



Dataskyddelsesombudets årsrapport

2025

2026-04-27

Dataskyddsbudets årsrapport
2025

Beatrice Helmersson

© Beatrice Helmersson och Huddinge kommun
Tryckeri, 2026-02-16

ISBN 91-85565-02-4

Förord

Dataskyddsbudet har under 2025 samarbetat med gymnasie- och arbetsmarknadsnämndens verksamheter och stöttat med rådgivning vid behov. Dataskyddsarbetet har främst utförts genom löpande stöd till verksamheten och genom en grundläggande inventering av gymnasie- och arbetsmarknadsnämndens efterlevnad av dataskyddsförordningen. Denna rapport sammanfattar de dataskyddsrelaterade aktiviteter som genomförts under året.

Innehåll

Förord	3
Inledning	5
Dataskyddssombudets uppgifter	5
Dataskyddsorganisationen	6
Granskning av dataskyddsarbetet 2025	6
Övergripande kontroll 2025.....	7
Personuppgiftsincidenter	14
Identifierade risker utifrån inträffade personuppgiftsincidenter	15
Rättighetsbegäranden och klagomål	16
Identifierade risker utifrån rättighetsbegäranden och klagomål.....	16
Dataskyddssombudets löpande arbete.....	17
Omvärldsbevakning.....	17
Nya regler om kamerabevakning.....	17
EU-kommissionens förslag om ändringar av dataskyddsförordningen ...	18
Personuppgiftsincident Miljödata	19
Rapportering	20

Inledning

Ett av de grundläggande syftena med dataskyddsförordningen är att skydda individers grundläggande friheter och rättigheter, särskilt med fokus på rätten till skydd av personuppgifter. Dataskyddsförordningen bottnar i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat och familjeliv samt skydd av sina personuppgifter.

Dataskyddsförordningen och annan närliggande lagstiftning, sätter tydliga ramar för hur personuppgifter får behandlas för att minska risken för skada och för att säkerställa att hanteringen av personuppgifter sker på ett ansvarsfullt och rättvist sätt. I Huddinge kommun är varje nämnd och styrelse personuppgiftsansvarig för de behandlingar av personuppgifter som sker i den egna verksamheten. Dataskyddsombudets uppdrag är att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. Det operativa dataskyddsarbetet ansvarar respektive förvaltning för.

Denna rapport innehåller en redovisning av dataskyddsombudets och dataskyddsteamets arbete och resultat för 2025.

Dataskyddsombudets uppgifter

Myndigheter och offentliga organ i Sverige (med undantag för domstolar) är skyldiga att utse ett eller flera dataskyddsombud. Det framgår direkt av dataskyddsförordningen vilka arbetsuppgifter dataskyddsombudet ska ha. Den främsta uppgiften som åligger dataskyddsombudet är att granska den personuppgiftsansvariges efterlevnad av dataskyddsförordningen. Ytterligare arbetsuppgifter som ingår i dataskyddsombudets roll är att informera och ge råd om de skyldigheter som följer av dataskyddsförordningen samt att vara kontaktperson för Integritetsskyddsmyndigheten (IMY) samt för de registrerade. Arbetsuppgifterna ska även utföras på ett oberoende vis.

Dataskyddsorganisationen

Dataskyddsombudet tillträdde sin tjänst i oktober 2024. Den befintliga dataskyddsorganisationen bestod från och med 1 januari 2025 till och med 31 juli 2025 av dataskyddsombudet (en halvtidstjänst som köps in från Salems kommun). Inom kommunens förvaltningar finns minst en dataskyddskoordinator, den personuppgiftsansvarige har fram till den 1 december 2025 två dataskyddskoordinatorer. Efter den 1 december reviderar den personuppgiftsansvarige detta på grund av omorganisation inom förvaltningen och det finns numera en dataskyddskoordinator.

