Kommunstyrelsen
Kommunledningskontoret
Ledningsstab
Karin Winberg 016-710 80 49

Datum
2022-04-28

Diarienummer
KSKF/2022:105

Handlingsnummer
2022:1798

Kommunstyrelsen

Dataskyddsombudets årsrapport 2021 avseende dataskydd

Förslag till beslut

Årsrapport 2021 avseende dataskydd, för kommunstyrelsen och kommunen som helhet, godkänns.

Sammanfattning

Dataskyddsombudets årsrapport 2021 är en sammanfattande rapport för dataskydd inom vissa utvalda områden inom dataskyddet för hela Eskilstuna Kommun. Rapportens innehåll inkluderar vissa av dataskyddsombudets fokusområden för år 2021 men även annat.

Kommunstyrelsens beslut består av två delar, då rapporten från kommunens datasskyddsombud (DSO) omfattar:

- Kommunstyrelsen som egen myndighet och nämnd utifrån det ansvar som dataskyddsförordningen reglerar.
- Eskilstuna kommun som helhet och som är ett underlag för kommunstyrelsens uppsiktsplikt. Dessa rekommendationer är nedan markerade med ordet ”uppsiktsplikt”.

Kommunledningskontorets bedömer att dataskyddsombudets rekommendationer är relevanta och ska beaktas och sammanfattas enligt följande:

1. Kontroll av rätten till information (uppsiktsplikt). Rekommenderade åtgärder hanteras av SEF via central DSS-organisation.
2. Kontroll av rätten till tillgång, dvs begäran om registerutdrag. Rekommenderade åtgärder hanteras av Kommunledningskontoret.
3. Kontroll av förekomst av rutiner för de registrerades rättigheter (uppsiktsplikt). Rekommenderade åtgärder hanteras av SEF via central DSS-organisation.
4. Kontroll av förekomst av beslut som enbart grundas på automatiserad behandling. Idag förekommer inte detta, och ingen rekommendation har givits. Kommunledningskontoret beaktar dataskyddsförordningen i förekommande fall.

5. Information och rekommendationer avseende aktuella frågor. Rekommendationer hanteras av Kommunledningskontoret.

Ärendebeskrivning

Nedan presenteras DSO kontroller, resultat och rekommendationer samt KLK:s kommentarer åtgärder och information om ansvarig.

1. Kontroll av rätten till information, Artikel 13 och 14 (uppsiktsplikt)

Kontroll
I detta kontrollmoment har granskning gjorts av följande som gäller information till registrerade: • Om personal som anställs i kommunen får information enligt dataskyddsförordningen om hur deras personuppgifter behandlas och hur informationen är formulerad. • Information till övriga registrerade. Behandlingar som kräver att information lämnas till den registrerade enligt dessa artiklar och för vilka av dessa behandlingar information lämnas. Stickprov av innehåll i informationen har gjorts.
Resultat
Kommunen har information till registrerade på hemsidan. Denna behöver viss utveckling. Information till anställda om behandling av deras personuppgifter finns och är obligatorisk för all nyanställd personal att ta del av. Denna behöver dock utvecklas genom att göras mer detaljerad för att uppfylla kraven i dataskyddsförordningen. Vad gäller information till övriga registrerade så finns inom kommunen en stor variation av behandlingar av personuppgifter för olika ändamål. Det framkom vid stickprov att det förekommer brister både vad gäller om information lämnas och om informationen är komplett enligt dataskyddsförordningen.
Rekommendation
DSO rekommenderar att identifierade brister åtgärdas och att det säkerställs att övrig information som lämnas till registrerade uppfyller kraven i dataskyddsförordningen.
KLK kommentar, åtgärder, tid och ansvar
Under 2021 startades ett KLK-finansierat uppdrag med mål att vidareutveckla Eskilstuna kommuns arbete med dataskyddsfrågor. Uppdragets syfte var att genomföra förändringar för att skapa en tydligare organisation, ökad kunskap för

området, tydliggörande av roller och ansvar samt förbättrad uppföljning. I uppdragets andra fas (ännu ej genomfört) ingår att se över kommunöverskridande rutiner och information till allmänhet eller medarbetare inom kommunen. Ansvar för stöd, kunskapsgivning och kontroller vad avser kommunens respektive nämnd/förvaltning (PUA[1]) ingår i Serviceförvaltningens (SEF) ansvar.

Uppdragets andra fas kommer drivs i SEF:s regi, med stöd och uppföljning av KLK. I den andra fasen kommer DSO:s rekommendationer att omhändertas, dvs:

- Informationen till registrerade som finns på kommunens webbplats (eskilstuna.se) samt information till medarbetare om behandling av deras personuppgifter behöver utvecklas för att uppfylla kraven i dataskyddsförordningen.
- I övrigt vara ett stöd till organisationen i dylika frågor för att skapa en samstämmig och korrekt information till registrerade.

