noterar att socialnämnden samt barn- och utbildningsnämnden framtagit förvaltningsplaner för att möjliggöra planering och utveckling av IT-stöd. Då förvaltningsplanerna ska, såsom vi uppfattar det, syfta till att säkra rutiner och riktlinjer för förvaltning av IT-system anser vi att det bör upprättas rutiner för att regelbundet följa upp och säkerställa att förvaltningsplanerna innehåller aktuell och väsentlig information.

Vi ser positivt på att barn- och utbildningsnämnden, socialnämnden och kultur- och tekniknämnden har upprättat rutiner vad gäller behörighetstilldelning för verksamhetssystem. Vi konstaterar däremot att varken barn- och utbildningsnämnden eller socialnämnden följt upp eller kontrollerat behörigheter till verksamhetssystemet ProCapita. Vi noterar från Centrala IT/informationssäkerhetssamordnarens sammanställning av interna kontroller för år 2019 brister vad gäller behörigheter i socialförvaltningens verksamhetssystem.

Vi rekommenderar socialnämnden samt barn- och utbildningsnämnden att regelbundet följa upp och säkerställa att förvaltningsplanerna innehåller aktuell och väsentlig information.

Vi rekommenderar barn-och utbildningsnämnden och socialnämnden att utifrån beslutade behörighetsrutiner regelbundet följa upp och säkerställa att rätt behörigheter har tilldelats och förhindra obehörig åtkomst.

Vad gäller kultur- och tekniknämnden pågår ett arbete att ta fram en förvaltningsplan som beräknas fortskrida under år 2020. Vi rekommenderar kultur- och tekniknämnden att säkerställa att arbetet med förvaltningsplanen slutförs.

3.2 Vägledande råd och bestämmelser

Den tredje rekommendationen riktade sig till kommunstyrelsen och handlade om att följa upp att styrdokumenten, bl.a. vägledande råden och bestämmelser, efterlevs. I granskningen hade följande punkter tagits upp, men rekommendationen gäller styrdokumenten som innehåller en mängd krav generellt:

- Behovet av två systemförvaltare
- Att riktlinjer för behörighetstilldelning upprättas och att blankett/e-tjänst ger mer stöd för tilldelning vad gäller nivåer
- Att regelbundna interna kontroller genomförs och att resultatet rapporteras till centrala IT

Styrelsen rekommenderades även att tillse att styrdokument regelbundet omprövas, gärna årligen.

Styrelsen meddelade i sitt svar att nya vägledande råd och bestämmelser (VROB) är gjorda och anpassade efter nya dataskyddsförordningen samt att dokumentet för drift och förvaltning har utökats med mer detaljerad och tydligare information vad gäller systemägare och systemförvaltarens ansvar. Även en mall för systemförvaltningsplan har upprättats och informerats om vid gemensamt möte i december år 2018.

Av svaret framgår att fastställda riktlinjer för behörigheter finns tillgängliga där ansvarig chef tilldelar behörigheter samt vid kommunens intranät. Styrelsen meddelade även att ett arbete vad gäller förbättrad säkerhet har genomförts som innebär att medarbetarens behörigheter stängs i och med sista arbetsdag samt att Centrala IT gjort en e-tjänst för beställning av behörigheter som förväntas publiceras Q1 år 2019.

Vad gäller internkontroll meddelade styrelsen i sitt svar att de under år 2017 genomförde en löpande intern kontroll av alla de prioriterade systemen med fokus på behörigheter och loggar. Kontroller genomfördes även på Centrala IT:s konsultkonton, VPN-koppling för distansarbetsplats, växelanknytningar, mobilabonnemang samt surfmängder. Under oktober år 2018 togs frågan upp med ansvariga för internkontroll i syfte att få till ytterligare stående kontrollpunkter.

Av svaret framgår också att Centrala IT har sedan år 2010 utfört egna interna dokument för ”året som gått 20xx” vilket kommer från och med år 2019 även inkludera kontroller från övriga förvaltningar. Dessa interna dokument ska anmälas till styrelsen som ett informationsärende.