Den 1 augusti 2025 tillträdde en dataskyddssamordnare sin tjänst inom kommunstyrelseförvaltningen. Denna tjänst har under hösten övergått till en kombinerad roll som dataskydds- och informationssäkerhetssamordnare och det har tillträtt ytterligare två dataskydds- och informationssäkerhetssamordnare inom förvaltningen (tillträdde sina tjänster 2026-01-12). Tanken är att dataskydds- och informationssäkerhetssamordnarna ska arbeta med rådgivning och utveckling av bland annat dataskyddsarbetet inom kommunstyrelseförvaltningen samt i kommunövergripande projekt. Ambitionen är vidare att dataskyddsombudet mer renodlat ska ägna sin tid åt granskning och uppföljning.

Konsultstöd har inhämtats under större delen av 2025, tidsomfattningen har varierat från 32 timmar i månaden till 80 timmar i månaden och har belastat kommunstyrelseförvaltningen ekonomiskt (alltså inte den personuppgiftsansvarige). Konsulten har främst arbetat med rådgivning samt informationsinsatser och stödet har varit tillgängligt för samtliga förvaltningar inom kommunen.

Granskning av dataskyddsarbetet 2025

Dataskyddsombudet tog initialt fram en årsplan över aktiviteter för 2025. Denna årsplan kunde emellertid inte hållas med anledning av en mycket hög efterfrågan av stöd kopplat till dataskyddsaktiviteter (kommunövergripande), på grund av

genomförande av större projekt samt på grund av en större incident. Detta beskrivs mer i detalj nedan.

Övergripande kontroll 2025

Dataskyddsombudet har initierat en inventering av den personuppgiftsansvariges efterlevnad av dataskyddsförordningens krav. Detta har gjorts genom en övergripande nulägesanalys som har bestått av granskning av befintliga styr- och stöddokument och processer samt genom intervjuer med nyckelpersoner i respektive verksamhet. Rapporten för denna inventering kommer att redovisas separat och kommer att innehålla en rekommenderad åtgärdsplan för eventuella utvecklingsområden.

I och med att denna analys har genomförts, och presenteras separat, kommer denna årsrapport inte belysa innehållet ytterligare, utan för detta hänvisas det till separat rapport med tillhörande åtgärdsplan. I skrivande stund är nulägesanalysen för gymnasie- och arbetsmarknadsnämnden inte färdigställd.

Uppföljning av rekommendationer från årsrapport 2023

För årsrapporten 2025 har dataskyddsombudet valt att följa upp årsrapporten och de rekommenderade åtgärderna som tidigare dataskyddsombud tog fram för 2023. Året 2024 har inte följts upp då dataskyddsombudet påbörjade sitt uppdrag i slutet av året.

Nedan presenteras de rekommendationer som dataskyddsombudet lämnade i rapporten för 2023 samt de åtgärder som verksamheten har arbetat med utifrån dessa.

DSO rekommenderar att GAF:s ledning står bakom initiativet (om att etablera ett nätverk för dataskyddskoordinatorer) och uppmuntrar dataskyddskoordinatorerna att delta i dessa nätverksmöten.

En samverkansgrupp för kommunens dataskyddskoordinatorer har skapats och möten hålls löpande. Dataskyddskoordinator inom gymnasie- och arbetsmarknadsförvaltningen deltar regelbundet vid dessa samverkansmöten och

bidrar till diskussioner samt till det gemensamma utvecklingsarbetet avseende dataskyddsfrågor.

Rekommendationen är uppfylld.

DSO rekommenderar att en detaljerad utbildning i användningen av Artvise inom GAF prioriteras för att garantera en standardiserad hanteringsprocedur för personuppgiftsincidenter inom nämnden.

Artvise är ett systemstöd som finns tillgängligt inom Huddinge kommun. Det används av några förvaltningar som ett systemstöd för hantering av personuppgiftsincidenter. Vid ett samverkansmöte i februari 2025 fick dataskyddsgruppen en visning av Artvise. Vid efterföljande möten har den kommungemensamma användningen diskuterats. Det har dock inte fattats något beslut om användandet av Artvise. Det kan konstateras att Artvise används i varierande utsträckning inom förvaltningarna.

