Granskning av kommunens hantering av offentlighets-principen och personuppgifter 2018

KOMMUNREVISIONEN

NORRKÖPING

NORRKÖPING

Kommunrevisorerna

REVISIONSSKRIVELSE 1(1)

2019-01-24

KR-2018/0045

Kommunstyrelsen
Utbildningsnämnden
Byggnads- och miljöskyddsnämnden
Vård- och omsorgsnämnden
Överförmyndarnämnden

Granskning av offentlighetsprincipen och personuppgifter

Kommunrevisionen har genomfört en granskning av kommunstyrelsens och nämndernas hantering av offentlighetsprincip och personuppgifter. Det övergripande syftet med granskningen är att översiktligt bedöma om styrelsen och de aktuella nämndernas hantering av offentlighetsprincip och personuppgifter är tillräcklig.

Den sammantagna bedömningen är att offentlighetsprincipen i många delar fungerar väl, men att de rutiner och riktlinjer som finns behöver uppdateras. Anpassningen till den nya dataskyddsförordningen har gått långsamt och mycket återstår. Det är allvarligt att bilder och bloggar exponerar personuppgifter inom utbildningsnämndens område, det behöver omedelbart åtgärdas.

Med anledning av rapporten vill vi ha ett skriftligt svar på följande:

- Hur ser kommunstyrelsen på en revidering av de centrala riktlinjerna för dokument- och ärendehantering samt e-posthantering i kommunen?
- Hur ser kommunstyrelsen på behovet av en centralt dokumenterad beskrivning avseende ansvarsfördelning och befogenheter för hantering av personuppgifter?
- Hur kommer kommunstyrelse och de granskade nämnderna arbeta för att säkerställa en tillräcklig internkontroll över personuppgifter?
- Vi önskar utbildningsnämndens återkoppling på vidtagna åtgärder kopplade till bloggtjänsterna.

Vi vill ha kommunstyrelsens och nämndernas skriftliga svar senast den 22 mars 2019.

KOMMUNREVISIONEN
2019-01-24

Tommy Svensson
Ordförande kommunrevisionen

Eva Andersson
Vice ordförande kommunrevisionen

Postadress
Norrköpings kommun
Kommunrevisionen
601 81 Norrköping

Besöksadress
Dalsgatan 14

Telefon
011-15 17 99

Telefax
011-15 17 90

E-post
revisionskontoret@norrkoping.se
Internet
www.norrkoping.se/revision

Granskning av hanteringen av offentlighetsprincipen och personuppgifter

Revisionsrapport

Norrköpings kommuns revisorer

KPMG AB

2019-01-30

Antal sidor 18

Innehållsförteckning

1 Sammanfattning och samlad revisionell bedömning

KPMG har av Norrköpings kommuns revisionskontor fått i uppdrag att granska nämndernas och styrelsens efterlevnad av offentlighetsprincipen samt hanteringen av personuppgifter.

Sammanfattningsvis kan konstateras att det finns ett behov av ett förbättrings- och utvecklingsarbete vad avser båda granskningsområdena. Vi anser dock att efterlevnad av offentlighetsprincipen ligger på en tillfredställande nivå.

Vad avser styrdokument, den praktiska implementeringen samt efterlevnad av dataskyddsförordningen kvarstår en del, där nämnderna uttrycker att det är nu de har insett omfattningen och bredden av den nya lagstiftningen. Vi rekommenderar att en fördjupad granskning genomförs under senare delen av 2019 med sikte på efterlevnaden av dataskyddsförordningen.

Vi anser vidare att det finns ett behov av riktade utbildningsinsatser för granskade nämnder, dvs. ej ”massutbildningar på övergripande nivå”, utan insatser som riktar sig till respektive verksamhet. Området ”rättsliga grunder” inom ramen för dataskydds-förordningen är bl.a. av vikt för verksamheterna.

Utifrån våra iakttagelser samt vår analys bedömer vi att följande punkter bör ses över:

Bedömningen avser: kommunstyrelsen, utbildningsnämnden, överförmyndarnämnden, byggnads- och miljöskyddsnämnden samt vård- och omsorgsnämnden.

