Kommunstyrelsen
Kommunledningskontoret
Ledningsstaben
Saba Yousif

Datum
2023-04-03

Diarienummer
KSKF/2023:118

Handlingsnummer
2023:1281

Kommunstyrelsen

Dataskyddsombudets årsrapport 2022 avseende dataskydd

Förslag till beslut

Årsrapport 2022 avseende dataskydd i Eskilstuna kommun godkänns.

Sammanfattning

Dataskyddsombudets årsrapport 2022 är en sammanfattande rapport för dataskydd inom vissa utvalda delar inom dataskyddsområdet för hela Eskilstuna kommun. Rapporten 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.

Ärendebeskrivning

Under 2022 utfördes kontroller som rör överföring av personuppgifter till länder utanför EU/EES.

Följande kontroller utfördes:

- Kontroll av arbetet med befintliga överföringar till tredje land efter ogiltigförklarandet av Privacy Shield.
- Kontroll av efterlevnad av beslutet i kommunfullmäktige gällande informationslagring i molntjänster.

Kontrollerna visade att:

- Kommunen har, efter att Privacy Shield ogiltigförklarades, bedrivit en del arbete för att inventera och kartlägga förekomsten av personuppgiftsbehandlingar med överföring av personuppgifter till tredjeland. Arbetet är dock inte klart.
- En vilja finns att följa beslutet i kommunfullmäktige och dataskyddsförordningen men brister finns på området och det finns även svårigheter med att förstå innebörden av beslutet.

Dataskyddsombudet rekommenderar att:

- Eskilstuna Kommun fortsätter, och slutför, arbetet med att kartlägga personuppgiftsbehandlingar och hantera identifierade brister för att säkerställa

att personuppgifter inte förs över till tredje land på ett olagligt sätt, samt att kommunen arbetar på ett korrekt sätt med anskaffning av molntjänster, gör objektiva analyser och ger personuppgifterna ett tillräckligt starkt skydd så att de registrerades friheter och rättigheter skyddas.
- Dataskyddsombudet rådfrågas och hålls informerad enligt kraven i dataskyddsförordningen

Kommunledningskontorets bedömer att dataskyddsombudets rekommendationer är relevanta och föreslår mot denna bakgrund att kommunstyrelsen godkänner Årsrapport 2022 avseende dataskydd i Eskilstuna kommun.

Finansiering

Ärendet har inga finansiella konsekvenser.

Konsekvenser för hållbar utveckling och en effektiv organisation

De föreslagna åtgärderna som redovisas i rapporten syftar till att utveckla, förtydliga och säkerställa kommunens hantering av dataskyddsfrågor och bidrar därmed till en effektiv organisation.

KOMMUNLEDNINGSKONTORET

Tommy Malm
Kommundirektör

Jannicke Patricny
Tf administrativ direktör

———

Beslutet skickas till:
Dataskyddsombudet

Servicenämnden
Serviceförvaltningen
Planeringsenheten
Charlotte Nilsson, 016-710 30 79

Dataskyddsombudets årsrapport för 2022 avseende dataskydd i Eskilstuna Kommun

Denna rapport är en kommunövergripande rapport över dataskydd i samtliga nämnder, utan att gå in på dataskyddet i enskilda nämnder.

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 och inte en fullständig rapport över allt som gjorts inom dataskydd under året.

Gången för årsrapporteringen är följande:

- I januari lämnades årsrapporten för föregående år till förvaltningschef för genomläsning.
- Under februari genomfördes dialog om innehållet i rapporten mellan förvaltningschef/direktörer och dataskyddsombud då innehållet diskuterades och det fanns möjlighet att lämna sina synpunkter. Vid detta tillfälle diskuteras även vad som är på gång i förvaltningen under 2023 som dataskyddsombudet behöver ha med i sin plan.

- I mars lämnades årsrapporten inför april månads nämndsammanträde, utifrån nämndernas tidsplan.
- Under april går rapporten upp på nämndsammanträde.
- Rapporten innehåller rekommendationer till nämnden och nämnden har möjlighet att lämna ett svar.

Samma rapport lämnas till samtliga nämnder och innehåller:

- Resultatet av gjorda kontroller under 2022.
- Rekommendationer utifrån gjorda kontroller och uppföljning av tidigare rekommendation.
- Information.