Inom den personuppgiftsansvariges verksamhet har just Artvise inte varit en prioritet under 2025. Det har på fler håll, inte uteslutande inom den personuppgiftsansvariges verksamhet, konstaterats ett antal nackdelar och viss opraktiskhet med själva utformningen av systemet. Arbete med översyn av incidenthanteringsprocessen, med tillhörande systemstödsfrågor, har initierats av dataskydds- och informationssäkerhetssamordnare inom kommunstyrelseförvaltningen, med stöd av de förvaltningsspecifika dataskyddskoordinatorerna. Detta arbete avser att förtydliga processen och finna ett lämpligt systemstöd för hantering av incidenter, såväl personuppgiftsincidenter som informationssäkerhetsincidenter.

Den personuppgiftsansvarige anger att det finns en standardiserad hanteringsprocedur på personuppgiftsincidenter, vilken reglerar att dataskyddskoordinator hanterar uppkomna ärenden.

Rekommendationen är uppfylld.

DSO rekommenderar att 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.

Samtliga medarbetare inom den personuppgiftsansvariges verksamhet har tillgång till en webbaserad GDPR-utbildning. Regelbundna workshops har dock inte kunnat prioriteras på grund av att kärnverksamhetens omfattande och föränderliga reglering har prioriterats. Detta skulle kunna medföra en risk för ojämn kunskapsfördelning inom organisationen, särskilt avseende mer praktiska moment såsom identifiering och hantering av personuppgiftsincidenter.

Förvaltningen bedömer att den generella medvetenheten kring dataskydd och säkerställandet av integritet är god.

Rekommendationen är delvis uppfylld.

DSO rekommenderar att en plan för genomförande av systemsäkerhetsanalyser SSA av befintliga system som används inom GAF, i de fall dem saknas, tas fram och implementeras.

Systemsäkerhetsanalyser genomförs i samband med upphandlingar inom respektive objekt eller centralt. Det är förvaltningens uppfattning att det saknas tillräcklig insyn i om och hur dessa analyser genomförs för samtliga system som används i verksamheten.

Detta medför en risk för bristande överblick över systemens säkerhetsnivå och därmed även över de risker som kan påverka behandlingen av personuppgifter. Särskilt gäller detta system som förvaltas av andra förvaltningar eller centrala funktioner, där etablerade strukturer för informationsdelning och uppföljning i dagsläget är begränsade.

Förvaltningen har identifierat ett behov av tydligare ansvarsfördelning samt stärkt samverkan mellan objekt och dataskyddsfunktion på central nivå.

Dataskyddskoordinatören har viss löpande dialog med berörda objekt, men saknar mandat och verktyg för att säkerställa att systemsäkerhetsanalyser genomförs och följs upp på ett enhetligt sätt.

Sammantaget bedöms att ett mer strukturerat och kommungemensamt arbetssätt krävs för att säkerställa tillräcklig kontroll över systemsäkerhet och därigenom minska risker kopplade till personuppgiftsbehandling. Förhållandet mellan personuppgiftsansvariga nämnder inom Huddinge kommun bör även ses över och regleras på lämpligt vis, exempelvis genom reglemente. Detta arbete bör ske kommunövergripande för berörda personuppgiftsansvariga nämnder.

Rekommendationen är delvis uppfylld och bedöms delvis ligga utanför den personuppgiftsansvariges direkta rådighet.

DSO rekommenderar att arbetet med hantering av registrerades rätt till tillgång 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. 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.

Den personuppgiftsansvarige har ett behandlingsregister upprättat som är föremål för kontinuerlig översyn. Det finns även en e-tjänst för att tillgodose en digital kanal för utövande av rätten till tillgång (registerutdrag) enligt artikel 15 dataskyddsförordningen. Hantering av registerutdrag sker löpande i enlighet med förvaltningens etablerade rutin.

Rekommendationen är uppfylld.

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

Förvaltningen anger att man arbetar regelbundet med uppdatering av behandlingsregistret. För drygt ett år sedan stöttade konsult med uppdatering av registret.

Det har på kommunövergripande nivå upphandlats ett stödsystem för hantering av bland annat behandlingsregister. Stödsystemet ska implementeras under 2026 och i samband med detta anger förvaltningen att behandlingsregistret kommer att granskas och uppdateras.

Rekommendationen är uppfylld.

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.

