Kalmar kommunrevision

2022-05-19

Kommunstyrelsen

För kännedom
Kalmarhem AB
Kalmar Vatten AB
Socialnämnden
Utbildningsnämnden
Kommunfullmäktiges presidium

Granskning av GDPR

På uppdrag av revisorerna i Kalmar kommun har PwC genomfört en granskning avseende om kommunstyrelsen, Kalmarhem och Kalmar Vatten samt förvaltningarna säkerställt att det finns ändamålsenliga rutiner, processer och kontroller kring GDPR.

Då flera av rapportens rekommendationer är generella för arbetet med GDPR och kan vara giltiga för flera förvaltningar och bolag inom kommunkoncernen, beslutade vi vid vårt sammanträde den 19 maj 2022 att överlämna upprättad rapport till kommunstyrelsen för ett samordnat svar. Rapporten överlämnas även för kännedom till Kalmarhem, Kalmar Vatten, socialnämnden och utbildningsnämnden, samt kommunfullmäktiges presidium.

Av rapporten framgår gjorda iakttagelser, revisionell bedömning och rekommendationer.

Vi önskar få svar från kommunstyrelsen senast den 31 oktober 2022 med redogörelse av åtgärder utifrån de påpekanden och rekommendationer som framkommer i rapporten.

Kommunfullmäktiges presidium får ta ställning till om revisionsrapporten ska biläggas fullmäktiges handlingar.

För kommunens revisorer

Per Dahl
Ordförande

Jan Bengtsson
Vice ordförande

Granskning av GDPR

Kalmar kommun

2022-05-19

Peter Olby, Sara Milenkovska

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Kalmar kommun genomfört en granskning av hur kommunen efterföljer GDPR. Granskningens syfte är undersöka om kommunstyrelsen och de granskade bolagen samt förvaltningarna säkerställt att det finns ändamålsenliga rutiner, processer och kontroller kring GDPR.

PwC har genomfört intervjuer med Kalmarhem AB, Kalmar Vatten AB, socialförvaltningen samt utbildningsförvaltningen. Utöver intervjuerna har PwC granskat relevant material från de olika enheterna.

Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelsen och de granskade bolagen delvis har ändamålsenliga rutiner, processer och kontroller kring GDPR. Bedömningen delvis grundas på revisionsfrågorna för incidenthantering och uppföljning. För övriga revisionsfrågor är bedömningen att det i allt väsentligt finns en ändamålsenlighet.

Nedan ses bedömning för varje revisionsfråga.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
1. Har kommunen och bolagen tydligt definierade roller och ansvar inom området dataskydd, med erforderlig dokumentation?	**Ja** De granskade bolagen och förvaltningarna har i allt väsentligt definierade roller och ansvar för data dataskydd. Det är tydligt kommunicerat såväl inom som utanför organisationerna vart frågor kring dataskydd ska ställas samt att det finns ett aktivt engagemang hos ledningarna för förvaltningarna och bolagen för området.	
2. Har kommunen och bolagen upprättat ett behandlingsregister där syfte och laglig grund för behandlingen framgår?	**Ja** De granskade bolagen och förvaltningarna har i allt väsentligt upprättat ett behandlingsregister där respektive personuppgift dokumenteras tillsammans med syfte och laglig grund samt annan relevant information.	

3. Säkerställer kommunen och bolagen att datasubjektens rättigheter tillgodoses genom erforderliga rutiner?	**Ja** De granskade bolagen och förvaltningarna har i allt väsentligt rutiner för att tillgodose datasubjektens rättigheter.	
4. Har kommunen och bolagen rutiner för de situationer där kommunen agerar personuppgiftsbiträde åt annan (inkl. hantering av tredje part)?	**Ja** Endast Socialförvaltningen och Kalmar Vatten AB har identifierat personuppgiftsbehandlingar där de agerar personuppgiftsbiträde åt andra organisationer. I samtliga dessa fall finns erforderliga biträdesavtal upprättade.	
5. Har kommunen och bolagen adekvata säkerhetsåtgärder och en dokumenterad incidenthantering för att minska effekterna av personuppgifts-incidenter? *(Hur många rapporteringsskyldiga personuppgiftsincidenter har rapporterats till Datainspektionen / Integritetsskydds-myndigheten från år 2020 och framåt?)*	**Delvis** De granskade bolagen och förvaltningarna har i allt väsentligt dokumenterade rutiner för incidenthantering. Dock har granskningen visat på att det finns vissa brister i att upptäcka och att rapportera incidenter.	
6. Genomför dataskyddsombudet uppföljningar med förvaltningar och bolag för att säkerställa att de lever upp till GDPR och att eventuella åtgärder vid behov vidtas? *(Exempel på större brister som framkommit vid uppföljningarna)*	**Delvis** Uppföljning av efterlevnad utförs, dock saknas det idag tid och resurser för att bedriva ett mer proaktivt arbete. Detta då dataskyddsombud även är kommunjurist och tiden måste delas mellan dessa två roller. Denna delade tjänst medför även en risk för självgranskning. Vidare sker idag ingen formaliserad rapportering från förvaltningarna eller bolagen av sin efterlevnad till dataskyddsombudet.	