Med vänlig hälsning

Charlotte Nilsson
Dataskyddsombud

Dataskyddsombudets årsrapport för 2022 avseende dataskydd i Eskilstuna Kommun

Denna rapport är en sammanfattande rapport för dataskydd inom vissa utvalda delar inom dataskyddsområdet 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.

Sammanfattning

Under 2022 utfördes kontroller som rör överföring av personuppgifter till länder utanför EU/EES, det vill säga så kallade tredje länder.

Följande kontroller har gjorts:

- Kontroll av arbetet med befintliga överföringar till tredje land efter ogiltigförklarandet av Privacy Shield
- Kontroll av efterlevnad av beslutet i kommunfullmäktige gällande informationslagring i molntjänster

Kontrollerna visade att:

- Visst arbete med att inventera och kartlägga förekomsten av personuppgiftsbehandlingar med överföring av personuppgifter till tredjeland har gjorts efter att Privacy Shield ogiltigförklarades. Arbetet är dock inte klart.
- En vilja finns att följa beslutet i Kommunfullmäktige och dataskyddsförordningen men brister finns på området och det finns även svårigheter med att förstå innebörden av beslutet.

Mina rekommendationer är att Eskilstuna Kommun fortsätter och slutför arbetet med att kartlägga personuppgiftsbehandlingar och hantera identifierade brister för att säkerställa att personuppgifter inte förs över till tredje land på ett olagligt sätt, samt att man arbetar på ett korrekt sätt med anskaffning av molntjänster, gör objektiva analyser och ger personuppgifterna ett tillräckligt starkt skydd så att de registrerades friheter och rättigheter skyddas.

Rekommendationen att involvera dataskyddsombudet enligt dataskyddsförordningen har följts upp och resultatet är att även om man i vissa delar har ökat involveringen så har involveringen inte ökat i stort. Rekommendationen har därför inte följts.

Rekommendationen är därför åter igen att dataskyddsombudet rådfrågas och hålls informerad enligt kraven i dataskyddsförordningen.

Molntjänster och risken för överföring av personuppgifter till länder utanför EU/EES är ett ständigt aktuellt ämne inom dataskyddet. Tillsynsmyndigheterna inom EU har under 2022 gjort en gemensam aktion där de har undersökt hur offentliga myndigheter använder molntjänster och den 17 januari i år publicerade Europeiska Dataskyddstyrelsen sin rapport med information och rekommendationer. De skriver i rapporten att det med hänsyn till att offentliga myndigheter kan behandla personuppgifter av känslig karaktär och att det kan förekomma stora mängder uppgifter så är det väsentligt att den grundläggande rätten till skydd av personuppgifter garanteras av alla offentliga myndigheter. EDPB understryker därför behovet av att offentliga myndigheter agerar i full överensstämmelse med GDPR när de använder molnbaserade produkter eller tjänster.

Innehåll

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.

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." Ett led i övervakandet är att göra kontroller.

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

Bakgrund till kontrollerna

Då dataskyddsförordningen endast gäller för länder inom EU och EES försvåras behandling av personuppgifter när en organisation vill behandla personuppgifter i IT-system och andra digitala lösningar där det finns en koppling så som ägande, leverantörer eller underleverantörer i länder utanför EU och EES. Personuppgiftsansvarig, dvs nämnden, har då ett ansvar för att säkerställa att dataskyddsförordningen efterlevs och att det inte finns risker för de personer vars personuppgifter behandlas vare sig det gäller personal, brukare, elever eller andra personer.

Ämnet överföring till tredje land lyftes upp på agendan för samtliga organisationer inom EU och EES i samband med en dom i EU-domstolen i juli 2020 när den överföringsmekanism som möjliggjorde överföring till USA ogiltigförklarades. Det är dock inget nytt utan är även sedan tidigare något som har behövt beaktas vid behandling av personuppgifter och dokumentation behöver finnas kring de överföringar som görs.