Information har i samband med publiceringen av utbildningen gått ut till förvaltningen och chefer inom förvaltningen har även informerat sina medarbetare om att utbildningen finns tillgängligt och att den ska genomföras. Bedömningen från förvaltningen är att utbildningen bör vara relevant för majoriteten av medarbetarna, då nästan samtliga behandlar personuppgifter inom ramen för sina arbetsuppgifter.

Uppföljning av graden av genomförande av utbildningen har inte tidigare varit möjlig för förvaltningen att självständigt kontrollera, detta på grund av att förvaltningen har saknat tillgång till statistiken. Detta har dock följts upp internt och i dagsläget ska det vara möjligt att få tillgång till rådata och på så sätt få tillgång till genomförandegrad av utbildningarna.

Förvaltningen framhåller att det sannolikt finns ett behov av att förnya informationen kring utbildningen för att säkerställa att den faktiskt genomförs av de medarbetare för vilken den är relevant. Påminnelse om utbildningen har skickats till chefer inom förvaltningen i mars 2026.

Rekommendationen är uppfylld.

DSO rekommenderar att 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.

Förvaltningen anger att denna rekommendation bör vara inaktuell och anger bland annat följande punkter som anledning till detta.

- Det finns ett giltigt personuppgiftsbiträdesavtal mellan Google och den personuppgiftsansvarige som reglerar den behandling av personuppgifter som biträdet utför.
- Huddinge kommun hade tidigare publicerat information på intranätet (2023-12-19)¹ där man förnyat sitt ställningstagande avseende användandet av amerikanska molntjänster (inkluderat både Google och Microsoft). Från en tidigare restriktiv hållning ska möjligheter att använda amerikanska molntjänster utökas med anledning av EU-kommissionens adekvansbeslut för USA.

Varken dataskyddskoordinator inom gymnasie- och arbetsmarknadsförvaltningen eller dataskyddsombudet har kunnat finna något formellt beslut eller underlag för beslut att använda amerikanska molntjänster. Förvaltningen anger dock att man genom publicering av informationen på intranätet bör beakta informationen som giltig.

Vad som ytterligare anges från förvaltningen är att man anser att detta ställningstagande bör ha medfört att en bedömning om användandet och

¹ Den tidigare publicerade informationen kan inte längre hittas, den har dock sparats ned separat innan den togs bort. Beslut om ställningstagandet eller underlag/förarbete till ställningstagandet går inte heller att finna. Dataskyddsombudet tolkar dock informationen som publicerats på intranätet 2023-12-19 som att ställningstagandet arbetats fram utifrån de nya förutsättningarna som skapats utifrån att EU-kommissionen fattat beslut om adekvat skyddsnivå för USA.

eventuella risker ska ha genomförts centralt inom kommunen, varför rekommendationen avseende gymnasie- och arbetsmarknadsnämnden i detta avseende bör vara inaktuell.

Dataskyddsombudet förstår och delar delvis bedömningen som förvaltningen anför. Först och främst kan konstateras att samtliga nämnder inom Huddinge kommun är personuppgiftsansvariga för den personuppgiftsbehandling som genomförs inom respektive område. Den som beslutar om ändamål och medel med en personuppgiftsbehandling är personuppgiftsansvarige. Om den personuppgiftsansvarige vill genomföra en personuppgiftsbehandling som riskerar medföra en hög risk för de registrerade ska en konsekvensbedömning utföras. Det är den personuppgiftsansvarige som självständigt ansvarar för detta. En enda konsekvensbedömning kan dock genomföras för bedömning av flera behandlingar som liknar varandra. Det kan vara fallet när en kommunkoncerns nämnder var för sig genomför liknande personuppgiftsbehandlingar, exempelvis när liknande teknik används för att samla in personuppgifter för samma ändamål. Det torde därmed kunna genomföras en gemensam konsekvensbedömning för de personuppgiftsbehandlingar som utförs i och med användandet av Google och Microsoft – förutsatt att det föreligger liknande behandlingar och att syftet med behandlingarna är samma.