Färdigtid: 2022-12-31
Ansvarig: Enhetschef DSS SEF

2. Kontroll av rätten till tillgång, dvs begäran om registerutdrag, Artikel 15

Kontroll
Kontrollen har omfattat om det finns rutiner och andra dokument eller tjänster för registerutdrag. Frågor har även ställts kring antalet begäranden om registerutdrag och om de besvarats inom tiden eller om förlängd tid tillämpats samt vilken information som lämnats om behandlingen.
Resultat
Det finns en kommunövergripande rutin för registerutdrag (rätten till tillgång) och en mall för svar till registrerad. Viss mindre komplettering behövs. Det finns en blankett, på Eskilstuna Kommuns hemsida, som kan skrivas ut och fyllas i av den registrerade för begäran om registerutdrag. Svar har inte lämnats på alla frågeställningar.
Rekommendation
Då svar inte inkommit på alla punkter går det inte att bedöma om processen fungerar. Min rekommendation är därför att man säkerställer att den fungerar.
KLK kommentar, åtgärder, tid och ansvar
Hantering av inkommen begäran om registerutdrag är för KLK som förvaltning

[1] PUA = Personuppgiftsansvarig

inte dokumenterad i någon egen rutinbeskrivning. KLK använder samma stödmaterial som har tagits fram för kommunen i stort. Dock ser vi att rutinerna behöver tydliggöras för att kunna hantera begäran effektivt. KLK kommer därför att särskilt ombesörja att en rutinbeskrivning avseende registerförfrågan tas fram, för att säkra processen och för att minska tiden för hantering.

Färdigtid: 2022-08-31
Ansvarig: Administrativ direktör och Kommunstrateg informationssäkerhet, KLK

3. Kontroll av förekomst av rutiner för de registrerades rättigheter (uppsiktsplikt)

Kontroll
Kontrollen har gällt huruvida det finns rutiner för de registrerades rättigheter.
Resultat
Brister finns då vissa rutiner saknas och utveckling behövs därför inom detta område.
Rekommendation
DSO rekommenderar att de brister som finns vad gäller rutiner för de registrerades rättigheter åtgärdas. Kommunen avgör om rutinerna ska tas fram centralt och gälla för samtliga nämnder eller om varje nämnd ansvarar för sina. De rutiner som finns har tagits fram centralt.
KLK kommentar, åtgärder, tid och ansvar
I det uppdrag som påbörjades 2021 vidareutveckla Eskilstuna kommuns arbete med dataskyddsfrågor ingick i fas 2 att se över kommunöverskridande rutiner. Arbetet kommer att fortsätta under 2022, som ett uppdrag inom SEF (se kontroll 1 ovan), och följs upp av KLK. DSO:s rekommendation kommer att omhändertas i det arbetet, dvs: • Ta fram rutiner för de registrerades rättigheter. **Färdigtid:** 2022-12-31 **Ansvarig:** Enhetschef DSS SEF

4. Kontroll av förekomst av beslut som enbart grundas på automatiserad behandling, Artikel 22

Kontroll
Kontrollen av automatiserat beslutsfattande omfattade följande: • Om det förekommer automatiserat beslutsfattande inom kommunen • Om det i så fall inkluderar profilering • Vilka kategorier av personuppgifter som inkluderas • Vilken information den registrerade får om behandlingen och det automatiserade beslutsfattandet inför behandlingen. •
Resultat
DSO har inte kunnat finna att automatiserat beslutsfattande förekommer i kommunen.
Rekommendation
-
KLK kommentar, åtgärder, tid och ansvar
KLK noterar DSO:s belysande av artikel 22, dvs förekomst rörande automatiserat beslutsfattande. Om det blir aktuellt med automatiserat beslutsfattande i framtiden kommer dataskyddsförordningen tas i beaktande, för att skydda den registrerades rättigheter. **Ansvarig:** Processägare IT

5. Information och rekommendationer som rör aktuella frågeställningar mm

Information
5.1 Överföring av personuppgifter till tredje land I normalfallet är det olagligt att föra över personuppgifter till så kallat tredje land, det vill säga länder utanför EU och EES. Det krävs att det finns en grund och att vissa krav uppfylls så att de registrerade och deras personuppgifter får ett adekvat skydd. Om skyddet inte kan säkerställas är personuppgiftsansvarig skyldig att inte föra över personuppgifterna. Som överföring räknas även möjlighet till åtkomst från tredjeland. **5.2 Molnbaserade MS365** MS365 består av ett antal molnbaserade tjänster som inkluderar kontorsprogram i form av ordbehandling och kalkylering, e-post, digitala möten, lagring mm. Leverantör är Microsoft som är ett amerikanskt bolag som även verkar i stora delar av världen inkl i Europa. Eftersom ägandet finns i USA faller bolaget under amerikansk lagstiftning oavsett var informationen behandlas fysiskt, dvs även när information som tillhör en svensk kommun finns i datacentra inom EU/EES. Detta innebär bl a att myndigheter i USA har rätt att ta del av personuppgifterna med stöd i amerikanska lagar. Det

finns också lag som gör att myndigheterna kan förbjuda leverantören att meddela kommunen om att de lämnat över personuppgifterna. Både kommunen och den enskilde förlorar då kontrollen över personuppgifterna.

5.3 Dataskyddsombudets involvering i kommunen
För att dataskyddsförordningen ska efterlevas och de registrerades friheter och rättigheter ska skyddas är det viktigt att dataskyddsombudet kontaktas enligt kraven i dataskyddsförordningen.

Rekommendation

5.1 Överföring av personuppgifter till tredje land
DSO rekommenderar att nämnden följer Europeiska Dataskyddstyrelsens modell och endast påbörjar behandlingen om en objektiv analys visar att de registrerades personuppgifter ges ett adekvat skydd. Det är lämpligt att kontakta dataskyddsombudet för råd.