Kontrollen är uppdelad i två delar:

- Kontroll av efterlevnad av dataskyddsförordningen vad gäller överföring av personuppgifter till tredje land och arbetet med personuppgiftsbehandlingarna utifrån EDPB:s riktlinjer efter att Privacy Shield blev ogiltigförklarat 200716.
- Kontroll av efterlevnad av inriktningsbeslutet kring molntjänster i kommunfullmäktige i november 2021.

Överföring av personuppgifter till tredje land

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

"Överföring av personuppgifter till tredje land är som regel när personuppgifter görs tillgängliga för någon i ett land utanför EU/EES-området", skriver IMY på sin webb.

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.

IMY ger följande exempel på överföring av personuppgifter till tredje land:

- När ni skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES.
- När ni anlitar ett personuppgiftbiträde i ett land utanför EU/EES.
- När ni ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När ni lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.
- När ni lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.

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.

Länk till GDPR Kapitel V, Artiklarna 44-49:
Kapitel V – Överföring av personuppgifter till tredjeländer eller internationella organisationer

Ogiltigförklarandet av Privacy Shield

Ett av de vanligaste tredjeländerna är USA då det är vanligt att leverantörer av tjänster och system eller deras underbiträden ägs i USA. I och med att ägandet finns 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/EES.

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 vända 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.

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. Europeiska medborgare som inte är USA-medborgare har inte samma fri- och rättigheter i USA som inom EU/EES och inte heller samma fri- och rättigheter som medborgare i USA har. 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 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. All överföring till tredje länder kräver att personuppgiftsansvarig gör noggranna objektiva analyser. Det räcker inte att komma till slutsatsen att risken är låg för de registrerade om åtkomst till dem blir möjlig från tredje land eftersom överföringen ändå inte blir laglig så länge åtkomst finns.

Europakommissionen har förhandlat med USA för att hitta ett sätt att föra över personuppgifter som ger de registrerade det skydd som krävs. USA:s president Biden skrev under en ”Executive Order” som en del av implementeringen av den politiska principöverenskommelse om ett nytt transatlantiskt ramverk för skydd av personuppgifter, Trans-Atlantic Data Privacy Framework, vilken träffades mellan EU-kommissionen och USA den 25 mars 2022. EU-kommissionen publicerade i slutet av 2022 ett utkast till beslut om adekvat skyddsnivå för USA. Europaparlamentet och Europeiska Dataskyddsstyrelsen, EDPB, har yttrat sig över utkastet till beslut och de var kritiska till flera delar. Frågan ska också behandlas i den så kallade Artikel 93-kommittén (som består av företrädare för medlemsstaternas regeringar). Adekvansbeslutet kan finnas till sommaren. Detta löser dock inte alla problem med alla molntjänster från USA utan man måste även säkerställa att hela behandlingen uppfyller dataskyddsförordningen. Det är därför ingen snabb lösning utan handlar om mycket mer än tredjelandsöverföringar. Det kan dessutom förekomma överföring till fler länder och dessa behöver då också analyseras och hanteras.

Innan ett adekvansbeslut är på plats är det inte möjligt att föra över personuppgifter i klartext till USA. Med överföring menas både att skicka personuppgifterna till USA eller att göra personuppgifterna åtkomliga för personer i USA när de lagras inom EU/EES.

Efter domen uppmanades alla organisationer att påbörja ett arbete med att se över de personuppgiftsbehandlingar som innebar en överföring till USA. EDPB publicerade efter en tid rekommendationer för arbetet med överföringar till tredje land och de gäller oavsett vilket tredje land man planerar att föra över personuppgifter till.

Det som behövde göras var att göra följande aktiviteter:

- Inventera tredjelandsöverföringarna. Kartlägg alla behandlingar av personuppgifter som innebär en överföring av personuppgifter till USA, genom att titta på personuppgiftsbiträdet och alla led av under biträden, tredjepartstjänster mm och hur personuppgifterna flödar genom tjänsterna.

- Identifiera vilka behandlingar som gjordes med Privacy Shield som grund.
- Se över övriga behandlingar med överföring till tredje land. Se så att de har en giltig grund för överföring. Används t ex standardavtalsklausuler?
- Finns tillräckliga extra skyddsåtgärder för att förhindra att personuppgifter kommer i orätta händer?
- Föra dialog med leverantörer och fråga dem hur de kommer att lösa det.
- Ta fram en handlingsplan för att följa de sex stegen i EDPB:s riktlinje
- Se över om det finns några behandlingar som kan avslutas.
- Dokumentera era bedömningar, vad som gjorts, vilka beslut som fattats inkl motiveringar.
- Åtgärda identifierade brister.