Rekommendationer

Kalmarhem AB

- Bolaget rekommenderas att tydliggöra och dokumentera rollen som ansvarar för frågor kopplat till GDPR, detta med fokus på vilket mandat denna roll har då denna i dagsläget upplevs som otydligt.
- Bolaget rekommenderas att formalisera rutiner för att säkerställa att behandlingregistret regelbundet revideras och hålls uppdaterat.
- Bolaget rekommenderas att utöka frekvensen i sina utbildningsinsatser kopplat till GDPR då ledningen idag upplever att det finns ett ökat behov.
- Bolaget rekommenderas att upprätta rutiner för att regelbundet och strukturerat genomföra uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att dessa fortfarande har adekvata säkerhetsåtgärder.

Socialförvaltningen

- Förvaltningen rekommenderas att upprätta rutiner för att regelbundet och strukturerat genomföra uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att dessa fortfarande har adekvata säkerhetsåtgärder.

Kalmar Vatten AB

- Bolaget rekommenderas att upprätta rutiner som säkerställer att den information som ges till datasubjekt inför en behandling möter kraven i förordningen.
- Bolaget rekommenderas att upprätta rutiner för att regelbundet och strukturerat genomföra uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder..

Utbildningsförvaltningen

- Förvaltningen rekommenderas att formalisera rutiner för att säkerställa att behandlingregistret regelbundet revideras och hålls uppdaterat.
- Förvaltningen rekommenderas att utforma och implementera kontroller som säkerställer att den information som ges till datasubjekt inför en behandling möter kraven i förordningen.
- Förvaltningen rekommenderas att stärka sina insatser för att upptäcka, rapportera och motverka personuppgiftsincidenter. Detta kan exempelvis ske genom ytterligare

utbildningsinsatser eller förtydligande av riktlinjer baserat på analyser av tidigare incidenter.

- Förvaltningen rekommenderas att upprätta rutiner för att regelbundet och strukturerat genomföra uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder.

Kommunstyrelsen

- Kommunstyrelsen rekommenderas att utvärdera om den delade rollen som kommunjurist och dataskyddsombud medför en risk för självgranskning.
- Kommunstyrelsen rekommenderas att införa processer för att säkerställa att det sker regelbunden sammanställning, analys och rapportering över personuppgiftsincidenter inom kommunkoncernen.

Innehållsförteckning

Inledning

Bakgrund - GDPR

EU:s dataskyddsförordning, General Data Protection Regulation (GDPR), innebär en skärpning av dataskyddslagstiftningen inom EU, både avseende organisationers åligganden och de registrerade personernas rättigheter. Den gäller för alla organisationer, företag och myndigheter som hanterar uppgifter om EU-medborgare. För att den ska respekteras införs möjligheten till kraftfulla sanktioner för de organisationer som ignorerar eller brister i att uppfylla de nya kraven. Sanktionsnivåerna har valts så att de ska vara avskräckande och för att det inte ska löna sig att bryta mot reglerna för att spara pengar. Väsentliga sanktionsavgifter för bristande efterlevnad, upp till 20 miljoner kronor, kan utfärdas för myndigheter. Det införs också en rätt för privatpersoner att kräva skadestånd av de organisationer som inte tillgodoser deras rättigheter enligt förordningen. Förordningen började tillämpas den 25 maj 2018.

Förordningen innehåller nya krav jämfört med Personuppgiftslagen, som exempelvis att alla organisationer själva har en skyldighet att bedöma riskerna för att de registrerades integritet kränks samt vidta lämpliga åtgärder för att minska dessa risker. Organisationer måste även i vissa fall utse dataskyddsombud och rapportera allvarliga personuppgiftsincidenter till tillsynsmyndigheten (och i vissa fall de berörda registrerade) inom 72 timmar. Om man misstänker att någon personuppgiftsbehandling kan medföra höga integritetsrisker för de registrerade måste man göra en konsekvensbedömning och vidta lämpliga åtgärder för att reducera riskerna för eventuella skador.