5.2 Molnbaserade MS365
DSO rekommenderar vidare att Eskilstuna Kommuns nämnder inte går över till att använda det molnbaserade MS365 under rådande omständigheter, dvs då det inte finns någon överenskommelse mellan EU/EES och USA som skyddar personuppgifterna, då personuppgifterna kan hamna hos amerikanska myndigheter och då det inte går att förhandla avtal samt ge instruktioner för att säkerställa att de registrerades personuppgifter skyddas.

5.3 Dataskyddsombudets involvering i kommunen
Slutligen rekommenderar DSO att dataskyddsombudet rådfrågas och hålls informerad enligt kraven i dataskyddsförordningen.

KLK kommentar

5.1 Överföring av personuppgifter till tredje land
23 oktober 2021 fattade kommunfullmäktige ett inriktningsbeslut rörande användning av molntjänster. Inriktningsbeslutets vilar på att kommunen i första hand ska använda inomeuropeiska molntjänster och om det inte är möjligt att information av karaktär öppen (0) eller intern (1) ska skyddas med adekvata skydd. KLK medverkar till beslutet genom att efterleva och bevaka att kommunfullmäktiges beslut efterlevs.
Ansvarig: Processägare IT

5.2 Molnbaserade MS365
I samband med licensförnyelse av MS365 (april 2022) beslutade KLK Kommunikationsdirektör att frysa allt utvecklingsarbete relaterat till MS365 molntjänster, men att kommunen behåller nuvarande nivå under det kommande året. Beslutet innebär bl.a. att kommunen behåller de tjänster som används idag (Teams, AD Azure och Microsofte In tune) ett år till. Piloten för MS365 som 100 personer testar ligger kvar. Den närmaste tiden behöver det säkras att kommunen minimerar

personuppgifter i de molntjänster som används. Det närmaste året kommer kommunen att se över alternativ till de molntjänstlösningar som vi redan gått in i, vilket innebär att vi kan gå till helt on-prembaserade tjänster 1 april 2023 och avveckla samtliga molntjänster om vi bedömer att det är lämpligt.
Ansvarig: Processägare IT

5.3 Dataskyddsombudets involvering i kommunen
KLK instämmer och verkar för att DSO ska rådfrågas och involveras i frågor som rör dataskyddsförordningen.
Ansvarig: Kommundirektören

Finansiering
Ärendet har inga finansiella konsekvenser.

Konsekvenser för hållbar utveckling och en effektiv organisation
De föreslagna åtgärderna som redovisas i ärendet syftar alla till att utveckla och förtydliga och säkerställa kommunens hantering av dataskyddsfrågor och bidrar därmed till en effektiv organisation.

Tommy Malm
Kommundirektör

Lena Lundberg
Administrativ direktör

Beslutet skickas till:

Dataskyddsombudets årsrapport för 2021 avseende dataskydd i Eskilstuna Kommun

Denna rapport är en sammanfattande rapport för dataskydd inom vissa utvalda områden inom dataskyddet för hela Eskilstuna Kommun. Det inkluderar vissa av årets fokusområden men även annat. Den tar inte upp dataskyddet hos enskilda nämnder. Årsrapporten innehåller rapportering från kontroller, information om dataskyddsförordningen och aktuella ämnen samt rekommendationer.

Fokusområden har under 2021 varit bl a de registrerades rättigheter, överföringar till tredje land samt nya system och tjänster inkl digitalisering.

Sammanfattning

Under 2021 utfördes kontroller som gäller de registrerades rättigheter. Dessa visade att:

- informationen till de registrerade om hur deras personuppgifter behandlas behöver viss utveckling
- brister finns vad gäller skriftliga rutiner, och utveckling på området behöver därför ske så att nämnderna kan tillgodose de registrerades begäran på ett korrekt när de vill utöva sina rättigheter
- det finns rutin och andra dokument för begäran av registerutdrag
- jag har inte kunnat finna att automatiserat beslutsfattande förekommer i kommunen

Ett ämne som är mycket aktuellt är huruvida personuppgifter får föras över till tredje land, dvs länder utanför EU/EES, och hur bedömningen ska göras. Ett vanligt land i sammanhanget är USA. Europeiska Dataskyddsstyrelsen har tagit fram en vägledning med en modell för hur verksamheterna behöver gå till väga i detta arbete. En objektiv analys av hur landets lagar och praxis påverkar den aktuella behandlingen krävs. Min rekommendation är att vägledningen följs och att överföring av personuppgifter inte påbörjas om den kan utgöra en risk för de registrerades fri- och rättigheter.

Microsofts molntjänst MS365 berörs av problematiken med tredjelandsöverföringar och är problematisk bl a pga USA:s lagar då dessa inte möjliggör det skydd för individens personuppgifter som dataskyddslagarna inom EU/EES. Personuppgifterna kan komma att begäras ut av amerikanska myndigheter med stöd av deras övervakningslagar. Även andra brister finns. Det går inte heller att förhandla avtal med

Microsoft eller ge dem instruktioner för att säkerställa att de registrerades personuppgifter skyddas. Min rekommendation är därför att Eskilstuna Kommuns nämnder inte går över till att använda det molnbaserade MS365 under nuvarande omständigheter.

För att dataskyddsförordningen ska efterlevas och de registrerades fri- och rättigheter ska skyddas är det viktigt att dataskyddsombudet kontaktas enligt kraven i dataskyddsförordningen, dvs att dataskyddsombudet rådfrågas i god tid i alla frågor som rör skyddet av personuppgifter och inför konsekvensbedömningar. I tider av digitalisering är detta extra viktigt då nya sorters digitala lösningar kan bli aktuella. Idag blir inte dataskyddsombudet rådfrågat helt enligt lagkrav. Min rekommendation är därför att dataskyddsombudet rådfrågas och hålls informerad enligt kraven i dataskyddsförordningen.

