Granskning av rutiner för efterlevnad av dataskyddsförordningen

Revisionsrapport
Huddinge kommun

KPMG AB

2022-01-17

Antal sidor 22

© 2021 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Huddinge kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2022-01-11

Innehållsförteckning

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

1 Sammanfattning, slutsats och rekommendationer

Vi har av Huddinge kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen. Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter.

Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter till skillnad från tidigare lagstiftning. En bristande hantering av personuppgifter riskerar också leda till förtroendeskador för kommunen som helhet samt personuppgifts-ansvariga nämnder och styrelser.

Utifrån ett tydligt behov av stödjande insatser har rapporten utformats på ett vägledande sätt för att bistå kommunstyrelsen i arbetet framåt.

Sammanfattningsvis kan konstateras att det finns brister vad avser efterlevnaden av dataskyddsförordningen. Vi bedömer att det finns ett behov av en central styrning från kommunstyrelsens sida vad avser nämndernas arbete med att uppfylla lagen. Bör noteras att det har passerat ca 3,5 år sedan lagens ikraftträdande, där det är hög tid att efterlevnaden ligger på en rimlig nivå.

Av granskningen framgår att det råder en låg kunskapsnivå i organisationen, där det finns behov av avgränsade och områdesspecifika utbildningsinsatser till samtliga nämnder.

Vi upplever intervjuad politik och tjänstepersoner som engagerade och bedömer det som positivt att kommunstyrelsen och kommunstyrelseförvaltningen har varit lyhörda för genomförd granskning och har ambitioner att efter delgivning av revisions-rapporten påbörja ett förbättringsarbete.

Vi vill också betona vikten av ett kontinuerligt internkontrollarbete, där efterlevnad av dataskyddsförordningen bör inkluderas.

Det bör framhållas att det är personuppgiftsansvariga nämnder och styrelser som är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen och ansvarar därmed för verkställandet. Kommunstyrelsens uppsiktplikt ska därmed inte förväxlas med rollen som personuppgiftsansvarig, där kommunstyrelsen inte kan inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse. Dock har kommunstyrelsen ett ansvar för framtagande av centrala kommunövergripande styrdokument och rutiner i syfte att säkerställa en enhetlig hantering inom samtliga nämnder och styrelser samt tillse att det råder en tillfredställande samt homogen kunskapsnivå.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- utöva en central styrning i syfte att öka graden av efterlevnad av dataskydds-lagstiftningen.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

- inom ramen för sin uppsiktsplikt följa upp huruvida verksamheterna efterlever dataskyddsförordningen.

- säkerställa att det finns fastställda samt aktuella kommunövergripande styrdokument och riktlinjer i syfte att uppnå en enhetlig hantering.

- snarast fastställa ett styrdokument för:
  - hantering, dokumentation och anmälan av personuppgiftsincidenter (se avsnitt 3.8 för vägledning).
  - begäran av registerutdrag
  - begäran om radering, rättelse och begränsning

- utöva en central styrning vad avser utbildningsinsatser inom dataskydds-förordningen, då det finns ett behov av att säkerställa en homogen kunskapsnivå inom nämnderna.

- årligen ta del av statistik i likhet med presenterad tabell 3.6.1, avseende inträffade personuppgiftsincidenter inom samtliga nämnder och styrelser, inom ramen för styrelsens uppsiktsplikt.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

2 Inledning

Vi har av Huddinge kommuns revisorer fått i uppdrag att granska vissa av kommunens rutiner för efterlevnad av dataskyddsförordningen.

2.1 Syfte, revisionsfråga och avgränsning

Rapporten syftar till att granska kommunens övergripande rutiner för efterlevnad av dataskyddsförordningen, där följande besvaras:

- Finns det ett centralt utsett dataskyddsombud?
- Befinner sig dataskyddsombudet i en oberoendeposition?
- Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
- Har kommunstyrelsen säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskydds-förordningen?
- Har dataskyddsombudet genomfört kontroller av registerförteckningarna?
- Är registerförteckningarna korrekt upprättade utifrån dataskydds-förordningens grundläggande principer?
- Finns dokumenterade rutiner för hantering av personuppgiftsincidenter?
- Hur många personuppgiftsincidenter har inträffat sedan lagens ikraftträdande?
- Har det genomförts någon riskbedömning av incidenterna och hur många har kategoriserats som allvarliga?
- Har incidenter som bedömts medföra allvarliga risker för den registrerades integritet anmälts till Integritetsskyddsmyndigheten (f.d. Datainspektionen)?
- Finns dokumenterade rutiner för begäran om registerutdrag?
- Finns dokumenterade rutiner för rättelse av uppgifter?
- Finns dokumenterade rutiner för radering av uppgifter?

2.2 Ansvarig nämnd/styrelse

Kommunstyrelsen.

2.3 Revisionskriterier

- 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.
- Riktlinjer från European Data Protection Board, (Europeiska dataskyddsstyrelsen)

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

— Interna riktlinjer/policys.

2.4 Metod

Granskningen har genomförts genom:

— Studium och genomgång av relevanta styrdokument och underlag.

— Granskning av registerförteckningar avseende personuppgiftsbehandlingar.

— Intervjuer och avstämningar med kommunstyrelsens ordförande, biträdande kommunchef, t.f. säkerhetschef samt dataskyddsombud.