Vi har tagit del av de vägledande råden och bestämmelserna som enligt uppgift håller på att revideras och som beräknas färdigställas under hösten år 2020. I den uppdaterade VROB för förvaltning och drift kommer det bl.a. att tryckas hårdare på att alla system som betecknas som stora eller mellan, d.v.s. kommunens tio prioriterade system eller 25–150 användare, ska ha två systemförvaltare samt att avsnittet för behörighetsadministration ska tydliggöras. Enligt uppgift ska VROB-dokument i övrigt årligen kontrolleras och vid behov revideras.

Vid avstämning framgår att samtliga systemförvaltare, främst för de tio prioriterade systemen, har regelbundna träffar för uppföljning och genomgång av IT-systemen. Enligt

uppgift är dessa träffar, som normalt genomförs fyra gånger per år, uppskattade bland systemförvaltarna där det ges möjlighet till att få hjälp och stöttning i arbetet.

Vad gäller behörigheter för kommunens intranät framkom vid avstämning att det pågår ett test av en ny e-tjänst vars syfte är att genom två steg garantera rätt beställare. Den nya e-tjänsten bygger dels på att endast de personer som har beviljats behörigheter ska ha åtkomst till tjänsten samt att Servicedesk ska ha möjlighet att kontrollera beställare, datum och tid vid utlämnande av beställningar. I praktiken bedöms det nya systemet säkra rutiner som i ska göra det omöjligt för obehöriga att få tillgång till kommunens nät.

Av centrala ITs/informationssäkerhetssamordnarens sammanställning av genomförda interna kontroller utförda under år 2019 med anledning av Dataskyddsförordningen framgår att det under december år 2019 genomfördes kontroller av behörigheter i kommunens tio prioriterade system. Kontrollerna visade på brister i kommunens kartsystem och socialförvaltningens verksamhetssystem, se även ovan. Enligt sammanställningen har felen åtgärdats.

Vi har även tagit del av Centrala IT/informationssäkerhetssamordnarens internkontrollplan för år 2020 och noterar att det finns ett antal planerade kontrollmoment med en prioritet från låg till hög fördelade kvartalsvis, däribland kontroll av VROB och instruktioner samt utbildningsinsatser. Vi kan av år 2020 års internkontrollplan inte ta del av något kontrollmoment kopplat till kontroll av behörigheter. Vid avstämning framgår att kontroll av behörigheter dock kommer att genomföras av kommunens tio prioriterade system under år 2020 även om det inte framgår av internkontrollplanen.

Enligt uppgift rapporterade Centrala IT för året som gått senast år 2018. Av IT-bokslutet framgår bl.a. uppföljning av IT-säkerheten och strategi samt vilka aktiviteter som genomförts under året. På grund av byte av leverantör har Centrala IT inte rapporterat för år 2019. Enligt uppgift planeras liknande rapporter att genomföras när de fått kännedom om vilka uppgifter som går att ta del av via den nya leverantören.

Till hösten år 2020 planeras även en ny informationssäkerhetspolicy färdigställas.

3.2.1 Styrelse och nämndernas internkontroll med anledning av IT-säkerhet och GDPR

Av kommunstyrelsens internkontrollplan för år 2019 och år 2020 noterar vi att det finns ett kontrollmoment kopplat till kontroll av behörigheter och användarnamn som ska granskas två gånger per år. Vi har inte tagit del av 2019 års uppföljning av internkontroll vad gäller behörigheter och användarnamn.

Vi har tagit del av socialnämndens samt barn- och utbildningsnämndens internkontrollplaner för år 2019 och noterar att internkontrollplanerna innehåller ett kontrollmoment kopplat till nano-utbildning inom GDPR och IT-säkerhet.

Av socialnämndens uppföljning av internkontroll per 18 december 2019[5] framgår att samtliga anställda inom förvaltningen har tagit del av nano-utbildning via centrala IT.

Av barn- och utbildningsnämndens uppföljning av intern kontroll framgår att 98 % av personalen hade genomfört utbildning. Nämnden bedömer att de som inte deltagit i

[5] 2019-12-18 § 162

utbildning med stor sannolikhet är nyanställda eller beror på ogiltiga mailadresser. Av uppföljningen framgår att inga åtgärder vidtas.

Av kultur- och tekniknämndens internkontrollplan för år 2019 framgår två kontrollmoment kopplat till IT- och informationssäkerhet vilket framgår ska granskas en gång per år. Uppföljning av kontrollerna avsåg dels kontroll av att behörigheter tagits bort i verksamhetssystem för de tjänstepersoner som avslutat anställning, dels att nyanställda har tagit del av VROB avseende IT-säkerhet. Enligt uppföljningen uppges att "resultatet av granskningen visar att den interna kontrollen är god".