Syfte och revisionsfrågor

Kalmar kommuns revisorer har uppdragit åt PwC att genomföra en granskning kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskyddsförordningen (GDPR) genomförts inom det kommunägda bolagen Kalmarhem AB och Kalmar Vatten AB samt förvaltningarna Socialförvaltningen och Utbildningsförvaltningen och därvid bilda sig en uppfattning om nuläget.

Frågeställningen för denna granskning är således: *“Har kommunstyrelsen och de granskade bolagen säkerställt att det finns ändamålsenliga rutiner, processer och kontroller kring GDPR?”*.

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

- Dataskyddsförordningen
- Kommunallagen
- Övriga styrande dokument relevanta för granskningen

Avgränsning

Granskning begränsas till kommunstyrelsens och de granskade bolagsledningarnas ansvar.

Granskningen begränsas till två förvaltningar (utbildningsförvaltningen och socialförvaltningen) och två bolag inom kommunkoncernen (Kalmarhem AB och Kalmar Vatten AB).

Granskningen uttalar sig inte om kommunens eller bolagens de facto efterlevnad av Dataskyddsförordningen, utan syftar till att se om det arbete som bedrivs inom området kan betraktas som ändamålsenligt, givet de krav som förordningen ställer.

Metod

Dokumentstudier av relevant dokumentation samt intervjuer med berörda tjänsteperson. Revisionsfrågan ovan besvaras huvudsakligen genom ett frågebatteri som täcker in områdena nedan:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter
- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder (inkl. incidenthanteringsprocess)

Följande roller har medverkat i intervjuer för denna granskning.

- Kalmar kommuns informationssamordnare, dataskyddsombud, kommunjurist
- Kalmar Vatten AB:s VD, kundansvarig, verksamhetsutvecklare, HR
- Utbildningsförvaltningens förvaltningschef, administrativ chef, planeringssekreterare för digitalisering samt GDPR samordnare
- Socialförvaltningens administrativa chef, förvaltningssekreterare samt digitaliseringsledare
- Kalmarhem AB:s VD samt dataskyddsansvarig.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Styrning, roller och ansvar

Revisionsfråga 1: Har kommunen och bolagen tydligt definierade roller och ansvar inom området dataskydd, med erforderlig dokumentation?

Kalmarhem AB

Styrning, roller och ansvar

Det finns en tydlig ambition med uppdrag från ledningsgruppen ut i organisationen att följa de regler och principer som omfattas av GDPR. Ledningen i Kalmarhem är engagerade i hur organisationen arbetar med dessa frågor. Det har funnits en tydlig ambition med uppdrag från ledningsgruppen att följa de regler och principer som omfattas av GDPR. Arbetet har främst drivits av en anställd på Kalmarhem AB som jobbar med dataskyddsfrågor. Kalmarhem AB följer en fastställd integritetspolicy som har kommunicerats externt till den registrerade.

I dagsläget saknas dock en tydlig dokumentation kring mandatet för frågor gällande dataskydd och då ledningen arbetar med att att identifiera ny person som får ägarskap för frågan blir detta än viktigare. Ledningen ser även ett ökat behov av en tydligare struktur kopplat till ansvarsfördelningen mellan Kalmarhem AB och Kalmar kommun men anser att de får bra stöd från kommunens dataskyddsombud vid direkta frågor eller genom det forum som upprättats inom kommunkoncernen för att diskutera informationssäkerhet och dataskydd.

Det är tydligt definierade och kommunicerade både internt och externt hur anställda och medborgare kan komma i kontakt med dataskyddsombudet. Kontakt kan även initieras via Kalmarhems kundcenter.

Socialförvaltningen

Styrning, roller och ansvar

Ledningen i socialförvaltningen är aktivt engagerad i dataskyddsfrågor. Detta visar sig bland annat i att tillägg har gjorts till de kommungemensamma riktlinjerna för informationssäkerhet. Dessa lokala tillägg har gjorts för att täcka socialförvaltningens till viss del specifika behov.

Förvaltningen har fastställt tydliga roller gällande arbetet kring dataskydd och informationssäkerhet. Anställda upplever att det är tydligt gällande vem som arbetar med frågor kopplat till GDPR och till vem man ska vända sig till. Förvaltningssekreteraren hos

socialförvaltningen har ett utpekat ansvar för arbetet kopplat till dataskydd, däremot finns det ingen beskrivning eller dokumentation för rollen.