Europeiska Dataskyddsstyrelsens rekommendationer för överföringar till tredje land

Europeiska Dataskyddsstyrelsen, EDPB, har tagit fram rekommendationer 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 anskaffar. Om den objektiva analysen visar att personuppgifterna inte kan ges det skydd som krävs finns en skyldighet att inte påbörja behandlingen av personuppgifterna. Även befintliga överföringar behöver analyseras och dokumenteras enligt modellen.

En sammanfattning av modellen presenteras nedan.

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 tekniska (t ex kryptering) och organisatoriska (t ex rutiner) säkerhetsåtgärder samt lydelser i kontrakt. Det som skrivs in i kontrakt räcker dock inte utan andra typer av åtgärder behövs också, t ex 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.

EDPB:s dokument finns nedan.

EDPB:s rekommendationer om modell för det arbete som behöver göras om en organisation planerar att föra över personuppgifter till ett tredje land:
Länk till EDPB:s Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter Version 2.0 Antagna den 18 juni 2021

EDPB:s rekommendationer om extra skyddsåtgärder vid överföring till ett tredje land:
Länk till EDPB:s Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder

EDPB:s riktlinjer för undantag vid särskilda situationer:
Länk till EDPB:s Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679

EDPB:s riktlinjer för vad som är en överföring till tredje land (ej slutligt godkänd än):
Länk till EDPB:s Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

Beslutet i kommunfullmäktige om informationslagring i molntjänster

I oktober 2021 fattade kommunfullmäktige beslut om informationslagring i molntjänster. Det sammanfattas i följande punkter som finns i beslutet:

1. Eskilstuna kommun ska i första hand använda inomeuropeiska molntjänster för informationslagring.
2. Där inomeuropeiska alternativ ej finns kan information på skyddsnivå 0 och 1 lagras i molntjänster som lyder under lagstiftning från tredje land, förutsatt att organisationen vidtagit tekniska och organisatoriska åtgärder för att minimera risker med röjande av information.
3. Personuppgifter som lagras för IT-drift ska minimeras till så få som möjligt och får inte vara känsliga eller anses särskilt skyddsvärda. Inga andra personuppgifter än de som anses nödvändiga för att upprätthålla IT-driften av tjänsten ska hanteras i molntjänsten.
4. Vid införande av tjänster som innebär informationslagring i molntjänster från tredje land ska en riskanalys och vid behov en konsekvensbedömning göras och personuppgiftsansvarig nämnd ska fatta beslut om införande.
5. Kommunstyrelsen får i uppdrag att följa utvecklingen nationellt och internationellt avseende informationslagring i molntjänster från tredje land och vid behov vidta nödvändiga åtgärder.

Dokumenten i sin helhet finner du här:

Länk till beslut

Länk till beslutsunderlag

Eskilstuna kommuns efterlevnad av GDPR gällande överföring till tredje land

Temat för årets kontroller har gällt överföring av personuppgifter till tredje land.

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.

Följande kontroller har gjorts:

- Kontroll av arbetet med befintliga överföringar till tredje land efter ogiltigförklarandet av Privacy Shield
- Kontroll av efterlevnad av beslutet i kommunfullmäktige gällande informationslagring i molntjänster

Metod för kontrollerna

För att utföra kontrollerna har jag sänt formulär med frågor till samtliga förvaltningar. Resultatet baseras även på observationer som gjorts.

Då svar på frågorna inhämtades under hösten 2022 kan brister ha åtgärdats efteråt.

Svar har inte lämnats av alla förvaltningar.

Kontroll av arbetet med befintliga överföringar till tredje land efter ogiltigförklarandet av Privacy Shield

Kontroll

Kontrollen innebar en granskning av hur långt Eskilstuna Kommun har kommit i sitt arbete med att inventera eventuella överföringar till tredje land, analysera dem och säkerställa att överföringarna är lagliga, utifrån Europeiska Dataskyddsstyrelsens modell.