Samma kontrollpunkter finns med i kultur- och tekniknämndens internkontrollplan för år 2020 med två planerade granskningstillfällen.

Miljö- och byggnadsnämnden hade år 2019 inga kontrollmoment kopplat till IT-säkerhet och GDPR i sin internkontrollplan.

3.2.2 Bedömning

Vi konstaterar att de vägledande råden och bestämmelserna (VROB) som är anpassade efter Dataskyddsförordningen är under revidering i syfte att bl.a. säkerställa behovet av två systemförvaltare i kommunens stora och medelstora system. Vi bedömde vid vår uppföljning 2018 att det rimligtvis borde finnas fler system än de uppräknade tio systemen som är verksamhetskritiska och att det bör övervägas om riskanalyser bör göras även för dessa. Såsom vi uppfattar det kommer denna synpunkt beaktas vid revideringen.

Vi ser positivt på de träffar som genomförs tillsammans med systemförvaltarna där det ges möjlighet till stöttning i arbetet för uppföljning och genomgång av systemen.

Vi anser att det är väsentligt att även systembehörigheter regelbundet följs upp.

Vi vill betona risken av att behörigheter inte justeras i samband med att en tjänst förändras. Vi anser att det bör säkras rutiner fram tills att den nya e-tjänsten är implementerad. Verksamheterna behöver också löpande följa upp att rätt personer har rätt behörighet för att säkerställa att obehöriga inte får tillgång till system.

Vi rekommenderar kommunstyrelsen att regelbundet följa upp och säkerställa efterlevnaden av de vägledande råden och bestämmelser, däribland kravet på två systemförvaltare i berörda system.

Vi rekommenderar styrelse och nämnder att, fram till dess att den nya e-tjänsten är i bruk, regelbundet följa upp och säkra rutiner i syfte att förebygga så att obehöriga inte får tillgång till kommunens system.

3.3 Dataskyddsförordningens efterlevnad

Den sista rekommendationen som lämnades riktade sig till styrelse och nämnder och handlade om att säkerställa att Dataskyddsförordningen efterlevs samt att inhämta statusrapport med tillhörande plan för åtgärder för uppföljning.

Styrelsen meddelade i sitt svar att dataskyddssamordnaren för kommunledningskontoret under år 2018 har skapat en handlingsplan för det genomförda arbetet med införandet av dataskyddsförordningen vilket förmedlats till samtliga förvaltningar med rekommendationen att göra liknande dokument för sin tillhörande nämnd. Av svaret framgår vidare att arbetet med dataskyddsförordningen är ständigt pågående där bl.a. register ska hållas aktuellt, incidenter anmälas och samtycken underhållas. Dataskyddsombudet har även under oktober/november år 2018 genomfört revision hos nämnderna enligt Datainspektionens riktlinjer.

Vi har tagit del av handlingsplanen vars syfte är att både fungera som ett stöd i arbetet med informationssäkerhet och dataskydd samt stödja medarbetarna i efterlevandet av de styrande dokumenten ”informationssäkerhetspolicy och ”VROB för Dataskydd” samt övriga riktlinjer samt mallar. Av handlingsplanen framgår att kommunchef samt respektive förvaltningschef ansvarar för att aktiviteterna i handlingsplanen följs upp och rapporteras till dataskyddssamordnare som därefter ska rapportera till dataskyddsombudet.

Enligt uppgift följs handlingsplanen, som utgår från Datainspektionens Vägledning till personuppgiftsansvariga och en checklista från SKR, upp löpande med regelbundna möten tillsammans med samordnare och dataskyddsombud. Den senaste träffen ägde enligt uppgift rum i januari år 2020. Ytterligare ett uppföljningsmöte var planerat under april 2020 som till följd av Covid-19 har blivit förskjutet, men förhoppningen är enligt uppgift att mötet ska genomföras innan sommarledigheten.

Socialnämnden samt barn- och utbildningsnämndens meddelade i deras svar att nämnderna kommer att erhålla en statusrapport vad gäller GDPR samt plan för åtgärder och uppföljning. Av svaren framgår också att nämnderna i sin internkontrollplan inför år 2019 kommer ha en kontrollpunkt gällande att all personal tagit del av utbildningsinsatser inom GDPR och IT-säkerhet. Resultatet ska årligen rapporteras till kommunstyrelsen.