Rapporten har faktaavstämts med biträdande kommundirektören och kommunstyrelsens ordförande. Iakttagelseavsnitten baserad på inkommen information från dataskyddsombudet har faktaavstämts med dataskyddsombudet.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

3 Resultat av granskningen

Nedan följer resultatet av granskningen. I ett vägledande syfte samt tydliggörande av de kriterier som vi har granskat mot, föregås avsnitten av sammanfattande beskrivningar av gällande lagstiftning.

3.1 EU-rättslig lagstiftning

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes 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 dataskyddsförordningen.

Bristande hantering samt överträdelser kan innebära betydande **sanktionsavgifter** till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av person-uppgifter leda till **förtroendeskador** för kommunen som helhet samt personuppgifts-ansvariga nämnder och styrelser.

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

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

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

Vidare ska styrelsen och nämnderna utse ett dataskyddsombud, (DSO), som bl.a. har till uppgift att övervaka efterlevnaden av dataskyddsförordningen.

3.2 Dataskyddsombud

Dataskyddsförordningen, artikel 37.1, fastställer att ett dataskyddsombud, (DSO) ska utses i följande tre fall:

a) Behandlingen genomförs av en myndighet eller ett offentligt organ.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

b) Den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning.

c) Den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter och personuppgifter som rör fällande domar i brottmål och överträdelser.

3.3 Dataskyddsombudets oberoende

Dataskyddsombudets främsta uppdrag är att ge råd och informera personuppgifts-ansvariga, personuppgiftsbiträden och anställda om deras skyldigheter samt systematiskt arbeta och övervaka efterlevnaden av dataskyddsförordningen.

Det är av vikt att dataskyddsombudet befinner sig i en **oberoendeposition**, där vederbörande ska kunna fullgöra sina uppgifter på ett oberoende sätt. Detta innebär att personuppgiftsansvariga eller personuppgiftsbiträden exempelvis inte får instruera dataskyddsombudet om hur ett inkommande klagomål ska utredas för att uppnå ett visst resultat eller huruvida tillsynsmyndigheten ska rådfrågas eller ej.

Det är tillåtet att dataskyddsombudet har andra arbetsuppgifter, dock är det av vikt att organisationen tillser att det inte finns några intressekonflikter. Det är bl.a. inte lämpligt att ett dataskyddsombud sitter i organisationens ledning eller är delaktig i att fatta strategiska beslut om kärnverksamheten.

3.3.1 Bedömning

Vi bedömer att utsett dataskyddsombud i Huddinge kommun vid tid för granskningen befinner sig organisatoriskt sett i en oberoendeposition.

3.4 Lägesstatus dataskyddsorganisation, kunskapsnivå, interngranskning mm.

Iakttagelser

Rollen som dataskyddsombud i Huddinge kommun har haft fyra innehavare sedan juni 2018. Nuvarande dataskyddsombud utsågs 2021-02-22 och har en tjänste-omfattning på 100 %. Tjänsten är renodlad och avser endast uppdraget som dataskyddsombud.

Under hösten 2021 har förvaltningarna utsett s.k. GDPR-ansvariga, med undantag för kommunstyrelseförvaltningen.

Av inkommet granskningsunderlag samt intervjuer med dataskyddsombudet framgår att mycket tid har fått ägnas till inventering och att få en överblick samt lägesbild av respektive nämnds arbete, mognad och kunskapsnivå vad avser hantering av personuppgifter.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

Som tidigare nämnts har dataskyddsombudet i uppdrag att övervaka efterlevnaden av dataskyddsförordningen. Dataskyddsombudets arbete, granskningar och resultat ska **dokumenteras** med **tydliga bedömningar och uttalande** om nämnders och styrelser efterlevnadsgrad, brister, risker och utvecklingsområden. Det är av vikt att dataskyddsombudets bedömningar och uttalanden är **oberoende**. Av granskningen kan konstateras att dataskyddsombudet har under hösten genom en omfattande nulägesanalys bedömt nämndernas efterlevnadsgrad och befintliga risker, där det framhålls att det finns flertalet väsentliga luckor och brister vad avser efterlevnaden av dataskyddsförordningen med bl.a. följande sammanfattande bedömningar:

- Mycket låg kunskapsnivå inom samtliga verksamheter i kommunen
- Avsaknad av organisation för incidenthantering
- Bristande integritets- och dataskydd
- Otillräckligt tidsutrymme och kunskapsnivå vad avser utsedda GDPR-ansvariga
- Behov av ytterligare resurser utöver GDPR-ansvariga i form av dataskydds-koordinatorer och dataskyddssamordnare inom respektive förvaltning samt ett centralt utsedd GDPR-strateg.

Utifrån rådande lägesstatus och kunskapsnivå uttrycks att det förebyggande och långsiktiga arbetet får stå tillbaka för mer hands-on-stöd. Vidare pågår ett arbete vad avser framtagande av kommunövergripande styrdokument i form av rutin-beskrivningar för bl.a. hantering av personuppgiftsincidenter och begäran om registerutdrag.

3.3.1 Bedömning

Vi bedömer det positivt att det finns en renodlad heltidstjänst med sikte på uppdraget som dataskyddsombud. Det förekommer ofta i kommunsverige att ett dataskydds-ombud innehar flera funktioner/befattningar, där uppdraget som dataskyddsombud avser endast viss tid av tjänsten, vilket kan försvåra utövandet.

Av granskningen framkommer att det har upprättats en omfattande nulägesanalys i form av en statusrapport av kommunens efterlevnad av dataskyddsförordningen, följt av ett separat dokument i form av övergripande sammanställning av nämndernas lägesstatus. Detta bedöms som positivt, där rapporten återger utvecklingsområden i detalj, utifrån gällande lagstiftning.