I kommunen finns IT-system, digitala tjänster och appar som används för behandling av personuppgifter. Vissa används av samtliga nämnder, andra används av några nämnder och en del används endast av en nämnd. Även konsulter behandlar personuppgifter. Detta gör att även om en nämnd har kontroll över sina egna behandlingar så kan det vara svårt att ha den kontrollen när anskaffningen görs centralt i kommunen.

Resultat

Resultatet som redogörs för är en sammanfattning av helheten för Eskilstuna Kommun.

Ett arbete med att inventera och kartlägga eventuella överföringar till tredje land och huruvida Privacy Shield eller annan grund för överföringen finns påbörjades 2020 och visst arbete med att arbeta enligt Europeiska Dataskyddsstyrelsens modell har gjorts. Vissa behandlingar har kartlagts och analyserats, dialog med vissa leverantörer har gjorts och man har avstått från att använda vissa tjänster eller system som ett resultat av arbetet.

Arbetet enligt Europeiska Dataskyddsstyrelsens modell är dock inte klart vilket innebär att det finns brister i dokumentation av personuppgiftesbehandlingar och därmed i kontrollen över personuppgifter som behandlas.

Utmaningar

Det finns utmaningar med det arbete som har gjorts och som behöver fortsätta. Molntjänster och appar kan vara komplext uppbyggda med underbiträden och

tredjepartstjänster i flera länder. Även dessa kan i sin tur ha underbiträden i flera led. Att göra en inventering och kartläggning av informationsflödena för att finna ut om personuppgifter förs över till tredje land och att de har ett tillräckligt skydd, kräver tid och kunskap hos de som gör arbetet och leverantörer som bidrar med korrekta svar.

Även om man vid upphandling av en digital tjänst har rett ut hur informationen flödar och konstaterat att en överföring till ett tredje land inte sker så kan detta ha ändrats under avtalstiden. Personuppgiftsbiträdet (leverantören) ska i dessa fall informera om detta. Om det gäller användande av nytt underbiträde (underleverantör) så ska dessutom personuppgiftsansvarig ha möjlighet att besluta om de godkänner underbiträdet för behandling av personuppgifter. Detta förutsätter att biträdet har kunskap om vad som utgör en överföring till tredje land och här finns idag brister då det fortfarande finns biträden som inte förstått t ex att möjlighet till åtkomst till uppgifter från ett tredje land, t ex USA, som lagras inom EU/EES räknas som en överföring. Det är vanligt att de som svar på en fråga om överföring till tredje land säger att informationen lagras inom EU/EES, vilket inte är ett svar på om det förekommer en överföring. Om inte biträdet förstått definitionen av överföring kan det även ha blivit fel information redan vid en upphandling. Biträdena är inte alltid intresserade av att samarbeta och göra de förbättringar som behövs för att deras system eller tjänst ska gå att använda.

Det finns även utmaningar i att bedöma om extra skyddsåtgärder så som till exempel kryptering och pseudonymisering är tillräckliga. De ska skydda personuppgifterna över tid. Det räcker inte med standardkryptering utan det krävs en typ av kryptering som inte kan avkodas av myndigheter i mottagarlandet, och den ska inte kunna låsas upp av biträdet eller underbiträdet i landet så att de får åtkomst. När t ex supporten eller systemutvecklare finns i det tredje landet blir det inte möjligt att skydda informationen med några extra skyddsåtgärder då åtkomst är en förutsättning för support och felsökning. Behandling av personuppgifter blir då inte förenlig med dataskyddslagarna.

När en handlingsplan finns framtagen behöver den hanteras i en lämplig prioriteringsordning.

Om det visar sig att ett system eller tjänst inte är laglig att använda finns en skyldighet att avbryta behandlingen. Det är en utmaning i de fall där verksamheten är beroende av den för att kunna bedriva sin verksamhet.

Rekommendation

Min rekommendation är att arbetet med att kartlägga personuppgiftsbehandlingar och hantera identifierade brister fortsätter och slutförs för att säkerställa att personuppgifter inte förs över till tredje land på ett olagligt sätt och att de registrerades friheter och rättigheter skyddas.

