Revisorerna 2021-09-15

Kommunstyrelsen
Socialnämnden
Utbildningsnämnden
Tekniska nämnden

För kännedom:
Kommunfullmäktiges presidium

Revisionsrapport: Uppföljande granskning av införande av dataskyddsförordningen

KPMG har på uppdrag av kommunens revisorer genomfört en fördjupad granskning avseende uppföljning av införande av dataskyddsförordningen.

Revisionen önskar att kommunstyrelsen lämnar synpunkter på de slutsatser som finns redovisade i rapporten. Svar önskas senast den 17 december 2021.

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

Uppföljande granskning av införandet av dataskyddsförordningen

Rapport

Ånge kommun

KPMG AB

2021-09-15

Antal sidor 9

Ånge kommun
Uppföljande granskning av införandet av dataskyddsförordningen

2021-09-15

Innehållsförteckning

1	Sammanfattning	2
2	Inledning/bakgrund	3
2.1	Syfte, revisionsfråga och avgränsning	3
2.2	Revisionskriterier	3
2.3	Metod	3
3	Resultat av granskningen	4
3.1	Införandet av dataskyddsförordningen	4
4	Slutsats och rekommendationer	9

1 Sammanfattning

Vi har av Ånge kommuns revisorer fått i uppdrag att genomföra en fördjupad uppföljning avseende iakttagelserna i revisionsrapporten ”införande av dataskyddsförordningen” samt iakttagelserna från den övergripande uppföljningen från år 2020. Uppdraget ingår i revisionsplanen för år 2020 och 2021.

Granskningen syftar till att konstatera om styrelse och nämnder har vidtagit tillräckliga åtgärder med anledning av iakttagelserna från granskningen avseende införandet av dataskyddsförordningen och den övergripande uppföljningen från år 2020.

Vår sammanfattande bedömning utifrån granskningens syfte är att ett antal åtgärder har vidtagits men att det finns utrymme för ytterligare förbättringar. Vi konstaterar att en ny checklista anpassad för det löpande arbetet med GDPR håller på att utformas. Vi vill betona vikten av att checklistan fortsättningsvis bör vara en del av rutinbeskrivningen för det arbete som ska genomföras kontinuerligt. Vi anser vidare att det är väsentligt att planen regelbundet följs upp och rapporteras för att minimera risken att dataskyddsförordningen inte efterlevs.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen och granskade nämnder:

att inhämta en statusuppdatering där det tydligt framgår vad som återstår för att uppfylla lagens krav samt säkerställa att de kvarstående uppgifterna/aktiviteterna enligt handlingsplanen tilldelas en ansvarig och slutförs

att tydliggöra att arbetet med den nya checklistan för att arbetet med dataskyddsordningen ska betraktas som löpande och som regelbundet ska följas upp samt rapporteras

att regelbundet följa upp och säkerställa att personalen har tillräckligt med kunskap och att nya arbetssätt anpassat för GDPR tillämpas

att regelbundet följa upp och säkerställa att rutiner och instruktioner är aktuella och efterlevs

2 Inledning/bakgrund

Vi har av Ånge kommuns revisorer fått i uppdrag att genomföra en fördjupad uppföljning avseende iakttagelserna i revisionsrapporten ”införande av dataskyddsförordningen” samt iakttagelserna från den övergripande uppföljningen från år 2020. Uppdraget ingår i revisionsplanen för år 2020 och 2021.

Revisionen anser det angeläget att göra en uppföljning av de åtgärder som vidtagits med anledning av granskningen.

Revisionen bedömer att det finns en *risk* att beslutade åtgärder inte genomförts fullt ut i enlighet med de svar revisionen erhållit. Det finns också en risk för att vidtagna åtgärder inte fått avsedd effekt. Det är även *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 styrelse och nämnder har vidtagit tillräckliga åtgärder med anledning av iakttagelserna från granskningen avseende införandet av dataskyddsförordningen och den övergripande uppföljningen från år 2020.

Granskningen ska besvara följande revisionsfrågor

- Har åtgärder vidtagits i enlighet med ansvarig styrelse/nämnds beslut?
- Har styrelse/nämnd följt upp att vidtagna åtgärder efterlevs och fått avsedd effekt

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Kommunallagen 6 kap § 6

— Tillämpbara interna regelverk och policys

2.3 Metod

Granskningen har genomförts genom dokumentstudier av relevanta dokument bl.a. handlingsplan för persondataskydd, rutinbeskrivningar och mallar samt intervjuer med berörda tjänstepersoner.