Förvaltningen upplever att de generellt får bra stöd från dataskyddsombudet i kommunen när detta efterfrågas.

Vid situationer då medarbetare eller externa parter vill komma i kontakt med dataskyddsombudet får de information om hur de ska gå tillväga direkt av socialförvaltningen eller via publicerad information på kommunens hemsida.

Kalmar Vatten AB

Styrning, roller och ansvar

Det finns ett aktivt engagemang för dataskyddsfrågor inom Kalmar Vatten AB med tydliga dokumenterade riktlinjer för informationshantering tillsammans med en integritetspolicy. Vidare finns det utpekad personal som arbetar med dataskydd och det är tydligt kommunicerat inom organisationen.

Bolaget upplever att de får bra stöd av kommunens dataskyddsombud, dels vid direkta frågor eller genom det forum som upprättats inom kommunkoncernen för att diskutera informationssäkerhet och dataskydd.

Det är tydligt definierat och kommunicerat, både internt och externt, hur anställda och externa parter kan komma i kontakt med dataskyddsombudet.

Utbildningsförvaltningen

Styrning, roller och ansvar

Utbildningsförvaltningen har ett aktivt arbete kopplat till GDPR och dataskydd som dels lutar sig mot kommungemensamma policys men även lokal riktlinjer som anpassats för förvaltningsspecifika processer och system.

Det finns utpekade roller som jobbar med dataskydd och informationssäkerhet inom förvaltningen. Även om dessa roller finns utpekade har förvaltningen upplevt utmaningar i att förstå och tolka alla delar i lagstiftningen. För dessa fall har det funnits stöd från dataskyddsombudet. Förvaltningen har även aktivt sökt vägledning från andra förvaltningar och även vänt sig till forum utanför kommunen för att dela kunskap med andra kommuner.

Det är tydligt definierat och kommunicerat, både internt och externt, hur anställda och externa parter kan ta kontakt med dataskyddsombudet.

Bedömning

Har kommunen och bolagen tydligt definierade roller och ansvar inom området dataskydd, med erforderlig dokumentation?

Ja

De granskade bolagen och förvaltningarna har i allt väsentligt definierade roller och ansvar för data dataskydd. Det är tydligt kommunicerat såväl inom som utanför organisationerna vart frågor kring dataskydd ska ställas samt att det finns ett aktivt engagemang hos ledningarna för förvaltningarna och bolagen för området.

Behandlingsregister

Revisionsfråga 2: Har kommunen och bolagen upprättat ett behandlingsregister där syfte och laglig grund för behandlingen framgår?

Kalmarhem AB

Behandlingsregister

Kalmarhem använder sig av det kommungemensamma systemet för att hantera sitt behandlingsregister och dokumentera sina behandlingar, dess syfte och laglig grund samt annan relevant information. Det saknas idag formaliserade rutiner för att säkerställa att behandlingsregister revideras. Dock sker detta på adhoc basis och nu senast vid en kartläggning av systemleverantörer från tredjeland (utfördes under våren 2022).

Socialförvaltningen

Behandlingsregister

Socialförvaltningen använder sig av det kommungemensamma systemet för att hantera sitt behandlingsregister och dokumentera sina behandlingar, dess syfte och laglig grund samt annan relevant information. Revidering av behandlingsregistret har skett löpande med uppdateringar vid nya eller förändrade behandlingar.

Kalmar Vatten AB

Behandlingsregister

Kalmar Vatten använder sig av det kommungemensamma systemet för att hantera sitt behandlingsregister och dokumentera sina behandlingar, dess syfte och laglig grund samt annan relevant information. Revidering av behandlingsregistret har skett som en del i det löpande arbetet.

Utbildningsförvaltningen

Behandlingsregister

Utbildningsförvaltningen använder sig av det kommungemensamma systemet för att hantera sitt behandlingsregister och dokumentera sina behandlingar, dess syfte och laglig grund samt annan relevant information. Det saknas idag formaliserade rutiner för att säkerställa att behandlingsregister revideras.

Bedömning

Har kommunen och bolagen upprättat ett behandlingsregister där syfte och laglig grund för behandlingen framgår?

Ja

De granskade bolagen och förvaltningarna har i allt väsentligt upprättat ett behandlingsregister där respektive personuppgift dokumenteras tillsammans med syfte och laglig grund samt annan relevant information.

