BONDE ADVOKATER

TILL: Huddinge kommun, gymnasie- och arbetsmarknadsnämnden (”**GAN**” eller ”**nämnden**”)

FRÅN: Tillförordnat dataskyddsombud för Huddinge kommun, Advokat Ana-Maria Barbu-Nyström, Bonde Advokater AB

DATUM: 25 april 2024

SAKEN: Dataskyddsombudets årsrapport 2023

1. Inledning

Dataskyddsförordningen (”**GDPR**”) trädde i kraft i maj 2018 med syftet att skydda individers rätt till privatliv och att garantera varje individens rätt att ha kontroll över hur deras personuppgifter används. Rätten till ett skyddat privatliv och personlig integritet är grundstenar i ett demokratiskt samhälle. GDPR reglerar hur personuppgifter får insamlas, användas och hanteras för att garantera att dem hanteras på ett korrekt och rättvist sätt. I sin kärna handlar GDPR om att bygga ett socialt hållbart samhälle.

Varje nämnd i Huddinge kommun är personuppgiftsansvariga för den behandling av personuppgifter som utförs inom respektive nämnd och dess förvaltning. Den personuppgiftsansvarige är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

När en nämnd är personuppgiftsansvarig innebär det att nämnden har det yttersta ansvaret för att säkerställa att all behandling av personuppgifter inom nämndens verksamhet sker i enlighet med GDPR. Detta innebär att nämnden måste se till att personuppgifter endast samlas in för specifika, uttryckligt angivna och legitima ändamål, och används på ett lagligt, rättvist och transparent sätt. Dessutom måste nämnden säkerställa att de personuppgifter som behandlas är adekvata, relevanta och begränsade till vad som är nödvändigt i förhållande till de ändamål för vilka de behandlas.

Som personuppgiftsansvarig har nämnderna ett ansvar för att implementera lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna påvisa att behandlingen överensstämmer med GDPR. Detta inkluderar att i vissa fall utse ett dataskyddsombud (”**DSO**”), att vid behov genomföra konsekvensbedömningar avseende dataskydd (se vidare i avsnitt 2.6.) och att rapportera personuppgiftsincidenter till Integritetsmyndigheten (”**IMY**”) samt, i vissa fall, till de berörda individerna.

2. Granskning av dataskyddsarbetet 2023

2.1. DSO i Huddinge kommun

Samtliga nämnder har utsett Ana-Maria Barbu-Nyström till DSO från och med den 1 december 2023. Enligt artikel 39 i GDPR innefattar DSO:s uppdrag att, på ett oberoende sätt, övervaka, granska, informera och ge rekommendationer om Huddinge kommuns efterlevnad av dataskyddslagstiftningen.

Enligt artikel 38.3 i GDPR ska DSO rapportera till den högsta förvaltningsnivån. I Huddinge kommun innebär detta att DSO rapporterar direkt till nämnder och styrelser. I samband med detta lämnar DSO årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd i Huddinge kommun. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts.

Årsrapporten är avsedd att fungera som ett stöd för verksamheten i verksamhetens fortsatta arbete med dataskydd. Eftersom DSO-rollen har en rådgivande funktion och inte får fatta beslut, är det upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar och för att på bästa sätt kunna hantera identifierade risker. Detta är viktigt för att säkerställa att verksamheten uppfyller verksamhetens skyldigheter enligt dataskyddslagstiftningen och för att minimera risken för sanktioner från IMY.

2.2. Huddinge kommuns dataskyddsorganisation

För att uppfylla dataskyddsförordningens krav på dataskydd behövs ett helhetsperspektiv på det systematiska arbetet med informationssäkerhet, IT-säkerhet, och personuppgiftshantering. DSO uppfattar att samtliga funktioner arbetar nära varandra för att väva ihop kommunens övergripande systematiska arbete med informationssäkerhet och dataskydd.

Inom Huddinge kommun finns en etablerad dataskyddsorganisation där DSO och informationssäkerhetssamordnaren samarbetar aktivt och ger stöd till dataskyddsskoordinator-funktionerna (med undantag för KSF, som saknar denna funktion).

Dataskyddskoordinator-funktionen är en roll som stöttar, samordnar och följer upp dataskyddsarbetet inom en viss nämnd inom Huddinge kommun. I Huddinge kommun ansvarar denna roll för löpande GDPR-arbetet i förvaltningarna (både utveckling och personuppgiftsincidenthantering). Dataskyddskoordinatorerna i Huddinge kommun är därmed stödjande operativa resurser som hjälper nämnderna, i nämndernas roller som personuppgiftsansvariga, att driva på det systematiska arbetet med dataskyddsfrågor. DSO är en oberoende funktion och det ska anmälas till tillsynsmyndigheten om en DSO har utsetts. Som nämnts ovan omfattar uppgifterna för DSO bland annat att informera och ge råd till personuppgiftsansvariga, övervaka efterlevnad av personuppgiftsbehandlingar, ge råd vid riskanalyser och övervaka genomförandet av konsekvensbedömningar, vara kontakt för registrerade och tillsynsmyndighet samt samarbeta och begära förhandsråd av tillsynsmyndigheten vid behov.