En formaliadel som behöver uppdateras i rapporten är att enskilda medarbetare inte kan stå som mottagare av ett kommunövergripande dokument, utan i detta fall är det kommunstyrelsen som är ägare av dokumentet.

Vidare behöver en formell punkt avseende ansvaret klargöras i statusrapporten, där det bör framgå att det är **nämnder och styrelser** som är föremål för granskningar. Av rapporten framgår att ”*revision av förvaltningarna för 2021 är inledd och pågående men att revision av nämnderna för år 2021 har ännu inte påbörjats*”. Denna del bör uppdateras då det är de facto revision av **nämnderna** som har påbörjats, där förvaltningarna inte är självständiga organ, utan tillhör och lyder under respektive nämnd och styrelse. Varje nämnd och styrelse har en förvaltning bestående av medarbetare, där förvaltningarna utför det arbetet som nämnden beslutat om.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

Nämnden i egenskap av politiska ledamöter och ersättare har ingen utförarverksamhet och därmed är revision av förvaltningens arbete detsamma som revision av beslutande nämnd. Viktigt också att betona att det alltid är **ansvarig nämnd/styrelse** i egenskap av personuppgiftsansvariga som är föremål för dataskyddsombudets granskningar.

Av granskningen framgår att den övergripande sammanställningen har återkopplats till respektive GDPR-ansvarig. Vi bedömer att nulägesanalyser samt resultatet av interna granskningar ska återkopplas till berörd nämnd vid lämpligt nämnds-sammanträde, då det är nämnder och styrelser som är personuppgiftsansvariga. Respektive förvaltningsledning ansvarar för att informationen når nämnden/styrelsen.

Interngranskningar

Vi bedömer att det är det är av vikt att dataskyddsombudet genomför **interna granskningar** av nämndernas samt kommunala bolags arbete med dataskydds-förordningen. Granskningarna bör efter en utförd nulägesanalys, genomföras av avgränsande och specifika områden i syfte att underlätta nämnders/styrelsers arbete att komma framåt, där olika frågor bör hanteras stegvis och i en rimlig takt.

Resultatet av en interngranskning bör sammanställas i form av en kortfattad och lättbegriplig rapport med framkomna utvecklingsområden och brister följt av ett avsnitt med tydliga rekommendationer avseende erforderliga åtgärder. Rapporten ska tillställas ansvarig nämnd/styrelse som avgör vilka åtgärder som ska vidtas.

Bör framhållas att oaktat om en granskning äger rum på förvaltningsnivå eller ett avgränsat verksamhetsområde (exempelvis äldreomsorgen, IFO, barnomsorg, grundskolan mm.), ska rapporten tillställas berörd nämnd som är ansvarig för verksamheten. Därefter är det upp till personansvarig nämnd/styrelse att avgöra vidarehanteringen, där dataskyddsombudets uppdrag stannar vid avlämning av granskningsrapporten. Dataskyddsombudet ska efter avlämning av en interngranskning finnas tillgänglig för råd och stöd.

Granskningsplan

Vad avser interna granskningar rekommenderar vi att en **årlig granskningsplan** upprättas, som i god tid förankras hos respektive förvaltningschef. Av granskningsplanen bör följande framgå:

- Vilka avgränsande områden som är föremål för granskning under aktuellt år, följt av
- En tidsplan för genomförandet, slutrapport och återkoppling.

Av intervju med dataskyddsombudet framgår att det finns ambitioner att arbeta fram en plan för interngranskningar, vilket bedöms som positivt.

Årlig statusrapport

Vidare bör dataskyddsombudet sammanställa en **årlig statusrapport** som tillställs **kommunstyrelsen i sin helhet** i syfte att möjliggöra utövandet av styrelsens **uppsiktsplikt** som är ett kollektivt ansvar för samtliga ledamöter i styrelsen.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

Den årliga statusrapporten bör på ett konkret och kortfattat sätt återge nämnders och styrelsers status vad avser efterlevnad av dataskyddsförordningens olika delar. Alltför omfattande underlag riskerar att tappa sin verkningsgrad samt leda till en dokumentationströtthet. Därmed är det av vikt att årliga statusrapporter redogör för respektive nämnds risker och de delar som inte har uppfyllts enligt lagstiftningens krav på ett summariskt sätt.

Av intervju med dataskyddsombudet framgår att upprättad nulägesanalys kommer att komprimeras med fokus på centrala brister och utvecklingsområden, för att tillställas kommunstyrelsen. Vi anser att detta bör prioriteras så att kommunstyrelsen kan utöva sin uppsiktplikt, där styrelsen har ett ansvar för att följa upp nämndernas och de kommunala bolagens efterlevnad av dataskyddsförordningen.

Ansvar

Det bör framhållas att det är personuppgiftsansvariga nämnder och styrelser som är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskydds-förordningen och ansvarar därmed för verkställandet. Kommunstyrelsens uppsiktplikt ska därmed inte förväxlas med rollen som personuppgiftsansvarig, där kommunstyrelsen inte kan inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse. Dock har kommunstyrelsen ett ansvar för framtagande av centrala kommunövergripande styrdokument och rutiner i syfte att säkerställa en enhetlig hantering inom samtliga nämnder och styrelser samt tillse att det råder en tillfredställande samt homogen kunskapsnivå.