Kontroll av efterlevnad av beslutet i kommunfullmäktige gällande informationslagring i molntjänster

Kontroll

Kontrollen gällde dels hur kommunikationen av beslutet och dess innebörd har nått de som behöver den i sitt arbete med anskaffning dels om man har följt beslutet i sitt arbete med anskaffning. En molntjänst är ett system eller en digital tjänst där lagring av information och andra tillhörande tjänster hanteras hos leverantören i stället för att IT-system finns på servrar hos kommunen och sköts av kommunens personal. Detta ställer höga krav på anskaffningsförfarandet.

Resultat

När beslutet om informationslagring i molntjänster fattats i Kommunfullmäktige 2021 var kännedomen om beslutet lågt bland de personer som behövde kännedom om det i sitt arbete med anskaffning av IT-system och digitala tjänster så som molntjänster. Det ökade under 2022 men via olika kanaler. Även när kännedom funnits har det visat sig finnas missuppfattningar kring vad beslutet innebär och betyder för förvaltningarna i form av arbete vid anskaffning och kring beslut av nämnd inför ett eventuellt införande av utomeuropeisk molntjänst.

Det finns en vilja i organisationen att följa GDPR och fattade beslut men det finns även brister på området. Om ett adekvat arbete och analyser inte görs kan det leda till att beslut fattas som kan leda till risker för de personer vars personuppgifter behandlas av kommunen.

Då jag som dataskyddsombud inte fullt ut blir involverad eller får kännedom om hur kommunen arbetar med anskaffning av molntjänster finns ingen fullständig bild av hur arbetet sker vilket ger begränsad möjlighet vid rapportering till nämnderna.

Utmaningar

Utmaningarna är till stor del desamma som de som uppstod i det arbete som gjorts för att säkra efterlevnaden av dataskyddsförordningen efter ogiltigförklarandet av Privacy Shield. Då handlade det om att säkra efterlevnaden för de system och tjänster som redan fanns i kommunen. I det här fallet handlar det om arbetet inför och med anskaffning av molntjänster. I båda fallen krävs tid, kunskap, att ett strukturerat arbetssätt följs och leverantörer som gör sin del av arbetet och bistår med information som visar att deras tjänst efterlever GDPR.

En utmaning är de oklarheter som finns kring beslutets innebörd. Det krävs kunskaper för att fullt ut förstå innebörden och tolka det rätt.

Om utomeuropeiska molntjänster ska användas får enligt beslutet inte extra skyddsvärda eller känsliga personuppgifter behandlas. I kommunen är det vanligt att dessa typer av personuppgifter behandlas. Exempel på känsliga personuppgifter är uppgifter om hälsa, religion, etniskt ursprung mm. Exempel på extra skyddsvärda personuppgifter är personnummer, alla uppgifter om barn (personer upp till 18 år) och social situation.

Enligt beslutet ska riskanalyser och vid behov konsekvensbedömning göras för att minimera risker. Dataskyddsförordningen tillåter inte risker för de registrerade vilket i praktiken innebär att om åtkomst finns från tredjelandet så innebär det att risker finns och att personuppgiftsansvarig inte kan skydda personuppgifterna tillräckligt.

Beslut om användande av utomeuropeisk molntjänst ska fattas av nämnd och kan inte delegeras. En utmaning här är att det behöver tas fram underlag inför beslut som ger en rättvisande bild av vad beslutet innebär så att det blir ett välinformerat nämndbeslut.

Rekommendation

Personuppgiftsansvariga ansvarar för att ha kontroll över var och hur personuppgifterna behandlas och det finns krav på att aktiviteter ska göras inför anskaffning av IT-system och digitala tjänster. Det kan upplevas som ett omfattande arbete inför anskaffning men det sparar den tid och de kostnader det medför att byta ut ett system som inte ger adekvat skydd eller de kostnader som sanktionsavgifter till staten eller skadestånd till drabbade individer kan orsaka. Först och främst leder arbetet till skydd för de personer som behöver nyttja kommunens service och för anställda hos kommunen.

Rekommendationen är att arbeta på ett korrekt sätt med anskaffning av molntjänster, göra objektiva analyser och ge personuppgifterna ett tillräckligt starkt skydd så att de registrerade inte utsätts för risker.