GAF har utsett en dataskyddskoordinator. Med hänsyn till GAF dataskyddskoordinators arbetsbelastning och det faktum att inte alla dataskyddskoordinatorer har möjlighet att avsätta tillräckligt med tid för GDPR-relaterade arbetsuppgifter, kommer DSO att etablera ett nätverk mellan dataskyddskoordinatorerna inom Huddinge kommun. DSO har haft dialog med KSF-ledningen för att etablera ett strukturerat samarbete eller internt nätverk för dataskyddskoordinatorerna där de kan ge varandra ömsesidig rådgivning och dela med sig av sina kunskaper. Resultatet av dessa diskussioner blev att en regelbunden mötesfrekvens, initialt en gång i månaden, kommer att fastställas. Efterhand som nätverket utvecklas kan mötesfrekvensen justeras för att bättre passa nätverkets behov. Ett internt kunskapsutbyte kan på detta sätt bidra till att harmonisera interna processer och därmed säkerställa en enhetlig efterlevnad av GDPR inom hela Huddinge kommun. DSO kommer att vara med i processen och delta i månadsmöten för att säkerställa att nätverket fungerar som en integrerad del av kommunens dataskyddsarbete.

- **DSO:s rekommendationer för förbättring av Huddinge kommuns dataskyddsorganisation under 2024**

DSO rekommenderar att GAF:s ledning står bakom initiativet och uppmuntrar dataskyddskoordinatorerna att delta i dessa nätverksmöten.

2.3. Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Det kan, bland annat, handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om incidenten uppstått avsiktligt eller oavsiktligt. Dokumentation av personuppgiftsincidenter är av stor betydelse i syfte att kunna visa på efterlevnad av GDPR. Personuppgiftsincidenter

som inte hanteras på ett korrekt sätt kan leda till sanktionsavgifter och även leda till förtroendeskada för den personuppgiftsansvarige, det vill säga nämnden. Således är det viktigt att alla medarbetare på Huddinge kommun är insatta i hur man ska agera om man misstänker en personuppgiftsincident.

Av artikel 33 i GDPR följer en skyldighet att rapportera vissa personuppgiftsincidenter till IMY. Alla incidenter är inte rapporteringspliktiga till IMY. Dock måste samtliga incidenter dokumenteras av den personuppgiftsansvarige. Artikel 33.5 GDPR stipulerar att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inklusive omständigheterna kring incidenten, dess effekter och de vidtagna korrigerande åtgärderna. Dokumentationen ska möjliggöra för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel. Detta innebär att varje nämnd, i egenskap av personuppgiftsansvarig, bör ha en god översikt över sina personuppgiftsincidenter för att kunna uppvisa detta vid eventuell tillsyn från IMY. Det finns beslut från IMY mot offentliga aktörer som inte har uppfyllt sina förpliktelser enligt dessa krav. Till exempel har Umeå universitet belagts med en administrativ sanktionsavgift om 110 000 kr för brott mot artikel 33 punkt 1 och punkt 5, då Umeå universitet inte dokumenterade och anmälde en personuppgiftsincident i form av ett oavsiktligt utskick av känsliga personuppgifter i okrypterat mejl via öppna nät (beslut 2020-12-10, dnr DI-2019-9432).

Enligt IMY:s rapport 2023:2[1] angavs den mänskliga faktorn som orsak i 59 procent av samtliga anmälningar om personuppgiftsincidenter i 2022. Oftast handlade det om personer som begått ett misstag när de hanterat personuppgifter i sina verksamheter. Mer än hälften av de personuppgiftsincidenter som orsakades av den mänskliga faktorn är felskickade brev, mejl eller sms. Detta visar att medarbetarnas hantering av information är av största vikt för att inte personuppgiftsincidenter ska uppstå.

Under 2023 har GAN hanterat 7 personuppgiftsincidenter:

Ansvarig nämnd	**Upptäckta personuppgiftsincidenter**	**IMY anmälda personuppgiftsincidenter**
GAN	7	3
Totalt i Huddinge kommun	21	16

DSO påpekar att det är svårt att få en samlad och aktuell statistik över personuppgiftsincidenter i Huddinge kommun eftersom rapporterna är utspridda över flera källor. Sedan 2022 finns ett systemstöd, Artvise PUI, som är avsett att stödja och delvis automatisera hanteringen av personuppgiftsincidenter i Huddinge kommun. Trots att alla dataskyddskoordinatorer har fått en timmes utbildning i systemet, anser DSO att det inte är tillräckligt, då Artvise upplevs som användarosäkert. Artvise-

[1] IMY rapport om anmälda personuppgiftsincidenter 2022, 7 juni 2023

systemet används inte inom GAN eftersom tidigare försök att arbeta med det inte gett goda erfarenheter, enligt GAFs dataskyddskoordinator.

Efter dialog med dataskyddskoordinatorerna och diskussioner med Trygghet och säkerhet i februari 2024, har det beslutats att utreda om problemen beror på bristande utbildning eller tekniska brister i Artvise.

- **DSO:s rekommendationer för förbättring av GANs hantering av personuppgiftsincidenter under 2024**

DSO rekommenderar att en detaljerad utbildning i användningen av Artvise inom GAF prioriteras för att garantera en standardiserad hanteringsprocedur för personuppgiftsincidenter inom nämnden. Det är avgörande att GAF:s dataskyddskoordinator är väl förtrogen med Artvise och dess funktioner för incidenthantering, särskilt eftersom en personuppgiftsincident måste anmälas till IMY inom 72 timmar från det att den upptäckts.