Offentlighetsprincipen

- kommunstyrelsen bör snarast revidera riktlinjerna för dokument- och ärendehantering samt e-posthantering. Styrdokumenten hänvisar bl.a. till lagstiftning som har upphävts samt dokument- och ärendehanteringssystem som inte används i kommunen sedan år 2012. Likaså bör dokumenten kompletteras med tydliga rutiner avseende registrering. Dokumenten kan med fördel slås samman till ett enda styrdokument. Detta i syfte att minimera antalet styrdokument samt underlätta för medarbetarna.
- Samtliga granskade nämnders dokumenthanteringsplaner är daterade, där planerna har fastställts mellan åren 2006-2015. Vi anser att dokument-hanteringsplaner bör genomgå en översyn årligen.
- Gallring av allmänna handlingar bör ske systematiskt. Det finns idag en eftersläpning i gallringsarbetet.
- Det finns en vaksamhet och medvetenhet bland personalen vad gäller efterlevnad av lagstiftningen avseende hantering av allmänna handlingar. Dock saknas ett dokumenterat internkontrollarbete och därmed är den interna kontrollen ej tillfredställande avseende hantering av allmänna handlingar. Hantering av allmänna handlingar är en återkommande risk. Vi rekommenderar

att ett kontrollmål avseende efterlevnad av offentlighetsprincipen tillförs de årliga internkontrollplanerna.

Personuppgifter

- Kommunstyrelsen bör utveckla samt komplettera stöddokumentet för hantering av personuppgifter. Fastställelsedatum samt beslutsinstans bör framgå av dokumentet, bl.a. i syfte att kunna bedöma styrdokumentets aktualitet.

- Nämnderna bör prioritera arbetet med att ta fram nämndsanpassade rutiner vad gäller efterlevnad av dataskyddsförordningen.

- Nämnderna bör arbeta fram interna dokument som fastställer ansvarsfördelning och befogenheter avseende hantering av personuppgifter. Detta i syfte att skapa en tydlig ansvarsstruktur i organisationen på tjänstemannanivå, ökad rättssäkerhet och effektivitet samt underlätta ett ansvarstagande och ett ansvarsutkrävande.

- De politiska nämnderna har det yttersta ansvaret i egenskap av personuppgiftsansvariga och bör vara engagerade i huruvida kontoren hanterar personuppgifter på ett korrekt sätt. Detta ställer krav på att nämndsledamöter och ersättare är aktiva och efterfrågar information om kontorens arbete med implementering och efterlevnad av dataskyddsförordningen.

- Det finns brister gällande efterlevnaden av rutinerna för personuppgifts incidenter. Kommunstyrelsen bör inom ramen för sin uppsiktsplikt tillse att samtliga nämnder har kännedom om befintlig rutin samt att rutinen efterlevs. Nämnderna har i sin tur ett ansvar för att säkerställa efterlevnaden av fastställda rutiner.

- Blanketten för incidentrapportering bör tillföras en ruta, där ansvarig nämnd framgår. Denna information är av vikt då det är nämnderna som är personuppgiftsansvariga.

- Uppföljningen och kontrollen av hantering av personuppgifter behöver säkerställas, där tydliga styrdokument och interna rutiner bör arbetas fram och integreras i det dagliga arbetet i syfte att kunna säkerställa en fullgod uppföljning och kontroll.

- Hantering av personuppgifter utifrån dataskyddsförordningen är och kommer att vara en viktig del i verksamheterna. Utifrån befintliga risker rekommenderar vi att olika kontrollmål med sikte på efterlevnad av dataskyddsförordningen tillförs de kommande årliga internkontrollplanerna. Detta gäller samtliga granskade nämnder exklusive överförmyndarnämnden.

- Dagens registerförteckningar avseende behandling av personuppgifter bör ses över, där efterfrågad information i enlighet med artikel 30.1 i dataskydds-förordningen ska framgå.

- Kommunstyrelsen bör genomföra en uppföljning om huruvida framkomna påpekanden från en extern utredning avseende kommunens dokument- och ärendehanteringssystem Public 360 har åtgärdats både på central och nämndsnivå.

- Samtliga inköp av IT-verktyg och IT-tjänster ska göras mot bakgrund av gällande lagstiftning vad gäller hantering av personuppgifter, där efterlevnad av dataskyddsförordningen måste garanteras. Härigenom bör risk- och konsekvensbedömningar genomföras inför varje beslut i syfte att bl.a. sondera huruvida verktyget/tjänsten uppfyller befintliga lagkrav.

- Utbildningsnämnden bör snarast åtgärda framkomna brister, där bloggarna inte ska vara öppna för allmänheten. Dagens hantering av bloggar strider mot dataskyddsförordningen. Likaså bör registerförteckningar upprättas i enlighet med artikel 30.1, dataskyddsförordningen.

