Revisorerna 2018-06-19

Kommunstyrelsen
Humanistiska nämnden
Socialnämnden

För kännedom:
Kommunfullmäktiges presidium

Revisionsrapport: Granskning av införandet av dataskyddsförordningen

Revisorerna har uppdragit till KPMG att genomföra en granskning av införandet av dataskyddsförordningen.

Revisionen önskar att kommunstyrelsen, humanistiska nämnden och socialnämnden lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 24 oktober 2018.

Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

För Ånge kommuns revisorer

Roger Sundin
Ordförande

Alf Hallén
Vice ordförande

Granskning av införandet av dataskyddsförordningen

Rapport

Ånge kommun

KPMG AB

2018-06-19

Antal sidor 11

Ånge kommun
Granskning av införandet av dataskyddsförordningen

2018-06-19

Innehållsförteckning

1 Sammanfattning

Vi har av Ånge kommuns revisorer fått i uppdrag att granska hur kommunen har förberett sig inför införandet av dataskyddsförordningen[1]. Uppdraget ingår i revisionsplanen för år 2018.

Syftet är att granska hur kommunen har förberett sig inför införandet av dataskyddsförordningen i maj 2018.

Vår sammanfattande bedömning utifrån granskningens syfte är det pågår ett arbete för att förbereda kommunen inför införandet av dataskyddförordningen. Såsom vi uppfattat kommer allt inte att vara klart när lagen träder i kraft. Då det saknas en strukturerad plan och uppföljning av vilka åtgärder som behöver vidtas respektive är vidtagna går det inte att bedöma om tillräckliga åtgärder har vidtagits.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelse samt humanistiska nämnden och socialnämnden

att inhämta en statusuppdatering där det tydligt framgår vad som återstår för att uppfylla lagens krav.

att utifrån sammanställning över kvarstående punkter lämna tidsbestämt uppdrag till förvaltningen att färdigställa arbetet samt att resurser avsätts.

att följa upp att uppdraget genomförs enligt plan. Eftersom lagstiftningen har trätt i kraft bedömer vi att detta måste ske skyndsamt.

[1] SFS 2018:218

2 Inledning/bakgrund

Vi har av revisorerna i Ånge kommun fått i uppdrag att granska hur kommunen förberett sig inför införandet av dataskyddsförordningen (även benämnd GDPR[2]). Uppdraget ingår i revisionsplanen för år 2018.

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 dataskyddsförordningen kommer att gälla som lag i samtliga medlemsstaterna och ersätter då tidigare nationell lagstiftning.

Mycket i dataskyddsförordningen liknar de regler som finns i personuppgiftslagen, men det är viktigt att poängtera att dataskyddsförordningen innehåller stora förändringar och vissa helt nya bestämmelser. Den personuppgiftsansvariges ansvar och skyldigheter förtydligas och utökas och de registrerades rättigheter förstärks. De nya kraven kan komma att medföra stora förändringar i kommunernas verksamhet.

Det är viktigt att organisationerna redan påbörjat arbetet med hur de ska anpassa sig till dataskyddsförordningen. Det kan handla om att införa rutiner för att tillmötesgå dataskyddsförordningens utökade krav på öppenhet och de registrerades rättigheter. Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket kan medföra ökade krav på dokumentation. En anpassning till dataskyddsförordningen kommer att kräva att kommunerna ser över sin interna styrning och riktlinjer för hur personuppgifter hanteras.

Revisorerna har bedömt att det föreligger *risk* att verksamheterna inte har kommit tillräckligt långt i sina förberedelser, och ser det som *väsentligt* att detta område granskas.

2.1 Syfte, revisionsfråga och avgränsning

Syftet är att granska hur kommunen har förberett sig inför införandet av dataskyddsförordningen i maj 2018.

Granskningen har besvarat följande revisionsfrågor:

- Har kommunen identifierat vilka åtgärder som ska vidtas inför införandet av dataskyddsförordningen?
- Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?
- Finns ansvariga för införandeprocessen utsedda i kommunerna?
- Är ekonomisk och personell resursåtgång identifierad?
- Utövar kommunstyrelsen uppsikt över införandeprocessen?

[2] General Data Protection Regulation

Granskningen omfattar enligt projektplanen kommunstyrelsens övergripande tillsyn och dess ansvar avseende anpassning till dataskyddsförordningen. Vid genomförandet inhämtades även uppgifter vad gäller humanistiska nämnden och socialnämnden, varför iakttagelser och rekommendationer även gäller dessa nämnder.