Regelbundna utbildningssessioner och workshops bör anordnas för att höja kompetensen och säkerställa att alla medarbetare inom GAF kan agera korrekt och effektivt vid en eventuell personuppgiftsincident. Det är positivt att notera att sedan januari 2024 finns en GDPR-grundutbildning tillgänglig för alla medarbetare (inklusive en version anpassad till de som arbetar inom skolverksamhet), vilket kommer att bidra till att öka GDPR-kunskapen inom GAF.

2.4. Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträdesavtal (”**PUB-avtal**”) är ett avtal som reglerar relationen mellan en personuppgiftsansvarig och ett personuppgiftsbiträde, det vill säga den som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige (exempelvis en leverantör till kommunen). PUB-avtalet ska tydligt ange vilka personuppgifter som ska behandlas, behandlingens syfte, tidsperioden för behandlingen och vilka behandlingsåtgärder biträdet är behörigt att utföra. Det ska även fastställa åtgärder för att skydda personuppgifterna, inklusive tekniska och organisatoriska säkerhetsåtgärder, och ge den personuppgiftsansvarige rätten att utföra revisioner och inspektioner av biträdets verksamhet. Dessutom ska PUB-avtalet säkerställa att personuppgiftsbiträdet hjälper den personuppgiftsansvarige att uppfylla sina skyldigheter enligt GDPR, som att hantera förfrågningar från registrerade och rapportera personuppgiftsincidenter. PUB-avtalets syfte är att garantera att personuppgiftsbiträdet hanterar personuppgifter i enlighet med den personuppgiftsansvariges dataskyddspolicy och de krav som ställs av GDPR, vilket är avgörande för att skydda individernas personuppgifter och för att undvika sanktioner vid eventuella dataskyddsförseelser.

DSO har tidigare konstaterat att det inte finns PUB-avtal med alla leverantörer som Huddinge kommun har. Därför har DSO påbörjat ett arbete 2023 med inventering av samtliga PUB-avtal inom Huddinge kommun som pågår för närvarande. DSO väntar på återkoppling från leverantörerna genom objektledarna, inklusive inom GAF. DSO har löpande påmint relevanta aktörer för att skynda på arbetet. Efter att återkopplingen har mottagits kommer DSO att kunna genomföra en revision av alla befintliga avtal och upprätta de som saknas. Parallellt med detta arbete ska eventuella SSA som inte finns för system som GAF använder i nuläget genomföras.

Under december 2023 har DSO uppdaterat och förbättrat kommunens standardmall för PUB-avtal och informerat upphandlingsfunktionen om den nya versionen. DSO har tidigare konstaterat att Huddinge kommun saknar PUB-avtal med vissa leverantörer.

- **DSO:s rekommendationer för förbättring av GANs hantering av PUB-avtal under 2024**

DSO kommer kontinuerligt att följa upp processen med kartläggningen av PUB-avtal och kommer att se till att det finns på plats PUB-avtal där de saknas. DSO har också kopplat in upphandlingsfunktionen för att få stöd med kartläggningen av PUB-avtal, samt kommer vid behov ta kontakt med objektledarna och systemägarna.

Vidare bör en plan för genomförande av systemsäkerhetsanalyser SSA av befintliga system som används inom GAF, i de fall dem saknas, tas fram och implementeras parallellt med revisionen av PUB-avtalen.

2.5. Rätten till tillgång (tidigare kallad ’registerutdrag’)

Den registrerade, det vill säga den vars personuppgifter behandlas, har ett antal rättigheter enligt GDPR. Som personuppgiftsansvarig har nämnden ett ansvar för att ha rutiner på plats för att hantera begäranden om att utöva dessa rättigheter när någon begär det. Artikel 12 GDPR stadgar hur information som lämnas till den registrerade ska vara utformad. Informationen ska utformas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

Rätten till tillgång till sina personuppgifter är en av rättigheterna i GDPR (artikel 13 i GDPR) och innebär att en person har rätt att vända sig till en organisation för att få information om huruvida organisationen hanterar personens personuppgifter och, om så är fallet, få tillgång till uppgifterna och information om hur personuppgifterna används. Det är viktigt att inte förväxla kraven i GDPR med utlämnande av offentliga

handlingar enligt offentlighetsprincipen. Varken artikel 12 eller 13 i GDPR reglerar dock i detalj i vilken form eller hur informationen ska lämnas till den registrerade.

Följande antal begäranden om registerutdrag har diarieförts under 2023:

Ansvarig nämnd	**Antal begäranden som har diarieförts under 2023**	**Antal obesvarade begäranden**
GAN	10	7
Totalt i Huddinge kommun	140	7

DSO har observerat att varje förvaltning hanterar dataskyddsfrågor om registerutdraget på ett individuellt sätt, vilket resulterar i varierande processer. Emellertid är GAF en av de förvaltningar som är mest aktiva i detta arbete och har en pågående process för att utveckla rutiner för GDPR-registerutdrag. En första version av denna rutin har skickats av GAF:s konsult för genomgång till GAF:s dataskyddskoordinator och DSO i januari 2024. Efter att ha mottagit kommentarer har konsulten tagit fram en ny, uppdaterad version av rutinen, vilken för närvarande granskas av GAF:s dataskyddskoordinator och DSO.