Resurser och benämningar

Vad avser utsedda ”GDPR-ansvariga” rekommenderar vi att respektive nämnd förtydligar hur stor andel av tjänsten som ska ägnas dataskyddsfrågor. Detta bl.a. i syfte att underlätta arbetsplaneringen för berörda då utsedda personer har i grunden andra funktioner som ska delas med uppdraget som GDPR-ansvarig. Ett förtydligande av tidsomfattningen är också central för att i ett senare skede kunna utvärdera huruvida avsatt tjänsteomfattning är tillräcklig.
Behovet av ytterligare resurser/funktioner avgörs av respektive **nämnd/styrelse**.

Vad avser benämningen ”GDPR-ansvarig” anser vi att den bör ersättas av ”GDPR-samordnare/handläggare”, då det är nämnden/styrelsen som är ansvarig och inte tjänstepersoner.

3.5 Utnämning av dataskyddsombud

Personuppgiftsansvariga[1] inom ramen för kommunens verksamheter ska utse ett dataskyddsombud i enlighet med artikel 37.1, dataskyddsförordningen. Beslutet ska dokumenteras och vara protokollfört.

Iakttagelser

[1] Personuppgiftsansvarig är respektive nämnd och styrelse.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

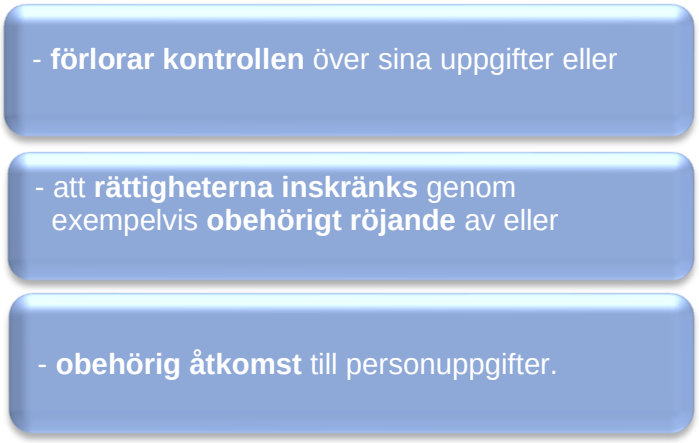
Vi har begärt ut och delgivits nämndernas beslut avseende utnämning av dataskydds-ombud, där nämnderna formellt har utsett ett dataskyddsombud.

3.4.1 Bedömning

Granskningen visar att nämnderna formellt har utsett ett dataskyddsombud.

3.6 Personuppgiftsincidenter

En **personuppgiftsincident är** en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna innebär närmare att individer:



Dataskyddsförordningen, (artikel 33, punkt 1), fastställer att vid en personuppgifts-incident ska den personuppgiftsansvarige utan onödigt dröjsmål och inte senare än **72 timmar** efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. I Sverige är det Integritetsskyddsmyndigheten (f.d. Datainspektionen) som är behörig tillsynsmyndighet.

Den **registrerade ska informeras** om personuppgiftsincidenten **utan onödigt dröjsmål**, om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 34, punkt 1).

De personuppgiftsincidenter som **inte bedöms medföra risker** för individers rättigheter och friheter **behöver ej anmälas** till tillsynsmyndigheten. Därav är det av vikt att ansvarig nämnd/styrelse genomför en konsekvensanalys vid eventuella incidenter i syfte att bedöma allvarlighetsgraden.

Samtliga personuppgiftsincidenter ska **dokumenteras oaktat allvarlighetsgrad**.

EU-rätten fastställer vidare att i de fall där organisationen har anlitat ett personuppgifts-biträde, (PuB), ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige, (nämnd/styrelse), utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, (artikel 33, punkt 2).

3.7 Omfattningen av personuppgiftsincidenter och kunskapsnivå

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

Iakttagelser

Vi har begärt in statistik avseende antal upptäckta personuppgiftsincidenter under perioden 2018 – 2021. Nedan redogörs för antal personuppgiftsincidenter som sedan dataskyddsförordningens ikraftträdande i maj 2018, uppgår till totalt 41 st enligt följande:

- 2018: 3 st
- 2019: 5 st
- 2020: 11 st
- 2021: 22 st

Tabell 3.6.1, KPMG

3.7.1 Bedömning

Nämnd	Antal incidenter **2018**	Varav anmälda till DI	Antal incidenter **2019**	Varav anmälda till DI	Antal incidenter **2020**	Varav anmälda till DI	Antal incidenter **2021**	Varav anmälda till IMY
Kommunstyrelsen					**1**	1	**4**	4
Socialnämnden							**5**	4
Vård- och omsorgsnämnden			**1**	0	**1**	1	0	0
Förskolenämnden	**1**	1			**1**	0	**3**	3
Grundskolenämnden	**2**	1	**4**	3	**7**	6	**8**	8
Gymnasie- och arbetsmarknadsnämnden					**1**	1	**1**	1
Bygglovs- och tillsynsnämnden							**1**	0
Klimat- och stadsmiljönämnden							0	0
Kultur- och fritidsnämnden			**1**	1			0	0

Dokumentation av personuppgiftsincidenter och inrapportering vid behov till Integritets-skyddsmyndigheten, (f.d. Datainspektionen), samt den registrerade är lagstadgad.