Det är även lämpligt att förtydliga innebörden av beslutet i Kommunfullmäktige avseende informationslagring i molntjänster..

Tolkningar av eller avsikter med beslutet i Kommunfullmäktige fråntar inte nämnderna ansvaret för efterlevnad av dataskyddsförordningen och för konsekvenserna av att inte efterleva densamma. Dataskyddsförordningen är lag i Sverige och hela EU och behöver som sådan följas.

Aktuell information och rekommendationer från Europeiska Dataskyddsstyrelsen rörande molntjänster

Drygt 20 av EU:s tillsynsmyndigheter har genomfört en gemensam undersökning av hur offentliga organisationer använder molntjänster. Europeiska Dataskyddstyrelsen, EDPB, antog rapporten över arbetet den 17 januari i år. IMY har tidigare publicerat sin rapport för den undersökning som de genomfört i Sverige. Rapporten från EDPB information om vad man funnit under undersökningarna och även rekommendationer till offentliga myndigheter som gäller molnbaserade produkter och tjänster.

EDPB skriver i sin rapport att det med hänsyn till att offentliga myndigheter kan behandla personuppgifter kan vara av känslig karaktär och att det kan förekomma stora mängder uppgifter så är det väsentligt att den grundläggande rätten till skydd av personuppgifter garanteras av alla offentliga myndigheter. EDPB understryker därför behovet av att offentliga organ agerar i full överensstämmelse med GDPR när de använder molnbaserade produkter eller tjänster. EDPB tar med anledning av detta i

sin sammanfattning av rapporten upp följande punkter som offentliga myndigheter bör ta hänsyn till när de ingår avtal med molntjänstleverantörer:

- Utföra en konsekvensbedömning (DPIA);
- Se till att de inblandade parternas roller är klart och otvetydigt bestämda;
- Se till att molntjänstleverantören endast agerar på uppdrag av och i enlighet med det offentliga organets dokumenterade instruktioner och identifiera eventuell behandlingar som molntjänstleverantören blir personuppgiftsansvarig för;
- Se till att ett meningsfullt sätt att invända mot nya underbiträden är möjligt;
- Säkerställa att personuppgifterna bestäms i förhållande till de ändamål för vilka de behandlas;
- Främja att dataskyddsombudet involveras;
- Samarbeta med andra offentliga organ i förhandlingarna med molntjänstleverantörerna.
- Genomföra en granskning för att bedöma om behandlingen utförs i enlighet med konsekvensbedömningen;
- Se till att upphandlingsförfarandet redan förutser alla nödvändiga krav för att uppnå överensstämmelse med GDPR;
- Identifiera vilka överföringar som kan äga rum i samband med att tjänsterna tillhandahålls, och vid behandling av personuppgifter för molntjänstleverantörens egna affärsändamål (se relaterad punkt), och se till att bestämmelserna i kapitel V i GDPR uppfylls, dvs rörande överföring av personuppgifter till tredjeländer, genom att identifiera och anta kompletterande åtgärder vid behov;
- Analysera om en lagstiftning i ett tredjeland skulle vara tillämplig på molntjänstleverantören och skulle kunna leda till begäranden om tillgång till data som lagras av molntjänstleverantören i EU.
- Granska noggrant och omförhandla vid behov kontraktet;
- Verifiera under vilka förutsättningar det offentliga organet tillåts och kan bidra till revisioner och se till att de finns på plats.

Den gemensamma aktionen pågår fortfarande och mer information och rekommendationer kan komma att publiceras under 2023.

Länk till rapporterna på EDPB:s webb

Länk till IMY:s rapport över undersökningen av molntjänstanvändning i Sverige

Uppföljning av tidigare rekommendation

Dataskyddsombudets involvering i kommunen

I årsrapporten för 2021 rapporterades om brister vad gäller involveringen av dataskyddsombudet i frågor som rör skyddet av personuppgifter. Rekommendationen var då att dataskyddsombudet rådfrågas och hålls informerad enligt kraven i dataskyddsförordningen.

Nämnderna informerades om de krav som gäller enligt dataskyddsförordningen. 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.