- **DSO:s rekommendationer för förbättring av GANs hantering av de registrerades rätt till tillgång under 2024**

DSO rekommenderar att arbetet inom detta område fortsätter. En grundläggande princip i GDPR är att en organisation ska kunna tillgodose de registrerades rättigheter. För att uppfylla detta krav är det nödvändigt att ha ett tillgängligt och uppdaterat behandlingsregister (vänligen se nedan under avsnitt 2.6.). Därför bör kartläggningen av vilka personuppgifter som finns i vilka system inom GAF fortsätta kontinuerligt. Detta kommer att visa att GAN har kontroll över personuppgiftsbehandlingen i alla verksamheter och att GAN är medveten om, samt vidtar åtgärder för, att begränsa befintliga risker för de registrerades rättigheter och integritet.

2.6. Register över personuppgiftsbehandlingar

Enligt artikel 30 i GDPR ska alla organisationer med fler än 250 anställda och/eller som utför personuppgiftsbehandlingar som kan innebära risker för de registrerades rättigheter och friheter föra ett register över behandlingarna (”**behandlingsregister**”). Behandlingsregistret ska innehålla:

- Uppgifter om den personuppgiftsansvarige, vilket är GAN.
- Ändamålen med personuppgiftsbehandlingarna, vilka ofta framgår av namnen på kommunens processer.

- Kategorier av registrerade vars personuppgifter behandlas, exempelvis 'elever'.
- Kategorier av personuppgifter som behandlas, exempelvis 'kontaktuppgifter'.
- Kategorier av mottagare till vilka personuppgifterna kan komma att lämnas ut, exempelvis 'leverantörer', andra nämnder inom Huddinge kommun, myndigheter eller polisen.
- Information om eventuellt utlämnande av personuppgifter till länder utanför EU eller EES.
- Om möjligt, tidsfrister för radering av de olika kategorierna av personuppgifter.
- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna.
- Den lagliga grunden för varje behandling läggs även till i registret.

Under 2023 anlitade GAF en konsult som, med stöd från DSO, arbetade med att utveckla ett kvalitetssäkrat behandlingsregister. En första version av GANs behandlingsregister slutfördes i januari 2024.

➢ **DSO:s rekommendationer för förbättring av Huddinge kommuns arbetet med behandlingsregistret under 2024**

DSO rekommenderar att en regelbunden översyn av informationen om behandlingsregistret för GAN genomförs för att säkerställa att det är uppdaterat och korrekt.

2.7. Utbildning

I november 2023 tog DSO fram ett förslag till en GDPR-handbok med centrala dataskyddsregler för Huddinge kommuns anställda och efter intern granskning publicerades dessa på Insidan i april 2024. Handboken innehåller bland annat en genomgång av GDPR:s grundprinciper och krav, samt beskriver medarbetarnas ansvar i GDPR-relaterade frågor. Dokumentet fastställer även generella rutiner för ett effektivt skydd av personlig integritet.

DSO anser att denna handbok är ett bra verktyg för de som jobbar aktivt med GDPR-frågor och olika GDPR-relaterade processer (exempelvis hantering av personuppgiftsincidenter) och har bjudit in de dataskyddskoordinatorerna att läsa in den. DSO planerar ta upp och göra en genomgång av handboken i första nätverksmötet med dataskyddskoordinatorena.

Vidare erhöll chefer och andra nyckelpersoner inom dataskyddsområdet hos Huddinge kommun tillgång till en digital GDPR-utbildning i december 2023. Efter samråd med HR och Kommunikationsavdelningen konstaterade DSO att det fanns ett behov av att integrera GDPR-utbildningen i kompetensutvecklingsplanen för alla anställda och inte bara chefer. Förslaget fick stöd av samtliga förvaltningschefer och godkändes. Sedan

februari 2023 har alla medarbetare haft möjlighet att delta i utbildningen. Under januari 2024 arbetade DSO tillsammans med Kommunikationsavdelningen för att ta fram informationsmaterial och internkommunikation angående utbildningen, vilket är slutfört.

Som ett resultat har alla förvaltningar, inklusive GAF, goda förutsättningar att öka förståelsen för vikten av att förstärka GDPR-kompetensen inom Huddinge kommun. Detta bidrar till att säkerställa att alla anställda i Huddinge kommun får grundläggande kunskaper om personuppgiftsbehandling och kraven i GDPR.

- **DSO:s rekommendationer för förbättring av Huddinge kommuns arbete med medarbetarutbildning under 2024**

DSO rekommenderar att GAF-direktören eller övriga chefer informerar och skickar påminnelser till sina medarbetare inom GAF om att en GDPR-grundutbildning finns tillgänglig och att det bör prioriteras (framför allt av de medarbetare som behöver hantera GDPR-relaterade frågor eller personuppgiftsbehandlingar i sitt arbete). GAF-direktören eller cheferna kan, när de bedömer det möjligt, även sätta en tidsfrist för genomförandet av utbildningen för att säkerställa att detta prioriteras av medarbetarna inom GAF.