Vi bedömer att det finns ett större mörkertal gällande antalet inträffade personuppgifts-incidenter. Vår bedömning är att sannolikheten att flertalet nämnder inte har haft någon form av personuppgiftsincident alternativt har endast ett par fall, är låg.
Denna bild delas av intervjuade tjänstepersoner, där det råder enighet att en kommun av Huddinges storlek med ca 6700 anställda borde ha betydligt fler incidenter än de som har

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

redovisats.

Som referens kan nämnas att Integritetsskyddsmyndigheten får in ca 90 anmälningar per vecka vad avser personuppgiftsincidenter samtidigt som det finns ett stort mörkertal avseende anmälningspliktiga incidenter som inte kommer till tillsynsmyndighetens kännedom.

Vi bedömer att avsaknad av tillräckliga kunskaper vara den bakomliggande orsaken. Bedömningen delas av politik och tjänstepersoner.

Vi anser att det finns ett tydligt behov av kunskapshöjande insatser för förvaltningarna samt personal ute i verksamheterna.

Vi bedömer att det finns ett behov av **avgränsade utbildningsinsatser** som behandlar enskilda områden, i detta fall utveckling av begreppet ”personuppgiftsincident”, upptäckt, dokumentation och hantering. Generella utbildningar är lämpliga i samband med att exempelvis nya lagstiftningar träder ikraft eller för nyanställd personal. Därefter krävs avgränsande och områdesspecifika utbildningar i syfte att konkretisera tillämpningen och öka graden av efterlevnad.

Vi rekommenderar en central styrning från kommunstyrelsens sida vad avser utbildnings-insatser inom dataskyddsförordningen, då det finns ett behov av att säkerställa en **enhetlig kunskapsnivå** inom nämnderna.

Vi rekommenderar att kommunstyrelsens ledamöter årligen får ta del av statistik, i likhet med presenterad tabell 3.6.1, avseende inträffade personuppgiftsincidenter inom samtliga nämnder och styrelser (kommunala bolag). Vid tid för granskningen saknar kommunstyrelsen en överblick över inträffade incidenter. Detta är av vikt för styrelsens uppsiktsplikt och utgör ett underlag för eventuella åtgärdsbehov. Lämplig tidpunkt för en redogörelse av samlad statisk för året som gått, är vid kommunstyrelsens första sammanträde nästkommande år.

3.8 Personuppgiftsincidenter – styrdokument, risk- och konsekvensbedömning och dokumentation

Iakttagelser

Vid tid för granskningen saknas fastställda kommunövergripande styrdokument och rutiner för hantering och dokumentation av personuppgiftsincidenter. Vi har delgivits ett äldre styrdokument daterad 2018-05-18 som enligt uppgift inte har fastställts. Kommun-övergripande styrdokument behöver godkännas av kommunstyrelseförvaltningens ledning samt fastställas av kommunstyrelsen. Ett nytt styrdokument i form av en rutinbeskrivning är nu under framtagning innehållande 9 steg, där vi har tagit del av utkastet.

Av totalt 41 ”kända” incidenter i enlighet med tabell 3.6.1, finns någon form av dokumentation för 22 av dessa.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

3.8.1 Bedömning

En korrekt hantering av personuppgiftsincidenter är avgörande för kommunmedborgarnas/brukarnas integritetsskydd. Vi bedömer att det är en väsentlig brist att det sedan lagens ikraftträdande maj 2018 inte har fastställts kommunövergripande rutiner för hantering av personuppgiftsincidenter som är en central del i dataskyddsförordningen. Det bör understrykas att personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till förtroendeskador samt sanktionsavgifter.

Vi bedömer att avsaknaden av ett kommunövergripande styrdokument/rutin i kombination med otillräckliga kunskaper avseende personuppgiftsincidenter är de bakomliggande orsakerna till bristande dokumentation och efterlevnad.

Dokumentation

Samtliga personuppgiftsincidenter **oaktat allvarlighetsgrad** ska dokumenteras enligt gällande lagstiftning. Bör noteras att det är personuppgiftsansvarig nämnd och styrelse som ansvarar för att det finns en dokumentation och att den uppfyller dataskyddsförordningen krav. Det är därmed inte dataskyddsombudets ansvar, utan vederbörande ska agera rådgivande.

Den befintliga dokumentationen för de 22 av 41 incidenterna är i form av flertalet korrespondens mellan olika parter, vilket gör det svårt att få en helhetsbild av hanteringen av en incident. Dock i de fall där tillsynsmyndighetens anmälningsunderlag har ifyllts för en vidareanmälan, återfinns en samlad bild av incidenten. Detta innebär att en erforderlig helhetsbild erhålls endast i de fall där en incident har anmälts till tillsynsmyndigheten, då det i dagsläget saknas en enhetlig dokumentationsstruktur vad avser personuppgiftsincidenter.

Beskrivning av en incident och omständigheterna kring den (dvs. samlat resultat från genomförd korrespondens med berörda), bedömning av risker och konsekvenser, vidtagna och korrigerande åtgärder, huruvida den registrerade (dvs. den drabbade) ska informeras mm. bör upprättas i ett samlat dokument. Detta är nödvändigt för att uppnå en enhetlig hantering av inträffade incidenter i enlighet med lagstiftningens krav.

Vi bedömer att kommunstyrelsen bör ta ett beslut om en **enhetlig struktur** följt av **en dokumentationsmall** vad avser dokumentation av personuppgiftsincidenter (se rekommendation och vägledning på sid 18).