- Det bör säkerställas att det finns gällande samt korrekta personuppgifts-biträdesavtal med aktuella leverantörer inom ramen för bloggtjänster i de fall där underleverantörer förekommer.

2 Inledning

2.1 Bakgrund

KPMG har av Norrköpings kommuns revisionskontor fått i uppdrag att genomföra en förstudie avseende nämndernas och styrelsens hantering av offentlighetsprincipen och personuppgifter. Denna granskning är ett komplement till den grundläggande granskningen.

Offentlighetsprincipen är en central del i den svenska rättsordningen. Det innebär att allmänheten har rätt till insyn och tillgång till information om statens och kommunernas verksamheter. För den demokratiska processen är det bl.a. betydelsefullt att det finns fungerande system, rutiner och riktlinjer för hanteringen av allmänna handlingar.

Den 25 maj 2018 trädde dataskyddsförordningen, (GDPR), i kraft och ersatte Personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för dataskydds-förordningen. Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter till skillnad från tidigare lagstiftning.

2.2 Syfte och revisionsfrågor

Den översiktliga revisionsfrågan är om styrelsens och nämndernas hantering av offentlighetsprincip och personuppgifter är tillräcklig.

I granskningen besvaras följande revisionsfrågor och delfrågor:

- Är kommunstyrelsens och nämndernas hantering av offentlighetsprincipen i enlighet med lag och riktlinjer?

  1. Finns ändamålsenliga riktlinjer avseende allmänna handlingars hantering?
  2. Tillämpas de riktlinjer som reglerar allmänna handlingars hantering?
  3. Har berörda medarbetare fått tillräckliga förutsättningar för att hantera allmänna handlingar?
  4. Är den interna kontrollen tillfredsställande avseende allmänna handlingars hantering?

- Är kommunstyrelsens och nämndernas hantering av personuppgifter i enlighet med lag och riktlinjer?

  1. Finns riktlinjer för hur verksamheten ska gå till väga vid behandling av personuppgifter?

2. Finns centralt dokumenterade systembeskrivningar som tydliggör ansvarsfördelning och befogenheter för hantering av personuppgifter?
3. Finns ett uppföljningssystem som säkerställer att styrelsen och nämnden får information om eventuella brister i hanteringen?
4. Har styrelsen och nämnden säkerställt en tillräcklig uppföljning och kontroll av hanteringen inom sina respektive verksamhetsområden?

2.3 Revisionskriterier

Vi har bedömt om rutinerna/verksamheten uppfyller:

- Tryckfrihetsförordningen, (SFS 1949:105)
- Offentlighets- och sekretesslagen, (SFS 2009:400)
- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
- Interna regelverk, policys och riktlinjer

2.4 Avgränsningar

Förstudien avser kommunstyrelsen, utbildningsnämnden, överförmyndarnämnden, byggnads- och miljöskyddsnämnden samt vård- och omsorgsnämnden.

2.5 Metod

Förstudien har genomförts genom dokumentstudier och intervjuer.

Intervjuer har genomförts med berörda nämnders ordförande/1:e vice ordförande, sakkunniga, nämndssekreterare, registratorer och kontorsledningar i egenkap av kontorschef/stabschef/administrativ chef/kanslichef. Intervjuer och avstämningar har också genomförts med kommunens dataskyddsombud.

Kommunstyrelsen ordförande närvarade ej vid intervjutillfället.

Rapporten har faktagranskats av intervjuade verksamhetsansvariga samt dataskydds-ombudet.

Analys och bedömningar avser samtliga granskade nämnder i de fall där en specifik nämnd inte anges.

2.6 Prövning av oberoende och integritet

Sakkunniga har i enlighet med Skyrevs, (Sveriges kommunala yrkesrevisorer), rekommendation nummer två prövat sitt oberoende.

2.7 Kvalitetssäkring

Rapporten är även kvalitetssäkrad enligt Skyrevs regler vid revisionskontoret.

3 Nationell lagstiftning

Offentlighetsprincipen är en central del i den svenska rättsordningen. Det innebär att allmänheten har rätt till insyn och tillgång till information om statens och kommunernas verksamheter. För den demokratiska processen är det bl.a. betydelsefullt att det finns fungerande system, rutiner och riktlinjer för hanteringen av allmänna handlingar.