Enligt uppgift erhöll socialnämnden statusrapport vad gäller arbetet utifrån GDPR och dataskyddslagen den 7 februari 2019[6]. Vi har tagit del av statusrapporten och noterar att ett antal aktiviteter inte bedöms som slutförda, däribland aktiviteten att säkerställa att PUB-avtal tecknas, som enligt rapporten har en hög prioritet. Vad gäller övriga aktiviteter som inte bedöms vara uppfyllda varierar dessa med en prioritet från normal till att bli aktuella utifrån krav och beställning.

Vi har tagit del av ytterligare en tillsynsrapport vad gäller socialnämndens arbete utifrån införandet av Dataskyddsförordningen som enligt uppgift kommer att rapporteras vid nämndens sammanträde den 2 september 2020. Av rapporten framgår att nämndens utmaningar bl.a. består av att öka medarbetarnas medvetenhet och kunskap vad gäller lagstiftningen och framförallt processer kring personuppgiftsincidenter. Av rapporten

[6] 2019-02-07 §26

framgår att ytterligare en utmaning för förvaltningen och nämnden är att hantera avtal med olika leverantörer för behandling av personuppgifter, s.k. personuppgiftbiträdesavtal – PUB-avtal. Enligt rapporten kommer förvaltningen tillsammans med dataskyddsombudet att fortsätta arbeta med denna fråga som bedöms vara aktiv så länge förordningen finns.

Barn- och utbildningsnämnden erhöll enligt uppgift statusrapport vad gäller arbetet utifrån GDPR och dataskyddslagen den 19 december 2018[7]. Av statusrapporten framgår att ett antal åtgärder har vidtagits till följd av införandet av GDPR, däribland inventering av IT-system och kontaktpersoner, identifiering av avtal och dess behov av personuppgiftsbiträdesavtal samt insamling av huvudavtal och identifiering av vilken hantering som kräver samtycke. Vid rapporteringstillfället fick nämnden även ta del av information vad gäller införandet GDPR och dataskyddslagen samt information kring utbildning för berörd personal.

Vi har tagit del av ytterligare en tillsynsrapport vad gäller barn- och utbildningsnämndens arbete utifrån införandet av Dataskyddsförordningen som enligt uppgift kommer att protokollföras vid nämndens sammanträde den 9 september 2020. Av rapporten framgår att det finns brister vad gäller tecknade avtal med leverantörer som hanterar processer för personuppgifter (PUB-avtal). Av tillsynsrapporten framgår också att det till följd av Covid-19 har bidragit ett ökat behov av digitala stöd och verktyg för distansundervisning som riskerar att medföra risker för registrerade, bl.a. elever.

Såsom vi uppfattat avser statusrapporterna det som i riskutvärderingen benämns som åtgärdsplan. Syftet med planen är att säkra kontinuiteten i riskutvärderingsprocessen genom återkommande och repetitiva utvärderingar och bedömningar i enlighet med årshjulsprincipen.

Kultur- och tekniknämndens meddelade i sitt svar att förvaltningens dataskyddssamordnare fått i uppdrag att informera kontorspersonal samt nämndens ledamöter om den nya dataskyddsförordningen GDPR och det aktuella läget av införandet. Av svaret framgår också att förvaltningen kommer att följa upp och rapportera aktiviteterna utifrån den centralt framtagna ”handlingsplan för dataskydd”.

Enligt uppgift har dataskyddssamordnaren informerat nämnden om det löpande arbetet med GDPR vid ytterligare tillfällen samt att förvaltningen årligen fyller i en checklista för uppföljning och rapportering vad gäller arbetet utifrån GDPR som förmedlas till dataskyddssamordnaren.

Vi har tagit del av kultur- och teknikförvaltningens checklista för uppföljning och rapportering för år 2019 och noterar att medparten av aktiviteterna bedöms som slutförda. Vad gäller aktiviteten ”Säkerställa att PUB-avtal tecknas” noterar vi att aktiviteten endast bedöms som uppfylld till 75 %. Av checklistan saknas bedömning av aktiviteternas prioritet. Enligt uppgift är en ny checklista är framtagen centralt vilket kommer tillämpas under år 2020.