Uppföljning av rekommendation

Sedan rekommendationen gavs har det inte skett någon märkbar förändring i positiv riktning vad gäller involvering av dataskyddsombudet. Kontakt tas inte i högre utsträckning än tidigare i digitaliseringsinitiativen och inte heller i god tid inför övrig anskaffning av system och digitala tjänster i förhållande till den mängd initiativ, projekt och upphandlingar som förekommer. Inom vissa delar av organisationen ses en förbättring och rekommendationen har därför troligen följts där, medan det i andra delar kan ses en försämring. På det stora hela har ingen förbättring skett. Slutsatsen är därför att rekommendationen inte har följts.

En anledning till att kontakt inte tas eller inte tas i god tid kan vara att organisationen inte förstår rollen och vad den kan bidra med. Därför följer nedan förtydligande information baserad på Artikel 29-arbetsgruppens riktlinje om rollen och uttalanden av Integritetsmyndigheten, IMY.

Den tidigare Artikel 29-arbetsgruppen tog fram en riktlinje om rollen dataskyddsombud. Denna riktlinje har sedan antagits av Europeiska Dataskyddsstyrelsen, EDPB, som har uppdraget att tolka GDPR för hela EU/EES.

Av riktlinjen framgår bland annat följande:
”Att säkerställa att dataskyddsombudet informeras och rådfrågas redan från början underlättar efterlevnaden av förordningen och främjar en strategi för inbyggt dataskydd och bör därför vara en standardrutin i organisationens styrning. Dessutom är det viktigt att dataskyddsombudet ses som en diskussionspartner inom organisationen och att han eller hon ingår i de relevanta arbetsgrupper som har ansvar för behandling av personuppgifter inom organisationen.”

Av riktlinjen framgår vidare:
”Organisationen bör bland annat säkerställa följande:

- Dataskyddsombudet ska regelbundet inbjudas att delta i möten på högsta och mellanliggande förvaltningsnivå,
- Dataskyddsombudet rekommenderas delta när beslut med följder för dataskyddet fattas. All relevant information ska i god tid förmedlas till dataskyddsombudet så att han eller hon kan ge lämpliga råd.
- Dataskyddsombudets åsikt måste alltid ges tillbörlig vikt. I händelse av oenighet rekommenderar artikel 29-arbetsgruppen att organisationen som god praxis dokumenterar skälen till att dataskyddsombudets råd inte har följts.
- Dataskyddsombudet ska rådfrågas omedelbart när en personuppgiftsincident eller annan incident har inträffat.”

Dataskyddsombudet ska även rådfrågas vid konsekvensbedömningar.

Anledningen till att det är lämpligt att involvera dataskyddsombudet redan på idéstadiet är att ombudet kan bidra med en utredning av dataskyddet för den specifika behandlingen och stötta verksamheten i att säkerställa att behandlingen av personuppgifter följer regelverken för dataskydd så att de når sitt mål utan att stöta på onödiga hinder som kan orsaka fördröjningar.

Att dataskyddsombuden inte används i organisationerna som var avsett har uppmärksammats av tillsynsmyndigheterna i Europa och de kommer att tillsammans via Europeiska Dataskyddstyrelsen under 2023 påbörja en gemensam aktion för att granska hur dataskyddsombuden används och resultatet ska leda till att ett förtydligande tas fram. Detta blir deras nästa aktion efter den som gäller användning av molntjänster som jag informerat om ovan.

Rekommendation

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

Dataskyddsombudets arbete i kommunen under 2022

Under 2022 har arbetet bestått av bl a följande:

- Rapporterat om dataskyddet till nämnder och förvaltningschefer för 2021.
- 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 om behandling av personuppgifter utifrån dataskyddsförordningen.
- Tagit fram mallar.
- Skrivit nyhetsbrev.
- Informerat om dataskydd.

- Omvärldsbevakat.
- Förmedlat omvärldsbevakning till berörda i kommunen.
- Utfört kontroller och övervakat.
- Svarat på frågor från registrerade.
- Hållit sig uppdaterad inom dataskyddsområdet genom att delta i utbildningar, webbinarier och konferenser.
- Sammankallat till nätverksmöten med övriga i kommunens dataskyddsorganisation.
- Deltagit i nätverksmöten för dataskyddsombud.