Rätten till insyn framgår av *tryckfrihetsförordningens 2 kap, 1 §* enligt följande:

”Till främjande av ett fritt meningsutbyte och en allsidig upplysning skall varje svensk medborgare ha rätt att ta del av allmänna handlingar.”

Med handling avses i tryckfrihetsförordningen en framställning i skrift eller bild samt en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med hjälp av tekniskt hjälpmedel, (TF, 2 kap 3 §).

Enligt tryckfrihetsförordningen krävs följande uppfyllda kriterier för att en handling ska anses som allmän. Dels ska handlingen **förvaras** hos myndigheten, dels ska den vara **inkommen** till eller **upprättad** hos myndigheten, (TF 2 kap. 6-7 §).

4 Offentlighetsprincipen

4.1 Finns ändamålsenliga riktlinjer avseende allmänna handlingars hantering?

Iakttagelser

Vi har delgivits följande centrala styrdokument avseende hantering av allmänna handlingar:

- Riktlinjer för dokument- och ärendehantering i Norrköpings kommun, antagen av kommundirektören 2000-12-01 och senast reviderad 2006-09-28.
- Riktlinjer för e-posthantering i Norrköpings kommun, fastställd av kommunstyrelsen 2011-05-09, § 146 och senast reviderad 2017-05-02, § 259.
- Arkivhandbok, antagen av stadsarkivarien 2018-08-28

Vi har också tagit del av samtliga granskade nämnders dokumenthanteringsplaner. En dokumenthanteringsplan redogör för hanteringen av en myndighets handlingar, där registrering, placering, förvaring och gallring av inkomna och upprättade handlingar ska framgå.

Av intervjuerna med professionen framgår att huvudstyrdokumentet ”Riktlinjer avseende dokument- och ärendehantering” samt ”Riktlinjer för e-posthantering” används ej, där uppdaterade styrdokument med fokus på hantering av allmänna handlingar har under en längre period efterfrågats av bl.a. nämndssekreterarnätverket samt nätverket för administrativa chefer i kommunen.

Revisionsbedömning

Vi bedömer att styrdokumentet ”Riktlinjer för dokument- och ärendehantering samt e-posthantering har tappat sin legitimitet och funktion. Styrdokumenten hänvisar bl.a. till lagstiftning som har upphävts samt dokument- och ärendehanteringssystem som inte används i kommunen sedan år 2012. Vidare bör styrdokumentet för dokument- och ärendehantering kompletteras med tydliga rutiner och exempel avseende vilka handlingar som ska registreras respektive gallras vid ankomst. I avsaknad av tydliga samt konkreta rutiner för registrering har nämnderna skapat egna ”hemsnickrade” varianter.

Ett av syftena med en myndighets registrering av allmänna handlingar är att underlätta för medborgarna att tillämpa offentlighetsprincipen. Även om grunderna för registrering regleras i lagstiftningen, är det till stor del myndighetens eget ansvar att skapa rutiner.

Rutiner som uppfyller lagens krav, som är väl förankrade i verksamheten och som alla inom myndigheten känner till, skapar förutsättningar för en funktionell och effektiv hantering av allmänna handlingar.

I samband med intervjuerna efterfrågar nämnderna ett centralt samt användarvänligt styrdokument avseende dokument- och ärendehantering som verksamheterna kan ha nytta av.

Vi bedömer att kommunstyrelsen snarast bör revidera riktlinjerna för dokument- och ärendehantering samt e-posthantering. Likaså bör dokumenten kompletteras med tydliga rutiner avseende registrering. Dokumenten kan med fördel slås samman till ett enda styrdokument. Detta i syfte att minimera antalet styrdokument samt underlätta för medarbetarna.

Dokumenthanteringsplanernas aktualitet utgör en viktig del för återsökning av handlingar. Samtliga granskade nämnders centrala dokumenthanteringsplaner är daterade, där planerna har fastställts mellan åren 2006-2015. Vi anser att en översyn av dokumenthanteringsplanerna bör ske årligen i syfte att sondera behovet av en uppdatering.

Det finns en medvenhet bland kontorssledningarna avseende ”åldrande” dokumenthanteringsplaner. Likaså medges att det finns en eftersläpning av

gallringsarbetet pga. bristande resurser.

4.2 Tillämpas de riktlinjer som reglerar allmänna handlingars hantering?

Iakttagelser

Som tidigare nämnts har riktlinjerna förlorat sin legitimitet och funktion i verksamheterna. Det finns dock en tydlig medvetenhet bland berörd personal avseende den lagstiftning som reglerar allmänna handlingars hantering.