Vid en anmälan

Det bör noteras att på frågan om vem som är ”personuppgiftsansvarig” i anmälningsblanketten, ska den nämnd/styrelse där incidenten har inträffat anges, då det är nämnd och styrelse som juridiskt sett är personuppgiftsansvariga. Vi har noterat att i samtliga fall har Huddinge kommun angivits som personuppgiftsansvarig. Kommunnamnet ska anges efter att personuppgiftsansvarig nämnd/styrelse har angivits.

Delar som behöver beaktas

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

Lagstiftningen ställer krav vad gäller dokumentation av personuppgiftsincidenter, där den personuppgiftsansvarige (dvs. nämnd/styrelse) ska:

- dokumentera samtliga personuppgiftsincidenter inbegripet
- omständigheterna kring incidenten,
- effekter (där en konsekvensbedömning erfordras), samt
- de korrigerande åtgärder som har vidtagits.

Anmälningsskyldighet till Integritetsskyddsmyndigheten råder vid de personuppgifts-incidenter som bedöms medföra en risk för de registrerade. Därmed behöver ansvarig nämnd/styrelse göra en **bedömning av risker och konsekvenser** av varje incident för att kunna avgöra huruvida incidenten ska anmälas till tillsynsmyndigheten eller ej.

Likaså ska **den registrerade** (dvs. de drabbade) informeras om incidenten utan onödigt dröjsmål, om incidenten sannolikt leder till en hög risk för de drabbades rättigheter och friheter.

En incident ska bedömas utifrån följande allvarlighetsgrader:

1. Obetydlig
2. Begränsad
3. Betydande
4. Mycket allvarligt

Ovan nämnda delar bör på ett enkelt och tydligt sätt framgå av det styrdokument som kommunstyrelsen behöver snarast fastställa.

Likaså är det av vikt att i styrdokumentet förtydliga att samtliga personuppgiftsincidenter ska dokumenteras och diarieföras på berörd förvaltning **oaktat allvarlighetsgrad.** Detta i syfte att tydliggöra för medarbetarna att **dokumentationsplikt** gäller oavsett om incidenten ska anmälas till tillsynsmyndigheten eller ej.

Vidare är det av vikt med en konkret beskrivning av den praktiska hanteringen av incidenter i styrdokumentet, dvs. vad ska en medarbetare göra när en incident upptäcks, vem ansvarar för dokumentationen, vilken dokumentationsmall ska användas mm.

Befintligt utkast till rutinbeskrivning

Dagens utkast till rutinbeskrivning avseende hantering av personuppgiftsincidenter innehåller 9 steg. Vad avser det sista steget (9) som avser att återge en helhetsbild, innan ärendet stängs, finns en mall framtagen som innefattar delar från tillsynsmyndighetens anmälningsblankett. Vi har granskat mallen, där den är i behov av kompletteringar med följande delar:

- Ansvarig nämnd/styrelse ska anges. Det är oerhört viktigt att personuppgifts-ansvarig nämnd/styrelse framgår i samtliga underlag då det är berörd nämnd/styrelse som är juridiskt ansvarig.
- Datum för incidentens inträffande.
- Datum för incidentens upphörande, (tidsperspektivet är viktig information för

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

bedömning av konsekvenserna).

- Av incidentbeskrivningen bör framgå huruvida det handlar om:

  - obehörigt röjande,
  - obehörig åtkomst,
  - förlust,
  - förstöring eller
  - ändring

- Antal berörda, dvs. hur många registrerade har påverkats.
- Antal uppgifter, dvs. hur många uppgifter om de registrerade som har påverkats.
- Kategori av drabbade (exempelvis anställda, brukare/kunder, barn mm.).
- Huruvida uppgifterna var krypterade.
- Vid kolumnen för ”konsekvenser” bör det finnas förslagsalternativ för huruvida det handlar om att: den registrerade förlorar kontrollen över sina personuppgifter, begränsning av rättigheter, identitetsstöld, bedrägeri, ekonomisk förlust, förlust av konfidentialitet avseende uppgifter som omfattas av tystnadsplikt (här ingår t.ex. individer med skyddad identitet), skadat anseende mm.
- Datum för korrigerande åtgärder.
- Beskrivning av vilka korrigerande åtgärder som **har** vidtagits (i dagsläget finns endast en kolumn avsett för framåtsyftande åtgärder som behöver vidtas)
- Huruvida incidenten har inträffat hos ett personuppgiftsbiträde med information om biträdet.

Det bör understrykas att om mallen i steg 9 ska tas i bruk är det centralt att ovan-nämnda delar upptas i mallen.

Styrdokumentens utformning

Vi anser att styrdokumentens omfattning, komplexitet, struktur, språk och användarvänlighet är bl.a. avgörande för graden av efterlevnad och verkställighet ut i verksamheterna, där omständliga och svårgenomförbara rutinbeskrivningar bör undvikas. Detta är än mer viktigt när kunskapsnivån inte är på en tillräcklig nivå i organisationen. Övervägande del av medarbetarna ska kunna förstå och hantera en rutinbeskrivning, därmed behöver styrdokument vara lättbegripliga, enkla och användarvänliga.

Vi bedömer att utkastet avseende rutinbeskrivningen innehållande 9 steg behöver förenklas samt reduceras vad avser antalet steg i syfte att underlätta genomförandet samt minska den administrativa omfattningen. I praktiken innebär det också att en incident kommer att ha flera dokumentationsunderlag med utredningar i flera steg.