Granskningen baseras främst på intervjuer, se även under metod, och lämnade uppgifter har verifierats endast i begränsad omfattning.

Intervjuerna med verksamheterna genomfördes den 17 maj, d.v.s. en dryg vecka innan dataskyddsförordningen började att gälla. Intervjuer med ordförande i kommunstyrelse och nämnder genomfördes i början av juni.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Kommunallagen 6 kap § 6
- Gällande lagar och rekommendationer avseende dataskyddsförordningen
- Tillämpbara interna regelverk och policys

2.3 Metod

Granskningen har genomförts genom hearing med berörda tjänstemän vid kommunkansliet, humanistiska nämnden (HUM) och socialförvaltningen. Kompletterande intervjuer har skett med ordförande för kommunstyrelsen, humanistiska nämnden och socialnämnden. Dokumentstudie har genomförts i begränsad omfattning.

Rapporten är faktakontrollerad av verksamhetsutvecklare, kommunkansliet.

3 Resultat av granskningen

3.1 Lagstiftning

EU:s dataskyddslag utgjorde från år 1995 en gemensam grund inom unionen, men som direktiv var det upp till varje land att realisera regelverket och tolka det.
Den 25 maj 2018 fick Sverige och övriga EU-medlemsländerna en ny gemensam lagstiftning, som ska ersätta den nuvarande personuppgiftslagen (PUL) i Sverige. Den nya lagstiftningen, dataskyddsförordningen, innebär bland annat nya och skarpare regler om hur företag, myndigheter och organisationer får behandla personuppgifter[3].

Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Förordningen har även mål om att frambringa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras. Detta uppfylls genom att förordningen är direkt tillämplig i de skilda medlemsstaterna och att samma regler gäller inom hela unionen. Andra syften med att ta fram en ny dataskyddsförordning har varit att modernisera dataskyddsdirektivets regler från år 1995 och att tillämpa dessa till det nya digitala samhället.

Tillsynsmyndigheten (datainspektionen) kan besluta att en myndighet som bryter mot reglerna ska betala en administrativa sanktionsavgifter. För en myndighet gäller beloppsgränserna för mindre allvarliga överträdelser högst 5 mnkr och för allvarliga överträdelser högst 10 mnkr.

3.2 Införandet av dataskyddsförordningen

Förberedelser inför införandet av dataskyddsförordningen inleddes enligt uppgift i maj 2017 med utbildning för chefer och nyckelpersoner från samtliga förvaltningar.

Ansvaret för att införa dataskyddsförordningen följer ordinarie linjeorganisation. Vid varje förvaltning finns en eller flera personer som har en samordnande roll i arbetet. Tidigare personuppgiftsombud (under år 2017) och efterföljande personuppgiftsombud (från år 2018 och nu som dataskyddsombud) har arbetat med att utbilda ansvariga och kontaktpersoner i förvaltningarna om dataskyddsförordningen och ge stöd i arbetet med registrering av behandlingar av personuppgifter. Införandet har inte tilldelats några särskilda resurser och sker därför parallellt med ordinarie arbetsuppgifter.

En plan för arbetet som kallas vägledning ”Förberedelser inför dataskyddsförordningen” har tagits fram. Den version vi har tagit del av är senast uppdaterad 2018-04-20. Såsom vi uppfattat är vägledningen inte fastställd av kommunstyrelsen eller av någon av de granskade nämnderna.

[3] Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.

Av vägledningen framgår:

- Att kommunledningskontoret tar fram gemensamma policys, riktlinjer, anvisningar och rutiner gällande personuppgifter inom kommunkoncernen.
- Att varje styrelse och nämnd är personuppgiftsansvariga. Det praktiska ansvaret för att genomföra anpassningar till den nya lagstiftningen inom varje förvaltning följer linjen från förvaltningschef ut till varje anställd.

I vägledningen finns ett antal punkter som vi uppfattar att varje förvaltning ska genomföra:

1. Kartlägga alla personuppgiftsbehandlingar som sker i verksamheten
2. Kartlägga samtliga personuppgiftsbehandlingar och upprätta en registerförteckning
3. Analysera, dokumentera och skapa en handlingsplan för nödvändiga åtgärder
4. Löpande införa koncerngemensamma policys, riktlinjer och anvisningar och rutiner som rör behandling av personuppgifter
5. Se över och införa rutiner vid behov.