Vi har också genomfört stickprovskontroller, där slumpvis utvalda ärenden har begärts ut. Begäran har genomförts utan någon synlig koppling till revisionskontoret eller anlitad revisionsbyrå. Detta i syfte att möjliggöra att utlämningsprocessen kan ske på objektiva grunder.

Vi har bedömt huruvida gällande lagstiftning efterlevs vad gäller tidsperspektiv, saklighet och efterforskningsförbud.

Nedan presenteras resultatet av kontrollerna:

Ansvarig nämnd	Antal begärda ärenden	Svarstid	Mottagnings-bekräftelse	Efterlevnad av efterforsknings förbud	Bedömning
Utbildningsnämnden	3	1 dag	Ja	Ja	- Sakligt - Välordnade handlingar
Vård och omsorgsnämnden	3	30 minuter	Ja	Ja	- Sakligt - Välordnade handlingar
Kommunstyrelsen	3	1-6 timmar	Ja	Ja	- Svar från 3 olika registratorer - Sakligt - Välordnade handlingar
Byggnads- och miljöskyddsnämnden	3	4 timmar	Ja	Ja	- Sakligt - Välordnade handlingar

Överförmyndarnämnden har ej inkluderats i undersökningen då det är en särskild verksamhet där handlingar inom ramen för föräldrabalken omfattas av sekretess.

Revisionsbedömning

Vi anser att efterlevnad av gällande lagstiftning är på en tillfredställande nivå utifrån vad som har framkommit vid tid för granskningen.

4.3 Har berörda medarbetare fått tillräckliga förutsättningar för att hantera allmänna handlingar?

Iakttagelser

Av intervjuerna med berörd personal framgår att det finns kontinuerliga kommungemensamma utbildningar vad gäller bl.a. offentlighetsprincipen och offentlighets- och sekretesslagen.

Samtlig berörd personal har genomgått en grundutbildning vad gäller hantering av allmänna handlingar. Kompetensutveckling sker via nätverksträffar.

Gruppen registratorer och nämndssekreterare uttrycker att det vidare finns möjligheter att delta vid externa utbildningstillfällen vid behov.

Vid mer komplexa fall vad gäller exempelvis sekretessbedömning kan vid förekommande fall kontorens jurist konsulteras. Det sker även samråd med kommunjuristen vid behov.

Revisionsbedömning

Vi bedömer att berörda medarbetare har fått tillräckliga förutsättningar för att hantera allmänna handlingar.

4.4 Är den interna kontrollen tillfredsställande avseende allmänna handlingars hantering?

Iakttagelser

Som tidigare nämnts finns en tydlig medvetenhet kring hanteringen av allmänna handlingar.

Vi har begärt in granskade nämnders interna kontrollplaner för de senaste tre åren i syfte att sondera huruvida konkreta kontroller har genomförts vad avser efterlevnad av offentlighetsprincipen.

Av genomgångna internkontrollplaner för åren 2016, 2017 och 2018 för samtliga granskade nämnder framgår en avsaknad av kontrollmål med sikte på hantering av allmänna handlingar.

Revisionsbedömning

Vi bedömer att det finns en vaksamhet och medvetenhet bland personalen vad gäller efterlevnad av lagstiftningen avseende hantering av allmänna hantering. Dock saknas ett dokumenterat internkontrollarbete och därmed är den interna kontrollen ej tillfredställande avseende hantering av allmänna handlingar.

Intern kontroll syftar bl.a. till att säkerställa **efterlevnad av lagar, föreskrifter och riktlinjer** samt undvika uppkomsten av **allvarliga fel, brister** och **förtroendeskador**.

Ett underbyggt internkontrollarbete har sin grund i systematiska risk- och väsentlighets-bedömningar som bör genomföras årligen. Vi anser att hantering av allmänna handlingar är en återkommande risk, där vi rekommenderar att ett kontrollmål tillförs de årliga internkontrollplanerna.

Denna ”egenkontroll” leder till minimering av befintliga och sannolika risker vad gäller hantering av allmänna handlingar.

5 EU-rättslig lagstiftning

Nedan följer en kortfattad beskrivning av den nya lagstiftningen som sedan den 25 maj 2018 är gällande ramverk för behandling av personuppgifter. I och med ikraft-trädandet av dataskyddsförordningen, (GDPR), upphävdes personuppgifts- lagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina person- uppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för Dataskydds- förordningen. Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter till skillnad från tidigare lagstiftning.