Dataskyddsförordningen

EU:s dataskyddsförordning (GDPR) gäller som lag i samtliga EU-länder, inklusive Sverige. Den har sina rötter i Europakonventionen om de mänskliga rättigheterna och finns till för att skydda enskildas (de registrerades) grundläggande rättigheter och friheter, särskilt deras rätt till privat- och familjeliv och skydd av personuppgifter. Syftet är även att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.

Varje behandling av personuppgifter behöver uppfylla dataskyddsförordningen och dess grundläggande principer. Dessa är i korthet att personuppgiftsansvarig:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- ska kunna visa att och hur de lever upp till dataskyddsförordningen.

Enligt dataskyddsförordningen har de registrerade rättigheter som innebär att de har rätt att t ex få information om hur deras personuppgifter behandlas och att de t ex kan få personuppgifter rättade och raderade, om ingen annan lag hindrar.

Kommunens personuppgiftsansvariga, dvs nämnderna, har ansvaret för att dataskyddsförordningen följs. Om nämnderna inte följer dataskyddsförordningen finns det en risk att enskildas personliga integritet utsätts för risker.

Dataskyddsombudets roll

Dataskyddsförordningen finns, som redan nämnts, för att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Därför finns det ett krav på att vissa organisationer, så som myndigheter, ska ha

dataskyddsombud. Dataskyddsombudets uppdrag är enligt artikel 39 att ge råd och information till organisationen om deras skyldigheter enligt förordningen och att övervaka efterlevnaden samt att vara kontaktpunkt för Integritetsskyddsmyndigheten, IMY (f.d. Datainspektionen) och registrerade. Ett led i övervakandet är att göra kontroller.

Dataskyddsombudet ska enligt artikel 38 utföra sitt arbete på ett oberoende sätt och får inte ges instruktioner av personuppgiftsansvarig om hur arbetet ska utföras. Det får inte heller straffas för att ha utfört sitt arbete. Dataskyddsombudet ansvarar inte för att dataskyddslagarna efterlevs i organisationen.

I dataskyddsombudets arbetsuppgifter ingår enligt artikel 39 att
”Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.”

Dataskyddsombudet rapporterar till nämnderna och det är i egenskap av rollen som dataskyddsombud som jag har skrivit denna årsrapport med rekommendationer för dataskydd.

Efterlevnad av regelverk för dataskydd gällande de registrerades rättigheter

Temat för årets kontroller har varit De registrerades rättigheter.

Dataskyddsförordningen är till för att skydda grundläggande rättigheter och friheter, särskilt enskildas rätt till skydd av sina personuppgifter och har sina rötter i Europakonventionen om de mänskliga rättigheterna. En av dessa rättigheter är individens rätt till respekt för sitt privat- och familjeliv och skydd av personuppgifter. Den innebär att ingen ska behöva utsättas för godtyckliga eller olagliga inskränkningar i sitt privatliv.

En central del i efterlevnaden av dataskyddsförordningen är att tillgodose de registrerades rättigheter. De registrerade är de personer vars personuppgifter behandlas hos Eskilstuna Kommun. De kan t ex vara brukare, elever, anhöriga, vårdnadshavare, anställda, kommuninvånare m fl. För att de registrerade ska ha insyn i hur deras personuppgifter behandlas och kunna påverka behandlingen av dem där så är möjligt finns ett antal rättigheter.

De rättigheter som de registrerade har enligt dataskyddsförordningen regleras i artiklarna 12–23 och är följande:

- Rätt till information om hur deras personuppgifter behandlas. (Art 13-14)
- Rätt till tillgång, dvs rätt att begära ut registerutdrag över personuppgifter och information kring behandlingen. (Art 15)
- Rätt att få felaktiga personuppgifter som rör honom eller henne rättade. (Art 16)

- Rätt att utan onödigt dröjsmål få sina personuppgifter raderade. Även kallat ”Rätten att bli bortglömd”. (Art 17 och 19)
- Rätt till begränsning av behandling. (Art 18 och 19)
- Rätt till dataportabilitet för att få ut sina personuppgifter eller få dem överförda till en annan organisation. (Art 20)
- Rätt att göra invändningar mot behandling. (Art 21)
- Rätt att inte bli föremål för automatiserat individuellt beslutsfattande, inbegripet profilering. (Art 22)

Möjligheterna för de registrerade att utöva dessa rättigheter begränsas i vissa fall av andra lagar i kommunen och det kan då göra att rättigheterna inte kan utövas. Till exempel går det inte att få sina personuppgifter raderade om det finns krav i annan lag på att de inte får raderas eller gallras förrän en viss tid har gått eller om de ska bevaras (arkiveras för all framtid).

Metod för kontrollerna

För att utföra kontrollerna har jag sänt formulär med frågor. Utifrån de svar jag har fått har jag sedan gjort stickprov för att granska informationstexter som lämnas till registrerade om hur deras personuppgifter behandlas. Även muntlig dialog har förekommit.

Då kontrollerna gjordes under hösten 2021 kan ev brister ha åtgärdats.