Rapporten är faktakontrollerad av kanslichef, verksamhetsutvecklare samt förvaltningschefer inom socialförvaltningen och för tekniska förvaltningen.

Uppgiftslämnare för utbildningsnämnden har fått rapporten för faktakontroll. Vi har inte erhållit någon återkoppling.

3 Resultat av granskningen

Granskningen bygger på de rekommendationer som lämnades i revisionsrapporten ”införande av dataskyddsförordningen” från år 2018 och de svar som styrelse och nämnder lämnade i samband med denna.

Vår sammanfattade bedömning av vår tidigare genomförda granskning från år 2018 var att det pågår ett arbete för att förbereda kommunen inför införandet av dataskyddsförordningen. Då det saknades en strukturerad plan och uppföljning av vilka åtgärder som behövde vidtas eller var vidtagna gick det inte att bedöma om tillräckliga åtgärder hade vidtagits.

3.1 Införandet av dataskyddsförordningen

Den 25 maj 2018 fick Sverige och övriga EU-medlemsländer en ny gemensam lagstiftning, som ersatte dåvarande personuppgiftslagen (PUL) i Sverige. Den nya lagstiftningen, dataskyddsförordningen, innebar bland annat nya och skarpare regler om hur företag, myndigheter och organisationer får behandla personuppgifter[1].

I syfte att säkerställa att arbetet med att införa dataskyddsförordningen skulle bli klart antog kommunstyrelsen den 4 september 2018 en handlingsplan för persondataskydd. Handlingsplanen är uppbyggd med information kring åtta insatsområden med aktiviteter som behöver genomföras för att säkerställa efterlevnaden av gällande lagstiftning. Följande insatsområden redovisas i handlingsplanen:

- Information och utbildning
- Behandlingar av personuppgifter
- Organisation och roller
- De registrerades rättigheter
- Personuppgiftsincidenter
- Särskilda integritetsrisker
- Skydd för personuppgifter i IT-system
- Avtal med personuppgiftsbiträden

[1] 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.

Till handlingsplanen finns en checklista i syfte att underlätta för förvaltningarna att dokumentera och rapportera status för aktiviteterna. Vi har tagit del av checklistan version 2021-01-04. Av checklistan framgår följande status:

	Antal
Slutförd 100 %	10
Slutfört 50 - 75 %	3
Ej slutförda	22
Totalt	35

Vi noterar att några av de ej slutförda uppgifterna/aktiviteterna anges som prioriterade. Checklistan presenterades för kommunstyrelsen den 2 februari 2021[2] som tackade för informationen. Av protokollet framgår att det pågår ett arbete att se över checklistans utformning och innehåll samt att framtida handlingsplaner kan komma att se annorlunda ut. Vid faktakontroll framkommer handlingsplanen redaktionellt kan komma att justeras men att fokus har varit på att utforma en ny checklista som ska underlätta för den löpande uppföljningen. Checklistan för år 2021 kommer att bytas ut mot en ny i form av en e-tjänst som utformats i samråd med kommunens dataskyddsombud.

Vid intervjuer framkommer att det är svårt att avgöra när införandet av dataskyddsförordningen kan bedömas som ”slutfört” då flera processer kräver ett kontinuerligt arbete, t.ex. registerförteckningar med personuppgiftsbehandlingar. Det uppges dock finnas rutiner och arbetssätt för att hantera detta löpande, bl.a. genom Draftit Privacy Records som är ett webbaserat verktyg där kommunen hanterar sina registerförteckningar över personuppgiftsbehandlingar. Draftit säkerställer också att personuppgiften hanteras på ett korrekt sätt genom att personen som registrerar personuppgiften får ta ställning till ett antal frågeställningar kring bl.a. syfte, gallringstid och samtycke. Vid personuppgiftsbehandlingar som sannolikt medför en hög risk för den registrerades integritet har kommunen utformat en mall för konsekvensbedömning (DPIA[3]). Mallen ska fungera som en vägledning vid konsekvensbedömningen och utgår från de riktlinjer som publicerats av Artikel 29-gruppen, en rådgivande arbetsgrupp inom EU:s samarbete kring dataskydd. Av mallen framgår att konsekvensbedömningen ska genomföras enligt följande fem steg:

1. Bakgrund – beskrivning av behandlingens ändamål
2. Behov av konsekvensbedömning
3. Dataflödesanalys
4. Riskhantering
5. De sju principerna för behandling

[2] § 31
[3] Data Protection Impact Assessment

För begäran om registerutdrag av personuppgifter enligt GDPR har kommunen utformat en självservicetjänst på hemsidan[4]. Via självservicetjänsten går det att genomföra begäran digitalt och beställa blankett för manuell ifyllnad. Om det inkommer en begäran om registerutdrag av personuppgifter så har kommunen utformat en rutin som omfattar elva steg om hur begäran ska hanteras.

Personuppgiftsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas har kommunen en skyldighet att anmäla till Datainspektionen inom 72 timmar från att det har upptäckts. För personuppgifts-incidenter har kommunen utformat rutin som omfattar en beskrivning av ärendeprocessen i sex steg. Av rutinen framgår att alla personuppgiftsincidenter ska anmälas, oavsett risknivå, i en intern e-tjänst. Efter att en anmälan är genomförd skickas den vidare till kommunens dataskyddsombud som bedömer om anmälan behöver skickas vidare till Integritetsskyddsmyndigheten. Det är den personen som upptäckt incidenten som enligt riktlinjen är skyldig att genomföra anmälan, vid behov kan personen få stöd att genomföra anmälan av närmsta chef. Enligt uppgift kommer rutinen för personuppgiftsincidenter revideras i närtid då det har identifierats ett behov att förenkla vissa delar.

Kommunstyrelsen

Inom kommunstyrelseförvaltningen uppges det vid intervju att roller och ansvar kring arbetet med GDPR är tydlig fördelat men att det finns ett behov av ytterligare utbildningar för att säkerställa att all personal tar sitt ansvar och att nya arbetssätt anpassat för GDPR tillämpas. Samtlig personal fick i samband med att lagen trädde i kraft ta del av både interna och externa utbildningar. Därutöver framkommer vid intervju att samtlig personal inom kommunen årligen ska genomföra en digital säkerhetsutbildning.

Arbetet med dataskyddsförordningen rapporteras årligen till kommunstyrelsen. Att detta rapporteras ansvarar enligt uppgift kommunchefen för. Uppföljningen uppges genomföras inom samtliga avdelningar inom förvaltningen som sedan sammanställs innan det görs en sammantagen bedömning. Till följd av covid-19 framkommer vid intervju att arbetet under år 2020 först rapporterades i början av år 2021[5].

Utbildningsnämnden

Vid intervju framkommer att det inom utbildningsförvaltningen pågår en rekrytering av en ny utvecklingsledare som tillsammans med förvaltningschefen ska ansvara för arbetet med GDPR. Vad gäller roller och ansvar inom förvaltningen i övrigt uppges detta vara tydligt fördelat och att förvaltningen har fått ta del av stöttning och hjälp av kommunens verksamhetsutvecklare.

Utöver den utbildningen som erbjöds i samband med att lagen trädde i kraft så har personal inom förvaltningen även tagit del av information kring dataskyddsförordningen i samband med arbetsplatsträffar och övriga interna möten. Skoladministratörerna har också haft regelbundna träffar tillsammans med kommunens dataskyddsombud och verksamhetsutvecklare då administratörerna uppges vara den personal som hanterar personuppgifter mest.

[4] Begäran om registerutdrag - Ånge kommun (ange.se)
[5] KS 2021-02-02

Skolchefen uppges ha det yttersta ansvaret för att arbetet med GDPR följs upp och återrapporteras till nämnden. Under år 2020 delgavs nämnden information om arbetet med checklistan vid sammanträdet den 18 mars 2020[6].

Socialnämnden

Inom socialförvaltningen upplevs roller och ansvar vara tydlig fördelat mellan förvaltningschefen, IT-strategen, systemförvaltaren och verksamhetsutvecklaren som tillsammans arbetar med att säkerställa att dataskyddsförordningen efterlevs.

Utöver den utbildning som personalen fick ta del av i samband med att lagen trädde i kraft så framkommer vid intervju att förvaltningen genomgått ett arbete att digitalisera verksamheterna. Som ett resultat av detta finns information om arbetssätt kopplat till GDPR samlat via bl.a. appar i mobiltelefoner och andra digitala arbetsverktyg. Inom förvaltningen brukar personalen under normala omständigheter också informeras om förändringar i arbetssätt kopplat till GDPR vid arbetsplatsträffar. Dessa träffar har till följd av covid-19 varit inställda under år 2020.