2.8. Konsekvensbedömning

Det är ett krav att genomföra en konsekvensbedömning för dataskydd vid all hantering av personuppgifter som potentiellt kan innebära en hög risk för individers rättigheter och friheter. Generellt sett, anses en sådan risk existera om behandlingen uppfyller minst två av kriterierna nedan. Det bör dock noteras att en hög risk kan föreligga även om endast ett, eller inget, av kriterierna är uppfyllda. Omvänt kan det också vara så att en behandling inte anses innebära en hög risk, trots att två eller fler kriterier är uppfyllda. I det senare scenariot är det viktigt att dokumentera anledningarna till beslutet att inte genomföra en konsekvensbedömning.

Konsekvensbedömningen ska leda till att minska risker genom olika åtgärder, exempelvis att begränsa insamlingen av vissa personuppgifter, att begränsa behörigheter, använda automatisk gallring och att ha tydliga rutiner för användare.

Denna bedömning ska utföras innan GAN påbörjar en behandling av personuppgifter som sannolikt leder till en hög risk för de registrerade.

Resultaten av denna analys ska dokumenteras för att kunna visa att förordningen följs. Baserat på riskanalysen beslutar kommunen om det är nödvändigt att gå vidare med en konsekvensbedömning. I tveksamma fall rekommenderas alltid att en konsekvensbedömning genomförs. IMY har publicerat vägledning och listor som beskriver kriterierna för när en GDPR-konsekvensbedömning bör göras.

Att inte utföra en konsekvensbedömning när det finns skäl, enligt artikel 35 GDPR, kan vara riskabelt och kan leda till sanktionsavgifter från IMY. IMY har påfört flera kommuner sanktionsavgifter för brott mot kravet. Exempelvis har IMY påfört en nämnd i Stockholms kommun en administrativ sanktionsavgift om fyra miljoner kronor för brott mot bland annat artikel 35 GDPR, för att nämnden inte hade gjort en konsekvensbedömning avseende dataskydd beträffande sin elektroniska skolplattform (beslut 2020-11-23, dnr DI-2019-7024). Avgiften avsåg även de delar av plattformen som redan var i drift den 25 maj 2018, då dataskyddsförordningen började tillämpas. Förvaltningsrätten i Stockholm satte efter överklagande ned sanktionsavgiften till 3 000 000 kr (dom 2021-10-04 i mål nr 27791-20), men efter överklagande fastställde kammarrätten i Stockholm sanktionsavgiften till fyra miljoner kronor (dom 2022-09-16 i mål nr 7837-21).

Vidare har IMY påfört en nämnd i Gnosjö kommun en administrativ sanktionsavgift om 200 000 kr för brott mot bl.a. artikel 35 GDPR för att nämnden inte hade gjort en konsekvensbedömning avseende dataskydd beträffande kamerabevakning i realtid utan inspelning av en boende i sovrummet på ett LSS-boende (beslut 2020-11-24, dnr DI-2019-7782). Dessutom har IMY utfärdat en sanktionsavgift på 300 000 kr mot barn- och utbildningsnämnden i Östersunds kommun (beslut 2023-11-28, dnr IMY-2023-1647). Nämnden gjorde inte en konsekvensbedömning innan den digitala skolplattformen Google Workspace infördes på 24 av kommunens skolor (vänligen läs vidare under avsnitt 2.9.)

Dessa beslut visar att IMY har ett stort fokus på att kontrollera hur offentliga aktörer hanterar deras GDPR-riskanalys och att GAN riskerar få sanktionsavgifter om konsekvensbedömningen för Google inte färdigställds.

- **DSO:s rekommendationer för förbättring av Huddinge kommuns arbetet med GDPR-konsekvensbedömningen under 2024**

I början av 2024 har DSO tagit fram en GDPR-konsekvensbedömningsmall för Huddinge kommun som uppfyller alla krav enligt artikel 30 i GDPR. Det pågår även ett samarbete med infosäkerhetssamordnaren för att utforska möjligheterna att uppdatera den befintliga SSA-mallen, i syfte att undvika flera parallella processer som kan överlappa varandra. I framtiden är det möjligt att skapa en hybridmall för riskanalyser inom Huddinge kommun, baserad på både SSA-mallen och GDPR-konsekvensbedömningsmallen. Infosäkerhetssamordnaren behöver lämna ett förslag på hur kommunen ska gå vidare med integrationsprocessen.

DSO kommer att informera dataskyddskoordinatorerna om att GDPR-konsekvensbedömningsmallen nu finns tillgänglig och kommer att publicera. Konsekvensbedömningen för Google for Education ska prioriteras inom GAN. Även konsekvensbedömningen för Microsoft-tjänster som används inom GAN ska prioriteras och göras färdig under 2024.

2.9. Överföring av personuppgifter till tredje land

Överföring av personuppgifter till tredje land definieras som regel när personuppgifter görs tillgängliga för någon i ett land utanför EU/EES-området, enligt IMY [2]. Med ’tredje land’ avses ett land som inte är medlem i EU eller EES. Det kan exempelvis ske personuppgifter lagras på en server i ett tredje land. Även när en leverantör anlitar en underleverantör från ett tredje land för supporttjänster, kan det innebära en överföring av personuppgifter. Detta beror på att supporttjänster ofta innebär att underleverantören behöver tillgång till vissa personuppgifter för att kunna utföra sina uppgifter.