Kontroll av rätten till information, Artikel 13 och 14

Den registrerade har rätt att få information om behandlingen av deras personuppgifter. Vilken information som ska ges beror på om uppgifterna samlas in från de registrerade själva eller om den samlas in från någon annan. Den information som de redan förfogar över behöver inte lämnas.

Artikel 13: Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade.
Artikel 14: Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade.

Information som kan behöva lämnas är följande:

- varför deras uppgifter kommer att användas
- i vissa fall den rättsliga grunden till att behandla deras uppgifter
- hur länge deras uppgifter kommer att lagras
- vem som kommer att ta del av deras uppgifter
- deras rättigheter enligt dataskyddsförordningen
- om deras uppgifter kommer att överföras till ett så kallat tredjeland (land utanför EU/EES)
- deras rätt att lämna in klagomål
- hur de tar tillbaka sitt samtycke, om de har lämnat det, i de fall det är tillämpligt.
- kontaktuppgifterna till den organisation som ansvarar för att behandla deras uppgifter och till dess dataskyddsombud.

Kontroll

I detta kontrollmoment har granskning gjorts av följande som gäller information till registrerade:

- Om personal som anställs i kommunen får information enligt dataskyddsförordningen om hur deras personuppgifter behandlas och hur informationen är formulerad.
- Information till övriga registrerade. Behandlingar som kräver att information lämnas till den registrerade enligt dessa artiklar och för vilka av dessa behandlingar information lämnas. Stickprov av innehåll i informationen har gjorts.

Resultat

Kommunen har information till registrerade på hemsidan. Denna behöver viss utveckling.

Information till anställda om behandling av deras personuppgifter finns och är obligatorisk för all nyanställd personal att ta del av. Denna behöver dock utvecklas genom att göras mer detaljerad för att uppfylla kraven i dataskyddsförordningen.

Vad gäller information till övriga registrerade så finns inom kommunen en stor variation av behandlingar av personuppgifter för olika ändamål. Det framkom vid stickprov att det förekommer brister både vad gäller om information lämnas och om informationen är komplett enligt dataskyddsförordningen.

Rekommendation

Min rekommendation är att identifierade brister åtgärdas och att det säkerställs att övrig information som lämnas till registrerade uppfyller kraven i dataskyddsförordningen.

Kontroll av rätten till tillgång, dvs begäran om registerutdrag, Artikel 15

Den registrerade har rätt att vända sig till personuppgiftsansvariga som behandlar deras personuppgifter, för att få veta om personuppgifter behandlas eller inte. Om den registrerades personuppgifter behandlas har personen rätt till en kopia på uppgifterna och information om personuppgiftsbehandlingen. Några exempel ses nedan, men fullständig lista finns i artikel 15 i dataskyddsförordningen:

- vilka kategorier av personuppgifter som behandlas
- vilka personuppgifter som behandlas
- vad personuppgifterna används till
- hur länge uppgifterna kommer att sparas
- vilka personuppgifterna har delats med
- varifrån uppgifterna kommer.

Undantag från bestämmelsen finns t ex i annan lag och det finns även tillfällen då personuppgiftsansvarig kan avstå från begäran.

Kontroll
Kontrollen har omfattat om det finns rutiner och andra dokument eller tjänster för registerutdrag. Frågor har även ställts kring antalet begäranden om registerutdrag och om de besvarats inom tiden eller om förlängd tid tillämpats samt vilken information som lämnats om behandlingen.

Resultat
Det finns en kommunövergripande rutin för registerutdrag (rätten till tillgång) och en mall för svar till registrerad. Viss mindre komplettering behövs. Det finns en blankett, på Eskilstuna Kommuns hemsida, som kan skrivas ut och fyllas i av den registrerade för begäran om registerutdrag.

Svar har inte lämnats på alla frågeställningar.

Rekommendation
Då svar inte inkommit på alla punkter går det inte att bedöma om processen fungerar. Min rekommendation är därför att man säkerställer att den fungerar.

Kontroll av förekomst av rutiner för de registrerades rättigheter
Skriftliga rutiner är ett viktigt led i att efterleva dataskyddsförordningen. För att de registrerades rättigheter ska hanteras på ett korrekt sätt behöver det finnas rutiner för hur detta ska göras. Rutiner kan vara kommunövergripande, dvs samma rutiner gäller för hela kommunen, eller på nämndnivå. En rutin kan innehålla alla registrerades rättigheter eller så skrivs ett dokument per rättighet.

Kontroll
Kontrollen har gällt huruvida det finns rutiner för de registrerades rättigheter.

Resultat
Brister finns då vissa rutiner saknas och utveckling behövs därför inom detta område.

Rekommendationer
Min rekommendation är att de brister som finns vad gäller rutiner för de registrerades rättigheter åtgärdas. Kommunen avgör om rutinerna ska tas fram centralt och gälla för samtliga nämnder eller om varje nämnd ansvarar för sina. De rutiner som finns har tagits fram centralt.

Kontroll av förekomst av beslut som enbart grundas på automatiserad behandling, Artikel 22
Enligt dataskyddsförordningen ska den registrerade ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad

påverkar honom eller henne. Det innebär att det inte är någon person inblandad i beslutet.

Automatiserade beslut kan fattas med eller utan profilering. Omvänt kan profilering användas utan att det leder till ett automatiserat beslut. Profilering innebär varje form av automatisk behandling av personuppgifter då uppgifterna används för att bedöma vissa personliga egenskaper, i synnerhet för att analysera eller förutsäga personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Profilering är en behandling av personuppgifter som måste följa samtliga bestämmelser i dataskyddsförordningen.