Under år 2020 beslutade nämnden att inkludera kontroll av persondataskydd som en aktivitet i internkontrollarbetet[7]. Av slutrapporteringen framgår att inga avvikelser har noterats.

Uppföljning och återrapportering av arbetet med GDPR till nämnden sker enligt uppgift i samband med att arbetet med intern kontroll återrapporteras. Vi har efterfrågat men inte tagit del av något protokoll eller underlag som visar att detta har följts upp.

Tekniska nämnden

Inom den tekniska förvaltningen är det förvaltningschefen som har över övergripande ansvaret för arbetet med dataskyddsförordningen.

Inom förvaltningen får personalen löpande information vid eventuella förändringar i arbetssätt kopplat till GDPR av både dataskyddsombud och förvaltningschef. Personalen uppges däremot inte ha tagit del av några ytterligare utbildningar utöver den utbildning som genomfördes i samband med införandet av dataskyddsförordningen.

Uppföljning och återrapportering av arbetet med GDPR till nämnden sker enligt uppgift en gång per år vid slutet av året. Nämnden informerades senast om arbetet med handlingsplanen och den tillhörande checklistan vid sammanträdet den 12 november 2020[8].

[6] UN 2020-03-18 § 30
[7] 2020-02-27 § 4
[8] TN 2020-11-12

3.1.1 Bedömning

Vi konstaterar att kommunen, i varje fall enligt checklistan, inte har fullgjort arbetet med att införa GDPR-lagstiftningen.

Vi delar bedömningen att efter införandet behöver arbetet övergå i en ”förvaltningsfas” med ett löpande arbete. Det arbetet kan dock inte fullt ut påbörjas förrän införandet är klart. Vi anser därför att det är viktigt att en statusuppdatering om vad som återstår för att uppfylla lagens krav inhämtas innan den nya checklistan för förvaltningsfasen upprättas. Även om benämningar inte är det mest väsentliga betraktar vi ändå det som kommunen benämner som ”checklista för det löpande arbetet” mer ska utformas som en rutinbeskrivning för att tydliggöra att det är ett arbete som ska genomföras kontinuerligt.

Vi konstaterar att personalen har tagit del av både interna och externa utbildningar samt att de informeras om förändrade arbetssätt kopplat till GDPR vid arbetsplatsträffar vilket vi ser positivt på. Vi uppfattar däremot att det finns ett fortsatt utbildningsbehov och vi rekommenderar därför styrelse och nämnder att regelbundet följa upp och säkerställa att personalen har tillräckligt med kunskap och att nya arbetssätt anpassat för GDPR tillämpas.

I övrigt bedömer vi att kommunens rutiner och instruktioner för bl.a. personuppgiftsbehandlingar och registerutdrag av personuppgifter i övrigt är ändamålsenliga. Vi anser dock att det är viktigt att styrelse och nämnder regelbundet följer upp att de är aktuella och dess efterlevnad.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att ett antal åtgärder har vidtagits men att det finns utrymme för ytterligare förbättringar. Vi konstaterar att en ny checklista anpassad för det löpande arbetet med GDPR håller på att utformas. Vi vill betona vikten av att checklistan fortsättningsvis bör vara en del av rutinbeskrivningen för det arbete som ska genomföras kontinuerligt. Vi anser vidare att det är väsentligt att planen regelbundet följs upp och rapporteras för att minimera risken att dataskyddsförordningen inte efterlevs.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen och granskade nämnder:

att inhämta en statusuppdatering där det tydligt framgår vad som återstår för att uppfylla lagens krav samt säkerställa att de kvarstående uppgifterna/aktiviteterna enligt handlingsplanen tilldelas en ansvarig och slutförs

att tydliggöra att arbetet med den nya checklistan för att arbetet med dataskyddsordningen ska betraktas som löpande och som regelbundet ska följas upp samt rapporteras

att regelbundet följa upp och säkerställa att personalen har tillräckligt med kunskap och att nya arbetssätt anpassat för GDPR tillämpas

att regelbundet följa upp och säkerställa att rutiner och instruktioner är aktuella och efterlevs

Datum som ovan

KPMG AB

Lena Medin
Certifierad kommunal revisor

Klara Engström
Kommunal revisor