Som överföring räknas även möjlighet till åtkomst från tredjeland. Även om personuppgifter lagras i Sverige eller inom EU/EES, men det finns möjlighet för en part i ett tredje land att få tillgång till dessa data, räknas det som en överföring. Det bör hållas i åtanke att fjärråtkomst från tredjeland (även om den endast sker genom att personuppgifter visas på en skärm, till exempel i supportsituationer, felsökning eller för administrativa ändamål) och/eller lagring i ett moln utanför EES som erbjuds av en tjänsteleverantör, också anses vara en överföring[3]. Även om uppgifterna i praktiken aldrig lämnar EU/EES, räknas det som en överföring till ett tredje land eftersom det finns en möjlighet till åtkomst från ett tredje land.

I normalfallet strider det mot GDPR att föra över personuppgifter till så kallat tredje land, det vill säga länder utanför EU och EES utan att det finns en grund enligt kap. V i GDPR 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.

<u>Överföringar av personuppgifter till USA</u>

USA är ofta involverat som ett tredje land i dataskyddsfrågor, eftersom många tjänsteleverantörer och system, eller deras underleverantörer, ägs av amerikanska företag. Detta gäller särskilt för stora teknikföretag som Google och Microsoft. På grund av detta, faller dessa företag under amerikansk lagstiftning. Detta innebär att amerikanska myndigheter, med stöd av sina övervakningslagar, kan få tillgång till europeiska personuppgifter som hanteras av amerikanska tjänster, även om dessa personuppgifter fysiskt finns inom EU/EES.

Den 10 juli 2023 antog EU-kommissionen ett beslut om adekvat skyddsnivå för USA (”**EU-US Privacy Framework**”). Beslutet innebär att personuppgifter kan flöda fritt

[2] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/
[3] EDPB:s Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, antagna den 14 februari 2023, §16.

från EU till amerikanska företag som har certifierat sig enligt beslutet, utan att ytterligare skyddsåtgärder är nödvändiga.

EU-US Data Privacy Framework innebär att amerikanska organisationer, genom att åta sig följa ett antal dataskyddsskyldigheter, kan ansluta sig till ramverket genom självcertifiering. Vid anslutning anses en adekvat skyddsnivå tillförsäkras de personuppgifter som är föremål för överföring till sådana organisationer. Därav behöver varken ytterligare skyddsåtgärder vidtas eller en Transfer Impact Assessment genomföras. Om den mottagande organisationen inte omfattas av EU-US Data Privacy Framework kan överföringen inte ske med stöd av EU-kommissionens beslut om adekvat skyddsnivå för USA, och särskilda skyddsåtgärder behöver vidtas[4].

Efter beslutet om adekvat skyddsnivå för USA har Huddinge kommun öppnat upp för att använda fler delar inom Googles och Microsofts molntjänster. KSF har analyserat beslutet och tagit fram ett förslag till ’reviderat ställningstagande för tredjelandsöverföringar’ som godkänds av kommunledningen i december 2023.

Ett register över de organisationer som har anslutit sig till ramverket finns tillgängligt på en av USA:s handelsdepartement särskilt upprättad hemsida. EU-kommissionen kommer att tillsammans med behöriga amerikanska myndigheter och europeiska dataskyddsmyndigheter regelbundet granska hur EU-US Data Privacy Framework fungerar i praktiken. Den första granskningen kommer genomföras inom ett år från det att ramverket trädde i kraft.

Det är viktigt att ha i åtanke att EU-US Data Privacy Framework, likt tidigare överenskommelser, kan bli föremål för prövning och därmed ogiltigförklaras av EU-domstolen. Intresseorganisationen None of Your Business (”noyb”) har indikerat att de kan utmana denna överenskommelse, vilket kan leda till ett så kallat "Schrems III"-mål.

Om EU-domstolen skulle ogiltigförklara EU-US Data Privacy Framework, kan det ha betydande konsekvenser för Huddinge kommun. Det kan innebära att den behöver ändra hur den överför och lagrar personuppgifter, vilket kan vara både tidskrävande och kostsamt. Dessutom kan det leda till att kommunen behöver omvärdera Huddingekommuns relationer med vissa tjänsteleverantörer, särskilt de som är baserade i USA. Således bör GAN ta fram exitplaner för att hantera den data som hanteras i Microsoft och Google tjänster om rättsläget skulle ändras.

DSO vill betona vikten av att fortsätta följa alla grundläggande principer i GDPR, även om USA nyligen har fått EU-kommissionens beslut om adekvat skyddsnivå. Detta beslut innebär att USA anses ha tillräckliga skyddsåtgärder på plats för att skydda personuppgifter enligt EU-standarder. Men det betyder inte att GAN kan underlåta att följa de grundläggande principerna i GDPR när GAN överför personuppgifter till USA, exempelvis genom användning av tjänster tillhandahållas av

[4] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/overforingar-till-usa/

en amerikansk leverantör såsom Google och Microsoft. Överföring av personuppgifter är i sig en form av behandling[5], och det är därför nödvändigt att fortsätta följa alla relevanta GDPR-principer.