Exempel på automatiserat beslutsfattande kan vara ett automatiserat avslag på en ansökan på internet eller vid ett nekande besked från e-rekrytering via internet utan personlig kontakt.

Den personuppgiftsansvariga måste informera de registrerade om att automatiserat beslutsfattande används enligt den generella informationsskyldigheten i förordningen. Om den personuppgiftsansvarige fattar automatiserade beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, måste den personuppgiftsansvarige:

- berätta för den registrerade att de tillämpar denna metod,
- lämna meningsfull information om den bakomliggande logiken, och
- förklara betydelsen och de förutsedda följderna av behandlingen.

Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för att ingå eller fullgöra ett avtal mellan den registrerade och den personuppgiftsansvariga eller om den registrerade har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning. Om det inte finns stöd i nationell lag är det inte tillåtet. Det finns inget stöd i kommunallagen för automatiserat beslutsfattande idag vilket gör att det inte är tillåtet för kommuner.

Kontroll

Kontrollen av automatiserat beslutsfattande omfattade följande:

- Om det förekommer automatiserat beslutsfattande inom kommunen
- Om det i så fall inkluderar profilering
- Vilka kategorier av personuppgifter som inkluderas
- Vilken information den registrerade får om behandlingen och det automatiserade beslutsfattandet inför behandlingen.

Resultat

Jag har inte kunnat finna att automatiserat beslutsfattande förekommer i kommunen.

Information och rekommendationer som rör aktuella frågeställningar mm

Överföring av personuppgifter till tredje land

I normalfallet är det olagligt att föra över personuppgifter till så kallat tredje land, det vill säga länder utanför EU och EES. Det krävs att det finns en grund och att vissa krav uppfylls så att de registrerade och deras personuppgifter får ett adekvat skydd. Om skyddet inte kan säkerställas är personuppgiftsansvarig skyldig att inte föra över personuppgifterna. Som överföring räknas även möjlighet till åtkomst från tredjeland.

Exempel på vad som räknas som överföring till tredje land:

- när man använder en systemleverantör, ett personuppgiftsbiträde, som lagrar kommunens personuppgifter på servrar i ett tredje land, eller inom EU men med åtkomst från tredje land för t ex support och systemutvecklare. Det kan gälla stora verksamhetssystem så väl som olika digitala tjänster videokonferens och vanliga kontorsprogram för t ex ordbehandling.
- när man har konsulter som har underbiträden med koppling till tredje land.
- när s k cookies, analysverktyg mm på webbsidor för över personuppgifter t ex i form av IP-adresser.
- När man skickar e-post med personuppgifter till ett tredje land.
- När myndigheter i tredje land begär ut eller samlar in personuppgifter, som fysiskt finns inom EU/EES, t ex i syfte att övervaka personer eller andra länder.

Europeiska Dataskyddsstyrelsen har tagit fram vägledningar för hur man behöver göra om man vill föra över personuppgifter till tredje land. De innehåller en modell för ett tillvägagångssätt som alla måste tillämpa för att pröva lagligheten och genomföra extra skyddsåtgärder. Varje personuppgiftsansvarig behöver göra sina analyser och fatta sina beslut. Analyserna måste vara objektiva.

Hänsyn till detta behöver tas i bl a projekt och upphandlingar då det idag är vanligt att leverantörer antingen ägs i tredje land eller har underbiträden som ägs i tredje land. Ett vanligt tredje land är USA. Analys och ställningstagande behövs inför varje behandling eller system som kommunen införskaffar. Om den objektiva analysen visar att personuppgifterna inte kan ges det skydd som krävs finns en skyldighet att inte påbörja behandlingen av personuppgifterna.

Dessa personuppgiftsbehandlingar behöver även uppfylla övriga delar i dataskyddsförordningen.

Personuppgiftsansvariga behöver även ha kännedom om överföring till tredje land förekommer idag och i så fall vidta lämpliga åtgärder.

Modellen innebär i korthet följande:

1. Kartlägg behandlingen och dess dataflöden. Hela kedjan behöver kartläggas. Ett biträde (leverantör av t ex molntjänst) kan ha flera underbiträden som levererar tjänster och även dessa kan i sin tur ha underbiträden som blir delaktiga. Dessa kan i

vissa fall finnas i olika länder vars lagstiftning påverkar möjligheterna att använda tjänsten och vilka åtgärder man behöver vidta om det ska bli möjligt.

Personuppgiftsansvarig måste också verifiera att de uppgifter som ska föras över är adekvata, relevanta och begränsade till vad som är nödvändigt i förhållande till de ändamål för vilka de behandlas.

2. Identifiera överföringsverktyg. Det finns ett antal sådan i dataskyddsförordningen som kan användas i olika överföringssituationer. Exempel är:

- Överföring på grundval av ett beslut av EU-kommissionen om adekvat skyddsnivå. Lista på länder finns.
- Standardavtalsklausuler som EU-kommissionen har beslutat om.
- Godkända uppförandekoder eller certifieringsmekanismer.
- Rättsligt bindande instrument mellan myndigheter.
- Undantag vid särskilda situationer enligt artikel 49.

Det vanligaste är standardavtalsklausuler när det gäller överföringar kopplade till molntjänster.