Datasubjektens rättigheter

Revisionsfråga 3: Säkerställer kommunen och bolagen att datasubjektens rättigheter tillgodoses genom erforderliga rutiner?

Kalmarhem AB

Datasubjektens rättigheter

Kalmarhem informerar tydligt om individens rättigheter dels via hemsidan men även genom tex. villkorstexter i avtal. Det finns formaliserade processer för att begära registerutdrag, rättning eller invända mot behandling.

Kalmarhem kan hantera känslig information såsom personer med helt skyddad identitet eller personer med skyddade personuppgifter. Känsliga uppgifter hanteras av två personer i Kalmarhem AB, uppgifterna hanteras separat och inte i verksamhetens ordinarie fastighetsregister eller markandsregister. För denna typ av behandling har det utförts en risk- och konsekvensanalys.

Det kan även förekomma behandling av känsliga personuppgifter för egen personal i form av HR-relaterad data för anställda eller namn och födelsedag på anställdas barn i syfte till att hantera föräldraledighet. För dessa typer av behandlingar finns definierade processer för att säkerställa individens rättigheter.

I samband med införanden av förordningen genomgick samtliga anställda utbildning inom GDPR för att öka den allmänna kunskapen. Utöver detta sker även löpande kommungemensamma nano-utbildningarna inom dataskydd och informationssäkerhet. Bolaget ser dock ett behov av större regelbundenhet i utbildningsinsatser inom området.

Socialförvaltningen

Datasubjektens rättigheter

Socialförvaltningen informerar tydligt om individens rättigheter dels som en del i det löpande

arbetet i möten med individer, dels via hemsidan men även genom informationstexter. Det finns formaliserade processer för att begära registerutdrag, rättning eller invända mot behandling.

Socialförvaltningen hanterar stora mängder känsliga personuppgifter som en del av sitt uppdrag där behandlingen sker via förvaltningens dedikerade verksamhetssystem. Det finns även väl definierad rutiner och policys för hur denna behandling ska genomföras på ett säkert sätt. För denna typ av behandling har det utförts en risk- och konsekvensanalys.

Det kan även förekomma behandling av känsliga personuppgifter för egen personal i form av HR-relaterad data för anställda eller namn och födelsedag på anställdas barn i syfte till att hantera föräldraledighet. För dessa typer av behandlingar finns definierade kommunövergripande processer för att säkerställa individens rättigheter.

I samband med införanden av förordningen genomgick samtliga anställda utbildning inom GDPR för att öka den allmänna kunskapen. Utöver detta sker även löpande kommungemensamma nano-utbildningarna inom dataskydd och informationssäkerhet.

Kalmar Vatten AB

Datasubjektens rättigheter

Kalmar Vatten informerar tydligt om individens rättigheter via hemsidan. Dock framkom det under intervju att det inte är helt tydligt vilken informationstext som ska användas om information ska ges till en individ utanför hemsidan. Oftast kopieras text från hemsidan och kompletteras efter behov men det saknas kontroller för att säkerställa att texten möter kraven i förordningen.

Det finns formaliserade processer för att begära registerutdrag, rättning eller invända mot behandling.

Kalmar Vatten behandlar inte några känsliga personuppgifter avseende kunder. Dock kan det förekomma behandling av känsliga personuppgifter för egen personal i form av HR-relaterad data för anställda eller namn och födelsedag på anställdas barn i syfte till att hantera föräldraledighet. För dessa typer av behandlingar finns definierade processer för att säkerställa individens rättigheter.

I samband med införanden av förordningen genomgick samtliga anställda utbildning inom GDPR för att öka den allmänna kunskapen. GDPR är även en del av det utbildningspaket som nyanställda genomgår. Utöver detta sker även löpande kommungemensamma nano-utbildningarna inom dataskydd och informationssäkerhet.

Utbildningsförvaltningen

Datasubjektens rättigheter

Utbildningsförvaltningen informerar tydligt om individens rättigheter dels som en del i det löpande arbetet i möten med individer, dels via hemsidan men även genom informationstexter till både elever och föräldrar. Dock framkom i intervju att förvaltningen upplever själva att de inte vet om den information som de delar är tillräcklig.

Det finns formaliserade processer för att begära registerutdrag, rättning eller invända mot behandling.

Förvaltningen hanterar stora mängder personuppgifter avseende barn som en del av sitt uppdrag där behandlingen sker via förvaltningens dedikerade verksamhetssystem. Det finns även väl definierade rutiner och policys för hur denna behandling ska genomföras på ett säkert sätt. För denna typ av behandling har det utförts en risk- och konsekvensanalys.