Hantering av personuppgifter ska ske utifrån förordningens grundläggande principer enligt följande:

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet

- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Det är av stor vikt att kommunmedborgarna, anställda och övriga som kommer i kontakt med kommunen upplever att personuppgifter hanteras utifrån ovan nämnda principer.

Vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”**rättslig grund**”. Utan en rättslig grund är personuppgiftsbehandling ej laglig.

Vidare ska nämnderna utse ett dataskyddsombud, (DSO), som bl.a. har till uppgift att övervaka efterlevnaden av dataskyddsförordningen. I detta arbete ingår att samla in information om samt granska hur verksamheterna behandlar personuppgifter.

6 Hantering av personuppgifter

6.1 Finns riktlinjer för hur verksamheten ska gå till väga vid behandling av personuppgifter?

Iakttagelser

Vi har delgivits ett styrdokument i form av ”stöd för hantering av personuppgifter” framtaget av kommunstyrelsens kansli. Dock saknas fastställelsedatum och beslutsinstans.

Vi har vidare tagit del av en projektplan, daterad 2018-04-11, avseende kartläggning inför implementering av dataskyddsförordningen. Projektplanen fastställer bl.a. att det ska genomföras en nulägesanlys följt av en GAP-analys som resulterar i en åtgärdsplan samt en skriftlig rapport.

Av granskningen framkommer att en nulägesanalys har genomförts, dock finns inget underlag avseende GAP-analys och åtgärdsplan.

Nämnderna har vidare utsett ett dataskyddsombud som tillträdde under juni 2018 och som bl.a. har till uppgift att övervaka efterlevnaden av dataskyddsförordningen samt interna föreskrifter och rutiner.

Bör noteras att samtliga nämnder uttrycker att implementeringen av dataskydds-förordningen är ett omfattande och tidskrävande arbete, där kontorssledningarna medger att verksamheterna inte har hunnit fullt ut med implementeringen och att stora delar kvarstår. En återkommande fundering som de intervjuade lyfter är: ”*Det är en oerhörd omfattande lagstiftning, där vi inte riktigt vet var man ska börja.”*

Av intervjuerna framgår att nämnderna under 2019 ska arbeta fram interna rutiner för behandling av personuppgifter. Likaså uttrycker kontorsledningarna att specifika rutiner

för hantering av ”**begäran om registerutdrag**” samt ”**personuppgifts- incidenter**” kommer att arbetas fram.

Revisionsbedömning

Vi bedömer att kommunstyrelsen bör utveckla samt komplettera stöddokumentet för hantering av personuppgifter. Fastställelsedatum samt beslutsinstans bör framgå av dokumentet, bl.a. i syfte att kunna bedöma styrdokumentets aktualitet. Av intervju med kanslichefen inom kommunledningskontoret samt dataskyddsombudet framgår en medvetenhet kring behovet av utvecklig av befintligt styrdokument.

Vi bedömer vidare att nämnderna bör prioritera arbetet med att ta fram nämnds-anpassade rutiner vad gäller efterlevnad av dataskyddsförordningen. Vi anser att rutinerna borde ha arbetats fram vid ett tidigare skede.

Vi anser att en GAP-analys följt av en åtgärdsplan i enlighet med fastställd projektplan skulle ha underlättat arbetet med att ta fram stöddokument samt bidragit till att säkerställa efterlevnaden av dataskyddsförordningen.

6.2 Finns centralt dokumenterade systembeskrivningar som tydliggör ansvarsfördelning och befogenheter för hantering av personuppgifter?

Iakttagelser

Vid tid för granskningen finns inte någon centralt dokumenterad beskrivning avseende ansvarsfördelning och befogenheter för hantering av personuppgifter.

Revisionsbedömning

Vi bedömer att det är av ännu större vikt att nämnderna arbetar fram interna dokument som fastställer ansvarsfördelning och befogenheter avseende hantering av person-uppgifter. Detta i syfte att skapa en tydlig ansvarsstruktur i organisationen på tjänstemannanivå, ökad rättssäkerhet och effektivitet samt underlätta ett ansvars-tagande och ett ansvarsutkrävande.

Bör också noteras att de politiska nämnderna har det yttersta ansvaret i egenskap av personuppgiftsansvariga och bör vara engagerade i huruvida kontoren hanterar personuppgifter på ett korrekt sätt. Detta ställer krav på att nämndsledamöter och ersättare är aktiva och efterfrågar information om kontorens arbete med implementering och efterlevnad av dataskyddsförordningen.