Vi anser att flera dokumentationsmallar, lösa worddokument, ostrukturerat innehåll mm. bör undvikas. Vi bedömer att det är fullt tillräckligt med **en enda dokumentationsmall**

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

som ifylls allteftersom ny information blir tillgänglig gällande en incident. Det är av vikt att personuppgiftsansvariga nämnder/styrelser med tillhörande förvaltningar får en lättöverskådlig samt samlad bild av en personuppgiftsincident som är nödvändig för att rutinen ska fungera.

Likaså är det av vikt med en samlad bild för kommunstyrelsens del i syfte att möjliggöra utövandet av uppsiktsplikten.

Vi rekommenderar kommunstyrelsen att använda sig av tillsynsmyndighetens anmälningsblankett i sin helhet för dokumentation av personuppgiftsincidenter, där samtliga nödvändiga delar (inklusive risk- och konsekvensbedömning) finns upptagna i enlighet med dataskyddsförordningen. Detta bidrar till en **enhetlig hantering** av upptäckta incidenter inom samtliga nämnder/styrelser, leder till minskad administration och tidsåtgång, underlättar spårbarheten samt bidrar till en effektivitet i form av ett centralt dokument. Vidare minimeras riskerna för bortfall av information. Vi anser att det är av vikt att undvika onödiga administrativa belastningar som i sin tur kan leda till minskad verkställighet.

Tillsynsmyndighetens mall innehåller färdiga förslagsalternativ i syfte att underlätta dokumentationen och öka efterlevnadsgraden i organisationerna. Detta innebär att utsedda medarbetare (GDPR-samordnare m.fl) som ska ifylla underlaget inte behöver vara sakkunniga.

Ytterligare reducering av administration och fördel med intern användning av IMY:s dokumentationsmall är att vid ett beslut att anmäla en incident till tillsynsmyndigheten, behöver förvaltningen inte fylla i ett nytt underlag, utan redan ifylld blankett skickas in.

3.9 Registerförteckningar

All behandling av personuppgifter ska uppfylla de grundläggande principerna i enlighet med dataskyddsförordningen.

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

Dataskyddsförordningen fastställer för att påvisa att förordningen följs ska person-uppgiftsansvariga föra register över behandling som sker under deras ansvar, (s.k. registerförteckningar). Registerförteckningarna ska på begäran redovisas för

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

tillsynsmyndigheten, dvs. Integritetsskyddsmyndigheten, där registren ska utgöra en grund för övervakning av behandling av personuppgifter.

Iakttagelser

Av granskningen framgår att det finns registerförteckningar för samtliga nämnder med varierande kvalité. Enligt avstämning med dataskyddsombudet har en kvalitetssäkring påbörjats, dock saknar utsedda GDPR-ansvariga tillräckliga kunskaper, där dataskyddsombudet får agera stöttande. Planen har varit att samtliga nämnder ska använda sig av SKR:s mall för registerförteckningar. Vi har dock uppmärksammat att **förskolenämnden** och **grundskolenämnden** använder sig av en annan mall.

Dataskyddsombudet har under hösten genomfört en övergripande kontroll av registerförteckningarna där register över behandlingarna bedöms hålla en låg och otillräcklig nivå inom samtliga nämnder med undantag för kultur- och fritidsnämnden.

3.9.1 Bedömning

Dataskyddsförordningen fastställer att för att påvisa att förordningen följs ska personuppgiftsansvariga föra register över behandling som sker under deras ansvar. Granskningen påvisar att nämnderna har upprättat register över behandlingar, dock med varierande kvalité.

Vi har vidare noterat att nämnderna inte använder sig av samma mall och frågeställningar, vilket leder till än mer oenhetlig hantering.

Vi har genomfört en granskning av registren, där vi har noterat väsentliga brister enligt följande:

- Vi bedömer antalet registerförteckningar/behandlingar vara för få i förhållande till de verksamhetsområden som hanteras.
- Respektive nämnd ska ha ett självständigt register, där registren för olika personuppgiftsansvariga inte ska slås samman. I dagsläget har förskolenämnden och grundskolenämnden ett gemensamt register.
- Gymnasie- och arbetsmarknadsnämndens register saknar väsentliga kolumner med centrala frågeställningar som har tagits bort fr SKR:s ursprungsmall. Mallen bör återställas snarast till att omfatta samtliga delar.
- Sammanslagning av flera ändamål/syften. Det bör noteras att personuppgifter får behandlas för specifika, särskilt angivna och berättigade ändamål.
- Sammanslagning av flera system. Respektive system/verktyg ska redogöras separat med särskilt angiva och avgränsade ändamål.
- Frågetecken kring vilken nämnd som är personuppgiftsansvarig.
- Avsaknad av information om överföring till tredje land.
- Avsaknad av information om huruvida det finns personuppgiftsbiträden.
- Hänvisning till ”systemförteckning” för information om huruvida ett personuppgiftsbiträde anlitas. (Vård- och omsorgsnämnden)
- Avsaknad av tidsfrister för radering.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