Det kan förekomma behandling av känsliga personuppgifter för egen personal i form av HR-relaterad data för anställda eller namn och födelsedag på anställdas barn i syfte till att hantera föräldraledighet. För dessa typer av behandlingar finns definierade processer för att säkerställa individens rättigheter.

Samtliga medarbetare inom förvaltningen ska genomgå utbildning inom dataskydd.

Bedömning

Säkerställer kommunen och bolagen att datasubjektens rättigheter tillgodoses genom erforderliga rutiner?

Ja

De granskade bolagen och förvaltningarna har i allt väsentligt rutiner för att tillgodose datasubjektens rättigheter.

Personuppgiftsbiträde

Revisionsfråga 4: Har kommunen och bolagen rutiner för de situationer där kommunen agerar personuppgiftsbiträde åt annan (inkl. hantering av tredje part)?

Kalmarhem AB

Personuppgiftsbiträde

Kalmarhem har inte identifierat någon personuppgiftsbehandling där de själva agerar personuppgiftsbiträde åt en annan organisation.

För de behandlingar där Kalmarhem har anlitat ett personuppgiftsbiträde finns biträdesavtal upprättade.

Socialförvaltningen

Personuppgiftsbiträde

Socialförvaltningen har identifierat personuppgiftsbehandlingar där de agerar personuppgiftsbiträde åt andra organisationer. För samtliga dessa behandlingar finns biträdesavtal upprättade. Förvaltningen har i vissa fall upplevt att det kan vara svårt att avgöra vem som är personuppgiftsansvarig och personuppgiftsbiträde. I dessa fall har ett bra stöd erhållits från dataskyddsombud.

För de behandlingar där Socialförvaltningen har anlitat ett personuppgiftsbiträde finns biträdesavtal upprättade.

Kalmar Vatten AB

Personuppgiftsbiträde

Kalmar Vatten har identifierat personuppgiftsbehandlingar där de agerar personuppgiftsbiträde åt andra organisationer. För samtliga dessa behandlingar finns biträdesavtal upprättade.

För de behandlingar där Kalmar Vatten har anlitat ett personuppgiftsbiträde finns biträdesavtal upprättade.

Utbildningsförvaltningen

Personuppgiftsbiträde

Utbildningsförvaltningen agerar inte personuppgiftsbiträde åt någon annan men är gemensamt personuppgiftsansvariga i vissa behandlingar, i dessa fall finns avtal på plats för att hantera förhållandet.

För de behandlingar där Utbildningsförvaltningen har anlitat ett personuppgiftsbiträde finns biträdesavtal upprättade.

Bedömning

Har kommunen och bolagen rutiner för de situationer där kommunen agerar personuppgiftsbiträde åt annan (inkl. hantering av tredje part)?

Ja

Endast Socialförvaltningen och Kalmar Vatten AB har identifierat personuppgiftsbehandlingar där de agerar personuppgiftsbiträde åt andra organisationer. I samtliga dessa fall finns erforderliga biträdesavtal upprättade.

Säkerhetsåtgärder och incidenthantering

Revisionsfråga 5: Har kommunen och bolagen adekvata säkerhetsåtgärder och en dokumenterad incidenthantering för att minska effekterna av personuppgiftsincidenter?

Kalmarhem AB

Säkerhetsåtgärder och incidenthantering

Bolaget utför och dokumenterar klassning av data för att säkerställa rätt skyddsnivå på ett strukturerat sätt. Vidare arbetar bolaget med behörighetsstyrning inom verksamhetens system för att säkerställa att endast rätt personer har behörighet. Behörighetshanteringen är dokumenterad och formaliserad.

Idag sker ingen regelbunden eller strukturerad uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder.

Bolaget har idag inte några formaliserade kontroller kring ostrukturerad data utöver utbildningsinsatser och viss automatik kopplat till att förhindra att personnummer skickas via e-post. Vid intervju framkom att det finns ett behov av att ytterligare kartlägga i vilken utsträckning personuppgifter förekommer i ostrukturerad data.

Det finns ett kommungemensamt system för att skicka personuppgifter på ett säkert sätt som används vid behov.