3. Bedöm om det finns något i det tredje landets lagar och/eller praxis som kan påverka effektiviteten av överföringsverktyget. En överföringsanalys (Transfer Impact Assessment) behöver göras och bedömningen måste vara objektiv. Den bör främst inriktas på tredjelands lagstiftning och praxis som är relevant för överföringen och det tilltänkta överföringsverktyget samt vilka konsekvenserna kan bli för den enskilde. Dokumentera bedömningen grundligt.

4. Identifiera och inför kompletterande skyddsåtgärder som är nödvändiga för att skyddsnivån för de data som överförs ska vara i väsentliga delar likvärdig med EU:s standard. Du behöver också genomföra denna bedömning av kompletterande åtgärder med tillbörlig aktsamhet och dokumentera den. Exempel på åtgärder kan vara viss typ av kryptering, pseudonymisering mm. Om det inte går att ge personuppgifterna adekvat skydd finns en skyldighet att inte påbörja behandlingen eller överföringen.

5. Vidta alla formella steg som behövs för att införa de kompletterande åtgärderna. Tillsynsmyndigheten, IMY, kan behöva rådfrågas om några av dem.

6. Omvärdera med lämpliga intervall skyddsnivån för de personuppgifter som förs över till tredje land och övervaka om det har funnits eller kommer att finnas någon utveckling som kan påverka den. Principen om ansvarsskyldighet kräver kontinuerlig vaksamhet om skyddsnivån för personuppgifter. Nya skyddsåtgärder kan behöva införas och om det inte är tillräckligt finns en skyldighet att sluta föra över personuppgifter.

Överföring av personuppgifter till USA

Ett av de vanligaste tredjeländerna är USA då leverantörer av tjänster och system eller deras underbiträden ofta ägs i USA. I och med att de ägs i USA omfattas de av USA:s lagar, och myndigheter i USA kan med stöd av övervakningslagar ta del av europeiska

personuppgifter som behandlas i amerikanska tjänster även när personuppgifterna befinner sig fysiskt inom EU.

Den 16 juli 2020 kom en dom från EU-domstolen som sa att Privacy Shield hade ogiltigförklarats. Privacy Shield var en överenskommelse mellan EU och USA som gjorde det lagligt att föra över personuppgifter till anslutna företag i USA. De anslöt sig via självcertifiering. En liknande överenskommelse fanns längre tillbaka och även den blev ogiltigförklarad. Detta innebär att det inte längre är tillåtet för personuppgiftsansvariga i EU att föra över personuppgifter till mottagare i USA med Privacy Shield som grund. Anledningen är att USA:s övervakningslagar inte stämmer överens med EU:s integritetslagar. Detta gör att det i nuläget är svårt att finna ett lagligt sätt att föra över personuppgifter.

EU-domstolen ansåg däremot att Kommissionens beslut om standardavtalsklausuler är giltigt och att sådana kan användas vid överföring till länder utanför EU och EES men att det i samband med användandet av dem i sin nuvarande form kan behövas ytterligare skyddsåtgärder. Så är fallet om mottagarlandet genom sin lagstiftning eller praxis inte kan anses ha en i allt väsentligt likvärdig skyddsnivå för uppgifterna som inom EU och EES. Dessa gäller inte för ett specifikt land. Det är varje personuppgiftsansvarigs ansvar att säkerställa att det blir lagligt. Europeiska Dataskyddsstyrelsen har tagit fram en vägledning. Se ovan. All överföring till tredje länder kräver att personuppgiftsansvarig gör noggranna objektiva analyser.

Europakommissionen håller på att förhandla med USA för att hitta ett sätt att föra över personuppgifter som ger de registrerade det skydd som krävs. När eller om detta kommer att lyckas är okänt.

Det är idag inte möjligt att föra över personuppgifter i klartext till USA.

Rekommendation inför planerad överföring till tredje land

Min rekommendation är att nämnden följer Europeiska Dataskyddstyrelsens modell och endast påbörjar behandlingen om en objektiv analys visar att de registrerades personuppgifter ges ett adekvat skydd. Det är lämpligt att kontakta dataskyddsombudet för råd.

Microsofts MS365

MS365 består av ett antal molnbaserade tjänster som inkluderar kontorsprogram i form av ordbehandling och kalkylering, e-post, digitala möten, lagring mm. Leverantör är Microsoft som är ett amerikanskt bolag som även verkar i stora delar av världen inkl i Europa.

Eftersom ägandet finns i USA faller bolaget under amerikansk lagstiftning oavsett var informationen behandlas fysiskt, dvs även när information som tillhör en svensk kommun finns i datacentra inom EU/EES. Detta innebär bl a att myndigheter i USA har rätt att ta del av personuppgifterna med stöd i amerikanska lagar. Det finns också lag som gör att myndigheterna kan förbjuda leverantören att meddela kommunen om

att de lämnat över personuppgifterna. Både kommunen och den enskilde förlorar då kontrollen över personuppgifterna. USA har ingen motsvarighet till dataskyddsförordningen och ger inte europeiska medborgare samma rättigheter som de har inom EU/EES, vilket utgör en risk för individen. Det finns t ex ingenstans de kan vänd sig för att lämna klagomål om de drabbas.

De personer vars personuppgifter kommunen behandlar står ofta i beroendeställning till kommunen och då kommunen tillhandahåller viktiga samhällsfunktioner samt är en stor arbetsplats kan de inte välja bort att få sina personuppgifter behandlade. Det gäller t ex brukare av olika kategorier, elever, personal m fl. Det går inte att avtala bort amerikanska myndigheters påverkan.