6.3 Finns ett uppföljningssystem som säkerställer att styrelsen och nämnden får information om eventuella brister i hanteringen?

Iakttagelser

Det finns idag skriftliga rutiner framtagna av kommunstyrelsen vad gäller hantering av så kallade ”personuppgiftsincidenter”. Av rutinen framgår tydliga instruktioner avseende en eventuell bristande hantering av personuppgifter. Rutinen fastställer vidare att varje personuppgiftsincident ska dokumenteras av berörd chef samt anmälas till nämnden. Likaså ska samtliga incidenter rapporteras till dataskyddsombudet.

Vi har också tagit del av aktuell blankett avseende incidentrapportering.

Personuppgiftsincidenter som kommer att medföra en risk för de registrerade måste rapporteras till Datainspektionen. Inrapportering ska ske inom 72 timmar efter det att överträdelsen har upptäckts. Den registrerade ska informeras omedelbart.

Enligt intervju med dataskyddsombudet har vissa incidenter nått vederbörande genom slump, där aktuella verksamheter inte har haft kännedom om vad som karaktäriserar en personuppgiftsincident.

Revisionsbedömning

Vi bedömer att det finns tydliga rutiner avseende eventuella brister i hanteringen av personuppgifter. Det finns dock brister gällande efterlevnaden.

Blanketten för incidentrapportering bör tillföras en ruta, där ansvarig nämnd framgår. Denna information är av vikt då det är nämnderna som är personuppgiftsansvariga.

Kommunstyrelsen bör inom ramen för sin uppsiktsplikt tillse att samtliga nämnder har kännedom om befintlig rutin samt att rutinen efterlevs. Nämnderna har i sin tur ett ansvar för att säkerställa efterlevnaden av fastställda rutinerna.

Det finns vidare ett utbildningsbehov gällande olika delar inom ramen för data-skyddsförordningen. Enligt intervju med dataskyddsombudet planeras riktade utbildnings- och informationsinsatser om bl.a. hantering av personuppgiftsincidenter.

6.4 Har styrelsen och nämnden säkerställt en tillräcklig uppföljning och kontroll av hanteringen inom sina respektive verksamhets-områden?

Iakttagelser

Av intervjuerna med profession och politik framgår att arbetet med att säkerställa en

tillräcklig uppföljning och kontroll pågår, där en hel del kvarstår.

Som tidigare nämnts har dataskyddsombudet bl.a. till uppgift att övervaka efterlevnaden av hantering av personuppgifter. Detta arbete kommer att påbörjas under 2019. Under första kvartalet kommer dataskyddsombudet att genomföra en första granskning av s.k. ”**registerförteckningar**”. Enligt dataskyddsförordningen *artikel 30.1* ska personuppgiftsansvariga organisationer föra ett register över personuppgiftsbehandlingar, där följande ska framgå:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
b) Ändamålen med behandlingen.
c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.
d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.
f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

Granskningen visar att det finns brister i dagens registerförteckningar, vilket också bekräftas av dataskyddsombudet. Granskningen kommer att genomföras mot bakgrund av dataskyddsförordningens grundläggande principer:

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet

Ytterligare insatser i att säkerställa uppföljning och kontroll är inrättning av befattningar som ”informationssamordnare”. Under våren 2019 kommer nämnderna att på uppdrag av kommunstyrelsen utse s.k. ”informationssamordnare”.

Informationssamordnaren ska vara kontaktperson inom och utom organisationen för frågor om:

- informationssäkerhet
- behandling av personuppgifter
- arkiv- och dokumenthantering
- säkerhet för skyddsvärd information.

Revisionsbedömning

Vi bedömer att uppföljningen och kontrollen inte är fullt tillräcklig vid tid för granskningen, där det bör beaktas att nämnderna är i startskedet vad gäller arbetet med att implementera dataskyddsförordningen. Vidare behöver styrdokument och interna rutiner arbetas fram och integreras i det dagliga arbetet i syfte att kunna säkerställa en fullgod uppföljning och kontroll.

Vi bedömer att internkontrollarbetet är ett viktigt verktyg i att kunna följa upp samt upptäcka eventuella risker i samband med hantering av personuppgifter. Härigenom rekommenderar vi att de kommande årliga internkontrollplanerna tillförs olika kontrollmål med sikte på efterlevnad av dataskyddsförordningen.