Det finns en formaliserad och dokumenterad process för incidenthantering tillsammans med en checklista specifikt för personuppgiftsincidenter. Gällande incidenter som sker hos ett personuppgiftsbiträde ansvarar dessa för att rapportera incidenterna vilket även framgår enligt avtal. Organisationen har inte identifierat några personuppgiftsincidenter av allvarlig karaktär som erfordrar rapportering till tillsynsmyndigheten.

Socialförvaltningen

Säkerhetsåtgärder och incidenthantering

Förvaltningen utför och dokumenterar klassning av data för att säkerställa rätt skyddsnivå på ett strukturerat sätt. Vidare arbetar förvaltningen med behörighetsstyrning inom verksamhetens system för att säkerställa att endast rätt personer har behörighet. Behörighetshanteringen är dokumenterad och formaliserad.

Idag sker ingen regelbunden eller strukturerad uppföljning, utöver den initiala bedömningen, av förvaltningens personuppgiftsbiträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder. Verksamheten uttrycker även under intervju att de finner det utmanande att göra denna typ av bedömning.

Verksamheten har som målsättning att ha så lite ostrukturerad data som möjligt men har idag inte några formaliserade kontroller kring ostrukturerad data utöver utbildningsinsatser och viss automatik kopplat till att förhindra att personnummer skickas via epost.

Det finns ett kommungemensamt system för att skicka personuppgifter på ett säkert sätt som används vid behov.

Det finns en formaliserad och dokumenterad process för incidenthantering. Därutöver finns även en dedikerad person som övervakar rapporterade avvikelser för att identifiera och rapportera personuppgiftsincidenter. Verksamheten har identifierat personuppgiftsincidenter av allvarligare karaktär som därmed rapporterats vidare till tillsynsmyndigheten. Vid dessa tillfällen har även dataskyddsombudet varit involverad eller informerad.

Kalmar Vatten AB

Säkerhetsåtgärder och incidenthantering

Bolaget utför och dokumenterar klassning av data för att säkerställa rätt skyddsnivå på ett strukturerat sätt. Vidare arbetar bolaget med behörighetsstyrning inom verksamhetens system för att säkerställa att endast rätt personer har behörighet. Behörighetshanteringen är dokumenterad och formaliserad.

Idag sker ingen regelbunden eller strukturerad uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder.

Bolaget har som ambition att inte behandla personuppgifter i ostrukturerad form men har idag inte några formaliserade kontroller kring ostrukturerad data utöver utbildningsinsatser och viss automatik kopplat till att förhindra att personnummer skickas via e-post.Det finns ett kommungemensamt system för att skicka personuppgifter på ett säkert sätt som används vid behov.

Det finns en formaliserad och dokumenterad process för incidenthantering för personuppgiftsincidenter. Gällande incidenter som sker hos ett personuppgiftsbiträde ansvarar dessa för att rapportera incidenterna vilket även framgår enligt avtal. Under intervju framkom att verksamheten känner viss osäkerhet kring bedömning av incidenter och vad som ska rapporteras vidare till tillsynsmyndigheten. Här efterfrågas ytterligare stöd från dataskyddsombudet i form av utbildning.

Organisationen har tidigare rapporterat incidenter till tillsynsmyndigheten utan att involvera dataskyddsombudet i processen.

Utbildningsförvaltningen

Säkerhetsåtgärder och incidenthantering

Förvaltningen utför och dokumenterar klassning av data för att säkerställa rätt skyddsnivå på ett strukturerat sätt. Vidare arbetar förvaltningen med behörighetsstyrning inom verksamhetens system för att säkerställa att endast rätt personer har behörighet. Behörighetshanteringen är dokumenterad och formaliserad. Dock framkom under intervjun att det har förekommit tillfällen då medarbetare som avslutar sin tjänst och påbörjar en ny tjänst i förvaltningen har haft kvar sina gamla behörigheter.

Idag sker ingen regelbunden eller strukturerad uppföljning, utöver den initiala bedömningen, av förvaltningens personuppgiftsbiträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder. Verksamheten uttrycker även under intervju att de finner det utmanande att göra denna typ av bedömning.

Verksamheten har etablerat en “digital städdag” där medarbetarna rensar ostrukturerad data. Till stöd för detta finns en framtagen mall för genomförandet. Utöver detta finns även utbildningsinsatser och viss automatik kopplat till att förhindra att personnummer skickas via e-post för att minska personuppgifter i ostrukturerat format. Det finns ett kommungemensamt system för att skicka personuppgifter på ett säkert sätt som används vid behov.