Punkterna, och även stor del av innehållet i vägledningen i övrigt, motsvarar SKL[4]s checklista.

Det framgår inte av vägledningen när punkterna ska vara genomförda. Enligt uppgift har kommunledningens målsättning varit att arbetet ska vara klart den 25 maj 2018.

Någon dokumenterad kartläggning (p 1 och 2) finns inte utan ansvariga menar att den skett direkt i registerförteckningen Draftit (p 2). Som kommentar till om förteckningen omfattar samtliga personuppgiftsbehandlingar uppges att förteckningen förs löpande och är ”klar” även om fler behandlingar kan tillkomma eller utgå. Vad gäller handlingsplaner (p 3) så pågår det arbetet.

Enligt uppgift har följande kommunövergripande dokument(p 4 och 5) tagits fram (dokument som kommer att tas fram kommenteras nedan):

1. Riktlinjer för hantering av e-post (ska enligt uppgift kompletteras)
2. Rutin samt e-tjänst för anmälan av personuppgiftsincident
3. Rutin samt blanketter förbegäran om registerutdrag
4. En e-tjänst för samtycke vid fotografering (klar men ej publicerad)
5. En mall för att dokumentera och redovisa hur varje personuppgiftsansvarig uppfyller dataskyddsförordningen (snart klar).
6. Mall för personuppgiftsbiträdesavtal

Frågan om kompletteringar i kommunens policy för informationssäkerhet behövs är under beredning.

[4] Sveriges kommuner och landsting

Den politiska ledningen är informerade om att det pågår ett arbete med att införa dataskyddsförordningen. Den politiska ledningen har däremot inte fått, eller begärt, rapport över hur arbetet fortlöper. Någon rapport till styrelse och nämnder för att rapportera statusen beträffande vad som är klart respektive inte innan lagstiftningen träder i kraft har inte lämnats. Efter våra intervjuer med ansvariga politiker uppfattar vi att en sådan förteckning kommer att begäras in.

3.3 Status för införandet

Vår granskning genomfördes en dryg vecka före dataskyddsförordningen trädde kraft. Såsom framgår ovan finns ingen förteckning över vilka åtgärder som ska vidtas, och därmed saknas även strukturerad sammanställning över vad som är klart respektive inte.

Bland annat följande uppgifter lämnades vid våra intervjuer gällande arbetet med att införa dataskyddsförordningens bestämmelser:

- Politiker och chefer samt nyckelpersoner och kontaktpersoner har erbjudits utbildning/information avseende dataskyddsförordningen. Övriga anställda kan ta del av informationsfilm och samlad dokumentation med checklistor och rutiner via intranätet samt ska få information vid arbetsplatsträffar. Enligt uppgift har personalen vid HUM ännu inte fått information vid arbetsplatsträffar.
- Registerförteckning sker i systemet DraftIt. I systemet finns möjlighet att registrera en stor mängd av de uppgifter som efterfrågas enligt dataskyddsförordningen. Samtliga system är enligt uppgift inte registrerade och det kan även saknas uppgifter för vissa registrerade system. Enligt uppgift har personuppgiftsansvariga fått i uppgift att färdigställa en förteckning över vad som är klart respektive saknas.
- Det är osäkert om samtliga register med känsliga personuppgifter är identifierade.
- Arbetet med att inventera och bedöma vilka system som innehåller känsliga uppgifter pågår. Det gäller även arbetet med att kartlägga så kallat ostrukturerat material.
- Frågor om samtycke, återtagande av samtycke och personuppgifter för minderåriga är inte fullt ut lösta.
- Stöd till verksamheterna i arbetet med klassning av information med bedömning av säkerhetsnivåer utförs av informationssäkerhetssamordnaren.
- Vad gäller personuppgiftsbiträdesavtal utgår kommunen från den mall som SKL tagit fram. Avtal har enligt uppgift skickats ut till ett antal leverantörer varav ett antal inte accepterar avtalsförslaget. Förteckning över vilka avtal som är klara, respektive inte saknas.
- Styrdokument behöver uppdateras för att bättre stämma överens med den nya lagstiftningen. Enligt kommunens bedömning gäller det främst policy för informationssäkerhet alternativt om särskild policy för persondataskydd ska upprättas.
- Avtal om dataskyddsombud har upprättats. Enligt uppgift har styrelse och samtliga nämnder fattat erforderliga beslut och anmälan till datainspektionen.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är det pågår ett arbete för att förbereda kommunen inför införandet av dataskyddförordningen. Såsom vi uppfattat det kommer allt inte att vara klart när lagen träder i kraft. Då det saknas en strukturerad plan och uppföljning av vilka åtgärder som behöver vidtas respektive är vidtagna går det inte att bedöma om tillräckliga åtgärder har vidtagits.