Detta innebär att det alltid måste finnas *en rättslig grund*[6] för att överföra personuppgifter. Denna grund kan vara myndighetsutövning, nödvändighet för att utföra ett avtal, nödvändighet för att uppfylla en rättslig skyldighet, eller samtycke från den registrerade. Inom den kommunala sektorn är det framför allt myndighetsutövning (punkt e i artikel 6 GDPR) som är relevant, men det kan även förekomma situationer där det finns en rättslig förpliktelse att överföra personuppgifter, till exempel när uppgifter lämnas till en annan myndighet (punkt c i artikel 6 GDPR). Ibland kan överföringen vara nödvändig för att fullgöra ett avtal med den registrerade, och i undantagsfall kan samtycke vara den rättsliga grunden för behandlingen.

Vidare är det viktigt att behandlingen av personuppgifter alltid är *nödvändig*. Detta innebär att ni inte bör överföra mer personuppgifter än vad som krävs för det specifika syftet.

Dessutom behöver GAN alltid sträva efter att *minimera* mängden personuppgifter som behandlas och överförs. Det är också av största vikt att GAN har *robusta säkerhetsåtgärder* på plats för att skydda de personuppgifter ni hanterar.

IMY beslut mot Östersunds kommun (Google Workspace)

I ärendet IMY-2023-1647 inledde IMY en tillsyn mot Barn- och utbildningsnämnden i Östersunds kommun för att undersöka om nämnden hade underlåtit att uppfylla sin skyldighet enligt artikel 35.1 i GDPR att genomföra en konsekvensbedömning innan Google Workspace började användas i 24 av kommunens skolor under hösten 2020.

IMY fastställde att behandlingen via Google Workspace-tjänsten utförs inom ramen för skolverksamhet och berör ett stort antal registrerade, huvudsakligen barn (det vill

[5] Se artikel 4 (2) i GDPR som definierar begreppet ”behandling” som en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

[6] Se artikel 6 (1) i GDPR som nämner att behandlingen är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:
a) Den registrerade har lämnat sitt samtycke
b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

säga elever). Dessutom har behandlingen omfattat anställda som befinner sig i ett beroendeförhållande till nämnden. Behandlingen har även i viss utsträckning innefattat återkoppling på skoluppgifter, vilket kan anses utgöra en utvärdering av de registrerades prestationer.

IMY bedömde att den aktuella behandlingen, med hänsyn till dess art, omfattning, sammanhang och ändamål, sannolikt har inneburit en hög risk för de registrerades rättigheter och friheter. Nämnden hade därför enligt artikel 35.1 i GDPR en skyldighet att genomföra en konsekvensbedömning innan behandlingen inleddes hösten 2020.

Inför en så omfattande behandling av barns personuppgifter inom skolverksamheten ska den personuppgiftsansvarige, i detta fall barn- och utbildningsnämnden, genomföra en konsekvensbedömning för att identifiera risker och behov av skyddsåtgärder. IMY konstaterade i sitt beslut att kommunen hade infört skolplattformen utan att ha genomfört en sådan konsekvensbedömning.

På grund av att barn- och utbildningsnämnden inte utförde en konsekvensbedömning innan skolplattformen infördes, utfärdade IMY en administrativ sanktionsavgift på 300 000 kronor mot nämnden för överträdelse av GDPR, enligt sitt beslut den 28 november 2023.

GAN är en av nämnderna i Huddinge kommun som använder Google for Education i sin verksamhet. Därför behöver GAN, med anledning av IMY:s beslut mot Östersunds kommun, färdigställa arbetet med konsekvensbedömningen för Google for Education. Huddinge kommun använder för närvarande en systemsäkerhetsanalysmall (”SSA-mallen”) för att genomföra informationssäkerhetsklassning, risk- och sårbarhetsanalyser. Den används även som en GDPR-konsekvensbedömningsmall. SSA-mallen hjälper till att identifiera och analysera risker samt konsekvenser för tekniska system eller operativa procedurer. Vissa delar av SSA-mallen tar upp GDPR-relaterade frågor, men DSO har identifierat att mallen inte fullt ut uppfyller kraven för en konsekvensbedömning enligt GDPR artikel 35, även känd som Data Protection Impact Assessment (DPIA). SSA:n hanterar informationsklassningen och hanterar visa GDPR DPIA-frågor, såsom klassificeringen av personuppgifter, kategorier av registrerande, och mottagare av personuppgifter. Det är DPO:s rekommendation att SSA-mallen kompletteras med en DPIA, eftersom i dagsläget är SSA-mallen inte tillräckligt inriktad på GDPR-frågor för att uppfylla alla krav under artikel 30 GDPR. IMY har publicerat en checklista med kriterier för en godtagbar konsekvens-bedömning[7], vilken kan användas för arbetet med att förbättra SSA-mallen.

[7] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/kriterier-for-en-godtagbar-konsekvensbedomning/

DK Datatilsynets beslut mot Helsingörs kommun (Google Workspace för utbildning, ChromeOS och Chrome-webbläsaren)

DSO vill nämna att det finns en serie beslut från den danska dataskyddsmyndigheten, Datatilsynet, som 2019 inlett tillsyn mot Helsingörs kommun avseende deras behandling av personuppgifter i grundskolan ("folkeskole") och som fokuserar på kravet att genomföra konsekvensbedömningen enligt GDPR. Besluten började med en specifik kommun, men det senaste beslutet, daterat 30 januari 2024, gäller alla 53 kommuner som använder samma tekniska stack och behandlingsuppsättning.