- Hänvisning till dokumenthanteringsplanen vad avser tidsfrister för radering. Det bör noteras att vad avser angivande av tidsfrister ska dessa anges uttryckligen, dvs. det räcker inte med en hänvisning till nämndens dokumenthanteringsplan. Denna punkt berör dataskyddsförordningens grundläggande princip om ”lagringsminimering”.
- Förekomst av ostrukturerat material på olika filytor.
- Avsaknad av rättslig grund för behandlingen ifråga.
- Förekomst av ogiltig rättslig grund. (t.ex.: att dokumenthanteringsplanen anges som rättslig grund)
- Avsaknad av beskrivning av tekniska och organisatoriska säkerhetsåtgärder för den aktuella personuppgiftsbehandlingen.
- ”**Uppgift av allmänt intresse**” anges som rättslig grund utan hänvisning till lagstöd. För att uppgifter av allmänt intresse ska kunna nyttjas krävs stöd i lagstiftningen eller beslut som har meddelats med stöd av lagstiftning. Det är av vikt att personuppgiftsansvarig nämnd kan motivera valet av rättslig grund.
- Behandling av känsliga personuppgifter med motiveringen att det är av allmänt intresse. Vad avser ”känsliga personuppgifter” är utgångspunkten att det är förbjudet att behandla dessa. Det finns dock undantag. Det ställs därmed krav på att behandling av känsliga personuppgifter ska vara väl motiverade och välgrundade med stöd i lagstiftningen.
- Ytterligare rättslig grund som används är ”**myndighetsutövning**”, dock saknas hänvisning till aktuell författning. All myndighetsutövning ska grundas på lagar inom EU-rätten eller nationell rätt.

Vi bedömer sammantaget att det finns väsentliga brister vad avser register över personuppgiftsbehandlingar.

Styrelsen samt samtliga nämnder bör snarast genomföra en inventering och säkerställa att förteckningar upprättas för samtliga personuppgiftsbehandlingar. Som exempel kan nämnas att grundskolenämnden samt förskolenämnden har i ett gemensamt register endast angivit 11 behandlingar, vilket är ytterst låg i förhållande till verksamheternas omfattning. Härigenom bör förskolenämnden och grundskole-nämnden skyndsamt genomföra en inventering samt också upprätta självständiga register över behandlingar.

Vi rekommenderar att kommunstyrelsen fastställer **en tidsram fastställas** då samtliga personuppgiftsbehandlingar bör ha upptagits.

Vi bedömer att det råder en låg kunskapsnivå vad avser hantering av register över personuppgiftsbehandlingar, där det finns behov av en riktad utbildning för att komma till rätta med befintliga brister.

Vi har noterat att det råder en oenhetlig struktur vad avser frågeställningarna i de registermallar som används. Vi bedömer att det krävs en central styrning från kommunstyrelsen sida, där styrelsen bör fatta ett kommunövergripande beslut om vilken **registermall** som ska användas, följt av en enhetlig struktur vad avser de frågor

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

som ska besvaras. Det bör noteras att **obligatoriska frågor** i enlighet med dataskyddsförordningen ska finns med i mallen för registerförteckningarna. Övriga frågor som kan vara till nytta för verksamheterna kan tillföras.

Vi anser att SKR:s mall är tillräcklig för upprättande av register över behandlingar, förutsatt att frågeställningar inte tas bort, att erfordrad information ifylls samt att frågorna besvaras på ett korrekt sätt.

3.10 Registerutdrag, rättelse, radering och begränsning

I enlighet med dataskyddsförordningen har den registrerade rätt att begära ut ett så kallat registerutdrag från offentliga och privata organisationer. Ett registerutdrag ska redogöra för de personuppgifter som en myndighet eller ett företag behandlar om en person samt på vilket sätt uppgifterna behandlas.

Likaså har den registrerade rätt till att utan dröjsmål få felaktiga uppgifter rättade. På samma sätt finns rättigheten att utan onödigt dröjsmål få sina personuppgifter raderade om de exempelvis inte längre är nödvändiga för de ändamål för vilka de samlats in eller att den registrerade återkallar sitt samtycke som behandlingen grundar sig på. Den registrerade kan också invända mot registreringen utifrån att det saknas en laglig grund för behandlingen.

Ytterligare rättigheter avser begränsning av behandling av personuppgifter, där den registrerade under visa omständigheter kan kräva att personuppgifter behandlas endast för vissa avgränsade syften.

Iakttagelser

Av granskningen framgår att en rutin för begäran av registerutdrag har upprättats under 2019, men som enligt uppgift inte har fastställts. Vid tid för granskningen finns ett utkast till ny rutinbeskrivning vad avser begäran om registerutdrag.

Vad avser hanteringen av begäran avseende rättelse, radering och begränsning, finns inget styrdokument.

3.10.1 Bedömning

Vi bedömer att kommunstyrelsen snarast bör upprätta en samlad rutinbeskrivning avseende hanteringen av inkomna **begäran om rättelse, radering och begränsning**. Rutinbeskrivningen bör vara kortfattad med tydliga ansvars- och rollfördelningar, med fokus på den praktiska hanteringen vid en inkommen begäran.

Vi bedömer att det är av vikt med enkla, användarvänliga och kortfattade rutinbeskrivningar, då det annars finns en risk för att styrdokumenten tappar sin legitimitet ut i verksamheterna och blir ”hyllvärmare”.

Vad avser befintligt utkast avseende rutin om **begäran om registerutdrag**, bedömer vi att den bör reduceras kraftigt i omfattning samt förenklas i syfte att underlätta för medarbetarna samt öka graden av verkställighet. I dagsläget är utkastet till rutinbeskrivningen 17 sidor, följt av två bilagor.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public

Datum som ovan

KPMG AB

Viktoria Bernstam

Viktoria Bernstam
Certifierad kommunal revisor

Micaela Hedin

Micaela Hedin
Certifierad kommunal revisor

Detta dokument har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.

© 2021 KPMG AB. All rights reserved.

Document classification KPMG Public