I normalfallet ger personuppgiftsansvariga instruktioner till leverantören, dvs personuppgiftsbiträdet, om hur det får behandla personuppgifter. När det gäller Microsoft har det hittills inte varit möjligt att ge dem instruktioner kring hur de får behandla personuppgifterna eller förhandla innehållet i avtalen. Ett fåtal organisationer i EU har lyckats. Detta gör att det inte går att ha tillräcklig kontroll och efterleva dataskyddsförordningen när tjänsterna används.

Rekommendation

Min rekommendation är att Eskilstuna Kommuns nämnder inte går över till att använda det molnbaserade MS365 under rådande omständigheter, dvs då det inte finns någon överenskommelse mellan EU/EES och USA som skyddar personuppgifterna, då personuppgifterna kan hamna hos amerikanska myndigheter och då det inte går att förhandla avtal samt ge instruktioner för att säkerställa att de registrerades personuppgifter skyddas.

Dataskyddsombudets involvering i kommunen

För att dataskyddsförordningen ska efterlevas och de registrerades friheter och rättigheter ska skyddas är det viktigt att dataskyddsombudet kontaktas enligt kraven i dataskyddsförordningen:

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. (Artikel 38.1)
- Den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd. (Artikel 35.2)

I tider av digitalisering är detta extra viktigt då nya sorters digitala lösningar kan bli aktuella och tidigare manuella processer kan komma att digitaliseras. Detta ställer höga krav på dataskyddsarbetet och de analyser som behöver göras.

Dataskyddsombudet behöver också kännedom om vad som är på gång för att kunna utföra sina arbetsuppgifter genom att övervaka, ge råd och informera personuppgiftsansvariga utifrån dataskyddslagarna. Kontakt med dataskyddsombudet

behöver tas mycket tidigt; redan när det finns en idé om vad man vill göra. Idag blir inte dataskyddsombudet rådfrågat helt enligt lagkrav.

Rekommendation

Min rekommendation att dataskyddsombudet rådfrågas och hålls informerad enligt kraven i dataskyddsförordningen.

Dataskyddsombudets arbete i kommunen under 2021

Under 2021 har arbetet bestått av bl a följande:

- Rapporterat om dataskyddet till nämnder och förvaltningschefer.
- Stöd i frågor om dataskydd i korta så väl som mer tidskrävande ärenden.
- Givit råd och övervakat vid dataskyddsarbete på kommunövergripande nivå och nämndnivå. T ex i upphandlingar och projekt, samt vid framtagande av styrande dokument.
- Skrivit olika informationsdokument och checklistor om behandling av personuppgifter utifrån dataskyddsförordningen.
- Tagit fram mallar.
- Skrivit nyhetsbrev.
- Informerat om dataskydd.
- Omvärldsbevakat.
- Förmedlat omvärldsbevakning till berörda i kommunen.
- Utfört kontroller.
- Genomfört utbildningar för nyckelpersoner.
- Svarat på frågor från registrerade.
- Hållit mig uppdaterad inom dataskyddsområdet genom att delta i utbildningar, webbinarier och konferenser.
- Sammankallat till nätverksmöten med övriga i kommunens dataskyddsorganisation.
- Deltagit i nätverksmöten för DSO:er.

Servicenämnden
Serviceförvaltningen
Planeringsenheten
Charlotte Nilsson, 016-710 30 79

Dataskyddsombudets årsrapport 2021 avseende dataskydd

EU:s dataskyddsförordning (GDPR) gäller som lag i samtliga EU-länder, inklusive Sverige. Den har sina rötter i Europakonventionen om de mänskliga rättigheterna och finns till för att skydda enskildas (de registrerades) grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Varje behandling av personuppgifter behöver uppfylla dataskyddsförordningen och dess grundläggande principer.

Det finns krav i förordningen att vissa typer av organisationer, så som kommuner måste ha ett dataskyddsombud som är en oberoende roll med uppdraget att ge råd och informera utifrån dataskyddsförordningen och övervaka att organisationen följer den.

Kommunens personuppgiftsansvariga, dvs nämnderna, har ansvaret för att dataskyddsförordningen följs.

Som dataskyddsombud rapporterar jag till samtliga 14 nämnder om dataskyddet och uppfyllandet av dataskyddsförordningen samt övriga bestämmelser som gäller skyddet av personuppgifter. Innehållet är avgränsat enligt nedan och inte en fullständig rapport över allt som gjorts inom dataskydd under året.

Gången för årsrapporteringen är följande:

- I mitten av januari lämnas årsrapporten för föregående år till förvaltningschef för genomläsning.
- Under andra halvan av januari samt under februari genomförs dialog om innehållet i rapporten mellan förvaltningschef och dataskyddsombud då innehållet diskuteras och förvaltningschef har möjlighet att lämna sina synpunkter. Vid detta tillfälle diskuteras även vad som är på gång i förvaltningen under 2021 som dataskyddsombudet behöver ha med i sin plan.
- I mars lämnas årsrapporten inför april månads nämndsammanträde, utifrån nämndernas tidsplan.
- Under april går rapporten upp på nämndsammanträde.

- Nämnden har möjlighet att lämna ett svar men det är inget formellt steg och är valfritt.

Samma rapport lämnas till samtliga nämnder och innehåller:

- Resultatet av gjorda kontroller under 2021.
- Rekommendationer utifrån gjorda kontroller och observationer.
- Behov inom dataskyddsområdet.

Med vänlig hälsning

Charlotte Nilsson
Dataskyddsombud