Det finns en formaliserad och dokumenterad process för incidenthantering. Dock noteras att det har skett incidenter som först har uppmärksammats av de registrerade vilket kan tyda på ett behov av ytterligare utbildning eller andra aktiviteter krävs för att motverka denna typ av incidenter. Vid dessa tillfällen har dataskyddsombudet blivit involverad.

Rapporterade personuppgiftsincidenter

Hur många rapporteringsskyldiga personuppgiftsincidenter har rapporterats till Datainspektionen/ Integritetsskyddsmyndigheten från år 2020 och framåt?

Kalmar kommun har endast statistik från och med maj 2021 då det införskaffades ett nytt rapporteringssystem. Sedan dess har de registrerat 46 stycken incidenter varav 19 stycken har rapporterats till tillsynsmyndigheten. Vid intervju med dataskyddsombudet framkom att det finns en kunskapsbrist inom detta område i flertalet förvaltningar och bolag. Detta kan medföra risk för att incidenter rapporteras felaktig eller att de inte rapporteras alls. Dataskyddsombudet rapporterar även vid behov personuppgiftsincidenter till kommunledningen.

Bedömning

Har kommunen och bolagen adekvata säkerhetsåtgärder och en dokumenterad incidenthantering för att minska effekterna av personuppgiftsincidenter?

Delvis

De granskade bolagen och förvaltningarna har i allt väsentligt dokumenterade rutiner för incidenthantering. Dock har granskningen visat på att det finns vissa brister i att upptäcka och att rapportera incidenter.

Vidare är det inget av de granskade bolagen eller förvaltningarna som genomför någon regelbunden eller strukturerad uppföljning, utöver den initiala bedömningen, av bolagets biträden för att säkerställa att de fortfarande har adekvata säkerhetsåtgärder.

Uppföljning

Revisionsfråga 6: Genomför dataskyddsombudet uppföljningar med förvaltningar och bolag för att säkerställa att de lever upp till GDPR och att eventuella åtgärder vid behov vidtas? (Exempel på större brister som framkommit vid uppföljningarna)

Dataskyddsombudet har lett ett antal uppföljningar gällande dataskydd under de senaste åren som även har mynnat ut i konkreta förbättringsåtgärder både centralt inom kommunen men även ute i förvaltningar och bolag. Det senaste arbetet avser en kartläggning av samtliga personuppgiftsbehandlingar som utförs med stöd av amerikanska molntjänstleverantörer som en följd av Schrems II (EU-domstolen domslut i mål C-311/18).

Utöver detta finns även etablerade forum där de olika bolagen och förvaltningarna samt dataskyddsombudet regelbundet träffas och diskutera dataskyddsfrågor med varandra. Dock saknas mer formaliserad rapportering eller självutvärdering från bolagen eller förvaltningarna till dataskyddsombudet. Vidare noteras att inga av de granskade bolagen

eller förvaltningarna själva har definierade formella kontroller för att säkerställa efterlevnad av kraven i förordning och mäter heller inte efterlevnad på annat något sätt.

Rollen som dataskyddsombud för kommunen har tilldelats till en av kommunjuristerna, som har många andra åtagande, vilket medfört vissa prioriteringar. Det har inte funnits tid till att genomföra ett proaktivt arbete i att säkerställa efterlevnad i det utsträckningen som skulle vara önskvärt. Det har även framkommit under intervjuer att en mer proaktiv tillsyn från dataskyddsombudet skulle välkomnas för att säkerställa ett bibehållet fokus på dataskydd och efterlevnad.

Förutom de utmaningar med tillgänglig tid, medför även den delade rollen som kommunjurist och dataskyddsombud en risk för självgranskning. Detta då rollen som kommunjurist kan förväntas aktivt medverka i aktiviteter som sedan dataskyddsombudet ska granska.

Bedömning

Genomför dataskyddsombudet uppföljningar med förvaltningar och bolag för att säkerställa att de lever upp till GDPR och att eventuella åtgärder vid behov vidtas? (Exempel på större brister som framkommit vid uppföljningarna)

Delvis

Uppföljning av efterlevnad utförs, dock saknas det idag tid och resurser för att bedriva ett mer proaktivt arbete. Detta då dataskyddsombud även är kommunjurist och tiden måste delas mellan dessa två roller. Denna delade tjänst medför även en risk för självgranskning. Vidare sker idag ingen formaliserad rapportering från förvaltningarna eller bolagen av sin efterlevnad till dataskyddsombudet.

2022-05-04

Jörn Wahlroth

Uppdragsledare

Peter Olby

Projektledare