Vi anser att det är väsentligt att identifiera vilka åtgärder som återstår. Det behöver upprättas en plan för vad som ska göras, av vem och när åtgärden ska vara klar. Vi anser vidare att kommunstyrelse och övriga nämnder, som ansvariga för person-uppgifter, måste tillse att arbetet slutförs och att lagstiftningen efterlevs.

Vår bedömning är att införandet av dataskyddsförordning med fördel skulle ha bedrivits som ett projekt, eller i varje fall under projektliknande former, för att därefter överlämnas till en förvaltande organisation. Den projektmodell som Ånge kommun tillämpar omfattar t.ex. kartläggning som identifierar vilka åtgärder som behöver vidtas och resulterar i en detaljerad aktivitet- och tidsplan, som i detta fall har kunnat vara indelad i övergripande, per system och/eller per förvaltning. Till planen ska såsom också framgår av projektmodellen knytas en projektorganisation r som ges tid att arbeta med införandet. Projektet kan därigenom också ekonomiskt följas upp. I projektmodellen finns även rutiner för status- och slutrapportering samt leverans.

4.1 Svar på revisionsfrågorna

— *Har kommunen identifierat vilka åtgärder som ska vidtas inför införandet av dataskyddsförordningen?*

Vi konstaterar att det saknas en formell genomgång över vilka åtgärder som behövde vidtas för att klara kraven enligt dataskyddsförordningen. Vi anser att det också finns en risk för att väsentliga åtgärder kan ha förbisetts eftersom systematisk genomgång över vilka åtgärder som behöver vidtas saknas.

— *Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?*

Det finns en övergripande plan (vägledning) avseende förberedelserna inför dataskyddsförordningen. Planen innehåller uppdrag såsom att kartlägga alla person-uppgiftsbehandlingar samt analyser, dokumentera och skapa handlingsplan för nödvändiga åtgärder. Kartläggningarna och handlingsplanerna har inte genomförts, eller i varje fall inte dokumenterats.

Vi bedömer utifrån våra intervjuer att allt inte är färdigställt inför att lagstiftningen började att gälla i slutet av maj.

— *Finns ansvariga för införandeprocessen utsedda i kommunerna?*

Vid respektive förvaltning har en eller flera personer utsetts för att arbeta med införandet av dataskyddsförordningen. Däremot finns det inte någon samordnare för att leda det kommunövergripande arbetet utöver vad som framgår ovan vad gäller utbildning och stöd bl a i form av olika dokument.

— *Är ekonomisk och personell resursåtgång identifierad?*

Arbetet med att införa dataskyddsförordningen har varken tilldelats ekonomiska eller särskilda personella resurser. Kostnader för dataskyddsombud och datasystem är enligt uppgift budgeterade.

— *Utövar kommunstyrelsen uppsikt över införandeprocessen?*

Kommunstyrelsen utöver enligt vår bedömning inte tillräcklig uppsiktsplikt över införandeprocessen. Vi anser att kommunstyrelsen och övriga nämnder bör inhämta en redogörelse för aktuell status vad gäller arbetet med anpassning till dataskyddsförordningen.

4.2 Rekommendationer

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelse samt humanistiska nämnden och socialnämnden

att inhämta en statusuppdatering där det tydligt framgår vad som återstår för att uppfylla lagens krav.

att utifrån sammanställning över kvarstående punkter lämna tidsbestämt uppdrag till förvaltningen att färdigställa arbetet samt att resurser avsätts.

att följa upp att uppdraget genomförs enligt plan. Eftersom lagstiftningen har trätt i kraft bedömer vi att detta måste ske skyndsamt.

Datum som ovan

KPMG AB

Lena Medin
Certifierad kommunal revisor