[7] 2018-12-19 §124

Miljö- och byggnadsnämnden meddelade i sitt svar att nämndens verksamhet har interngranskats av kommunens dataskyddsombud avseende Dataskyddsförordningen och avser vidta de konkreta förbättringsförslagen från interngranskningen.

Miljö- och byggnadsnämnden meddelade också i sitt svar att nämnden planerar att använda kommunens övergripande ärendehanteringssystem för handläggning från och med februari år 2019. När det nya ärendehanteringssystemet införs så kommer mallar att uppdateras och kraven i Dataskyddsförordningen tillgodoses. Av svaret framgår vidare att nämnden i övrigt lämnar synpunkterna om systemförvaltning, behovstilldelning m.m. utan synpunkt eller åtgärd.

Vid avstämning framgår att miljö- och byggnadsnämnden har vidtagit de konkreta förbättringsförslagen som framgick vid interngranskningen och att nämnden använder kommunens övergripande ärendehanteringssystem (LEX) sedan oktober år 2019. Mallar för ärendehantering uppges vara uppdaterade så att kraven enligt dataskyddsförordningen tillgodoses. Vi har inte närmare verifierat den uppgiften.

3.3.1.1 Bedömning

Vi konstaterar att åtgärder vidtagits efter 2018 års lämnade rekommendationer.

Vi ser positivt på att en handlingsplan framtagits i syfte att säkerställa efterlevnaden av Dataskyddsförordningen och konstaterar att handlingsplanen regelbundet följs upp.

Vi konstaterar att nämnderna erhåller statusrapporter vad gäller arbetet utifrån införandet av dataskyddsförordningen och noterar att rapporterna visar på ett antal utmaningar och brister. Vad gäller socialnämnden konstaterar vi bl.a. att utmaningen med personuppgiftbiträdesavtal (PUB) som noterades vid den första statusrapporteringen kvarstår enligt den uppföljning som kommer rapporteras till nämnden vid sammanträdet i september 2020. Även barn- och utbildningsnämnden samt kultur- och tekniknämnden har konstaterade brister vad gäller PUB-avtal. Vi anser att det är väsentligt att nämnderna vidtar åtgärder för att säkerställa att hanteringen av avtal med olika leverantörer sker ändamålsenligt och i enlighet med Dataskyddsförordningen.

Vi rekommenderar att socialnämnden, barn och utbildningsnämnden samt kultur- och tekniknämnden vidtar åtgärder och säkerställer att hanteringen av avtal sker ändamålsenligt.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att ett flertal åtgärder är vidtagna enligt lämnade rekommendationer men att det finns utrymme för ytterligare förbättringar. Några av dessa bland annat gällande behörigheter anser vi är ytterst väsentliga att dessa beaktas. Vi vill betona vikten av att kommunstyrelsen och nämnderna säkerställer att fattade beslut verkställs och att effekten av besluten följs upp.

4.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi att:

- kommunstyrelsen säkerställer att beslutade åtgärder genomförs, se avsnitt 3.1
- socialnämnden samt barn- och utbildningsnämnden regelbundet följer upp och säkerställer att förvaltningsplanerna innehåller aktuell och väsentlig information, se avsnitt 3.1.
- barn-och utbildningsnämnden samt socialnämnden att utifrån beslutade behörighetsrutiner regelbundet följer upp och säkerställer att rätt behörigheter har tilldelats och förhindrar obehörig åtkomst, se avsnitt 3.1 och 3.2.
- kultur- och tekniknämnden säkerställer att arbetet med förvaltningsplanen slutförs, se avsnitt 3.1.
- kommunstyrelsen regelbundet följer upp och säkerställer efterlevnaden av de vägledande råden och bestämmelser, däribland kravet på två systemförvaltare i berörda system, se avsnitt 3.2.
- styrelse och nämnder, fram till dess att den nya e-tjänsten är i bruk, regelbundet följer upp och säkrar rutiner i syfte att förebygga så att obehöriga inte får tillgång till kommunens system, se avsnitt 3.1 och 3.2.
- socialnämnden, barn och utbildningsnämnden samt kultur- och tekniknämnden vidtar åtgärder och säkerställer att hanteringen av avtal sker ändamålsenligt.

Datum som ovan

KPMG AB

Klara Engström
Kommunal revisor

Lena Medin
Certifierad kommunal revisor