Av de granskade nämnderna är överförmyndarnämnden den verksamhet som har i inför 2019-års internkontrollplan inkluderat kontrollmål som berör efterlevnad av dataskyddsförordningen.

7 Övriga delar av vikt utanför ramen för revisionsfrågorna

7.1 Dokument- och ärendehanteringssystem

Iakttagelser

Under juni 2018 har en översyn av kommunens dokument- och ärendehanterings-system Public 360 genomförts. Översynen har utförts av extern konsult. Rapporten lyfter viktiga delar som behöver anpassas mot bakgrund av dataskyddsförordningen.

Av intervjuerna med professionen framgår exempelvis att Public 360 hänvisar till tidigare personuppgiftslagstiftning som har upphävts.

Av intervjuerna med kommunledningskontoret framgår att digitaliseringsavdelningen hanterar inköp av IT-verktyg och IT-tjänster i samråd med berörd beställare.

Revisionsbedömning

Vi anser att kommunstyrelsen utifrån sin centrala samordningsroll bör genomföra en uppföljning om huruvida framkomna påpekanden har åtgärdats vad gäller Public 360.

Granskade nämnder har i sin tur ett ansvar för att säkerställa att framkomna påpekanden har åtgärdats.

Vidare ska samtliga inköp av IT-verktyg och IT-tjänster göras mot bakgrund av gällande lagstiftningen vad gäller hantering av personuppgifter, där efterlevnad av dataskyddsförordningen måste garanteras. Härigenom bör risk- och konsekvens-bedömningar genomföra inför varje beslut i syfte att bl.a. sondera huruvida verktyget/tjänsten uppfyller befintliga lagkrav.

7.2 Bloggar

Iakttagelser

Av intervju med dataskyddsombudet framgår att Norrköpings kommuns skolor använder sig av publika bloggar för att förmedla information till vårdnadshavare, där hanteringen strider mot dataskyddsförordningen. Enligt uppgift förekommer person-uppgifter och bilder på elever samt känsliga uppgifter som exempelvis berör hälsotillstånd.

Bristerna avseende hantering av personuppgifter har kommunicerats med utbildningskontoret, där ett förslag har varit att stänga befintliga bloggar, radera samtliga känsliga personuppgifter och därefter lösenordskydda bloggarna, där endast den enskilda skolklassens elever och vårdnadshavare har tillgång till aktuell blogg. Likaså bör information om tidigare terminer raderas.

Vi har tagit del av en rutin för användande av webb och sociala medier inom utbildningskontorets verksamheter, fastställd av utbildningsdirektören 2018-06-12.

Vid avstämning med dataskyddsombudet framgår att fastställd rutin inte efterlevs, där det fortfarande förekommer personuppgifter i olika former. Likaså efterlevs inte gallringsbestämmelserna.

Dataskyddsombudet har uppmärksammat att det finns brister i befintliga samtyckesblanketter till vårdnadshavare. Vad gäller samtyckesunderlag bör det specificeras för varje ändamål, dvs. i enlighet med principerna om ändamåls-begränsning. Ytterligare juridisk princip som ska beaktas är uppgiftsminimering. Likaså ska publiceringsplattformen redogöras i samtyckesblanketten samt om huruvida personuppgifterna kommer att överföras till tredje land.

Vid avstämning med kontorschefen framgår att bloggarna fortfarande är oskyddade och att upphandling av ett nytt elevdokumentationssystem pågår där krav avseende en blogg samt kommunikationsmodul med vårdnadshavarna har specificerats.

Revisionsbedömning

Dagens hantering av bloggar strider mot dataskyddsförordningen. Vi bedömer att utbildningsnämnden snarast ska åtgärda framkomna brister, där bloggarna inte ska vara öppna för allmänheten.

Likaså bör registerförteckningar upprättas, där bl.a. följande ska framgå:

- ändamål med personuppgifts behandling
- omfattning, typ av personuppgifter
- rättslig grund
- tidsfrist för radering
- tekniska och organisatoriska säkerhetsåtgärder
- uppgifter om eventuell personuppgistbiträde

Vidare ska det även säkerställas att det finns gällande samt korrekta personuppgifts-biträdesavtal med aktuella leverantörer inom ramen för bloggtjänster i de fall där underleverantörer förekommer.

2019-01-30

KPMG AB

Viktoria Bernstam
Specialist
Revisor

Magnus Larsson
Kundansvarig