Nedan följer en sammanfattning av de fem besluten från Datatilsynets på området:

Ett klagomål från en förälder 2019 ledde till att Datatilsynet fann att Helsingörs kommun hade misslyckats med att bedöma risker för elevernas rättigheter och friheter, inte kunde visa att de hade tillräcklig säkerhet för behandlingsaktiviteter, saknade laglig grund för att behandla personuppgifter i Googles "Ytterligare tjänster" (som YouTube och Gmail), och hade brutit mot flera artiklar i GDPR. Datatilsynet beordrade kommunen i september 2021 att anpassa sina behandlingsaktiviteter till GDPR.

I juli 2022 instruerade Datatilsynet Helsingörs kommun att omedelbart upphöra med all dataöverföring till USA och införde ett omfattande förbud mot att använda Google Workspace för all datahantering. Datatilsynet konstaterade att kommunen hade överträtt flera GDPR-artiklar, bland annat genom att inte kunna visa att deras dataskyddsombud kunde erbjuda de garantier som krävs enligt artikel 28(1), samt att de inte hade säkerställt att personuppgiftsöverföringar till USA var skyddade mot potentiell övervakning av den amerikanska regeringen.

I augusti 2022 bekräftade Datatilsynet sitt tidigare beslut men modifierade det till att specifikt förbjuda användningen av Google Chromebooks och Workspace inom utbildningssektorn. Detta förbud trädde i kraft omedelbart och skulle gälla tills kommunen hade justerat sin datahantering för att överensstämma med GDPR och genomfört en konsekvensbedömning enligt artiklarna 35 och 36.

I september 2022 valde Datatilsynet att tillfälligt häva sitt förbud mot kommunens datahantering fram till den 5 november 2022. Myndigheten krävde också att kommunen skulle revidera sitt databehandlingsavtal med Google för att åtgärda de punkter som Datatilsynet hade påpekat, samt uppdatera sin konsekvensbedömning med hänsyn till alla identifierade risker.

I januari 2024 utvidgades beslutet till att omfatta alla 53 kommuner som använde samma tekniska lösningar och behandlingsmetoder från Google. Datatilsynet fastslog att kommunerna hade en laglig grund för att dela elevers personuppgifter i syfte att tillhandahålla tjänster, förbättra säkerheten och tillförlitligheten i dessa tjänster, kommunicera med kommunerna och uppfylla lagliga förpliktelser. Däremot hade de inte rätt att använda informationen för att underhålla och förbättra Google Workspace

för utbildning, ChromeOS och Chrome-webbläsaren, eller för att mäta prestanda och utveckla nya funktioner i dessa system. Datatilsynet instruerade alla kommuner att säkerställa att de hade en laglig grund för alla sina behandlingsaktiviteter.

Kammarrättens dom i 1177-målet

Kammarrätten i Stockholm har i domen från den 12 februari i "1177-målet" beslutat att Medhelp Sjukvårdsrådgivning AB ska betala en sanktionsavgift om 11 300 000 kronor. Ärendet gällde att telefonsamtal till 1177 Vårdguiden hade vidarekopplats till ett företag i Thailand utan lagligt stöd i svensk rätt. De personuppgifter som behandlades var av känslig natur och rörde individernas hälsa. Kammarrätten fann att det thailändska bolaget inte var omfattat av svensk sjukvårdslagstiftning och att behandlingen av känsliga personuppgifter därmed skedde i strid med artikel 9.1 i GDPR, eftersom det inte fanns någon lagreglerad tystnadsplikt enligt kraven i artikel 9.3. Överträdelsen ansågs så allvarlig att även den grundläggande principen om laglighet, korrekthet och öppenhet i artikel 5.1 a GDPR ansågs vara överträdd.

Domen understryker vikten av att Huddinge kommuner tar ansvar för att noggrant utreda frågor om överföring av personuppgifter till tredjeland och att alltid säkerställa att det finns lagligt stöd för sådana överföringar.

Som nämnts ovan tog Huddinge kommun fram ett ställningstagande den 1 december 2023 att prioritera svenska eller europeiska molntjänstleverantörer. Om sådana inte finns tillgängliga på marknaden, eller om det finns andra starka skäl, kan kommunen överväga en amerikansk leverantör. DSO påpekar att detta beslut gäller alla amerikanska molntjänster, men att Microsoft och Google är de mest relevanta för kommunen. Beslutet understryker också att det för närvarande inte finns några fullgoda alternativ till dessa leverantörer.

- **DSO:s rekommendationer för förbättring av Huddinge kommuns hantering av överföringar av personuppgifter till tredje land under 2024**

Av ovan nämnda praxis framgår det att IMY sannolikt kommer att öka sitt fokus på användningen av Google-tjänster inom den offentliga sektorn. Därför rekommenderar DSO att Huddinge kommun prioriterar arbetet med konsekvensbedömningen för användningen av tjänster från Google. Dessutom rekommenderar DSO att kommunstyrelseförvaltningen (KSF) prioriterar arbetet med att genomföra en riskanalys för att bedöma om sin nuvarande strategi för tjänster från amerikanska leverantörer som innebär behandling av personuppgifter är tillräcklig. Infosäkerhetssamordnaren bör kunna genomföra denna analys tillsammans med IT-funktionen. Det är viktigt att vara förberedd på att den juridiska situationen med överföringar av personuppgifter till USA kan förändras och bli striktare.