Dataskyddsombudet har sökt finna genomförd konsekvensbedömning för det kommunövergripande användandet av Google och Microsoft, dock utan framgång. Därmed kvarstår rekommendationen att genomföra en konsekvensbedömning avseende användandet av Microsoft och Google. Det kan med fördel ske ett kommunövergripande arbete för denna konsekvensbedömning, då det troligtvis sker liknande personuppgiftsbehandlingar för samma ändamål.

Den personuppgiftsansvarige kan utföra egna personuppgiftsbehandlingar som inte är kommunövergripande där Google och Microsoft används som systemstöd. I dessa fall ska den personuppgiftsansvarige utföra en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen om behandlingen kan medföra en hög risk för de registrerade. Förvaltningen har svarat att det under 2025 uppstått en

fråga avseende tilläggstjänster till Google, vilket inte har täckts av befintligt publiceringsavtal. I och med detta har förvaltningen påbörjat en konsekvensbedömning för de aktuella behandlingsaktiviteterna.

Rekommendationen uppfylls delvis.

DSO rekommenderar 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.

Den del av rekommendationen som uppmanar till prioritering av konsekvensbedömning för användandet av Googles tjänster besvaras till viss del ovan. Dataskyddsombudet hänvisar i denna del till rubriken ovan.

Rekommendationen riktad till kommunstyrelseförvaltningen anser dataskyddsombudet sakna relevans för den personuppgiftsansvarige, då kommunstyrelseförvaltningen tillhör en annan personuppgiftsansvariges verksamhet. Denna del av rekommendationen bör enligt dataskyddsombudets mening därför bortses från.

Rekommendationen är delvis uppfylld, delvis inaktuell.

Personuppgiftsincidenter

Under året har det rapporterats in totalt två personuppgiftsincidenter internt inom den personuppgiftsansvariges verksamhet.

Den ena incidenten bestod i att en fysisk handling där uppgifter om en klient inom ekonomiskt bistånd hamnade i akten för en annan klient.

Den andra incidenten bestod i att en medarbetare inom gymnasie- och arbetsmarkandsförvaltningen skickat ett mailsvar till fyra personer. Mailsvaret

innehöll personuppgifter tillhörande frågeställaren och dessa tillgängliggjordes således för obehöriga. Samtliga inblandande informerades om det inträffade och de personer som mottagit det felaktiga mailsvaret ombads radera det.

Ingen av dessa incidenter har ansetts innebära en hög risk för de registrerade och har således inte anmälts vidare till IMY.

Dataskyddsombudet kan konstatera att antalet rapporterade incidenter är lågt. Därför rekommenderar dataskyddsombudet att verksamheten överväger att genomföra utbildningsinsatser för att informera om vad en personuppgiftsincident är samt hur de ska hanteras. Genom att öka medvetenheten om personuppgiftsincidenter och tydliggöra hanteringen kan den personuppgiftsansvarige både undvika allvarliga konsekvenser för de registrerades fri- och rättigheter samt tillsynsmyndighetens korrigerande åtgärder och proaktivt förhindra att allvarliga incidenter ens inträffar.

Identifierade risker utifrån inträffade personuppgiftsincidenter

Då det inte rapporterats mer än två personuppgiftsincidenter samt att dessa inte bedömts som av särskilt betydande art finns inte tillräckligt underlag för dataskyddsombudet att uttala sig om risker utifrån inträffade incidenter i någon större utsträckning.

Den risk som dataskyddsombudet kan belysa är, som ovan nämnts, det låga antalet rapporterade incidenter. Där finns en risk att den personuppgiftsansvarige tappar insyn i problem och brister, vilket i sin tur kan leda till bland annat följande konsekvenser:

- Risk att incidenter inte upptäcks i tid, mindre incidenter som kan leda till större och allvarliga konsekvenser,
- Organisationen inte drar lärdom av eller förbättrar sin verksamhet, att liknande misstag återupprepas,
- Det uppstår en felaktig riskbild genom att ledningen tror att verksamheten fungerar bättre än vad den kanske gör, samt

- Ökad sårbarhet exempelvis i processer och system kan innebära att angripare kan utnyttja dem. Det kan även finnas risker för att personuppgifter exponeras samt att säkerhetsåtgärder inte förbättras.

Det kan således konstateras att om det brister i inrapportering av incidenter saknas underlag för verksamheten att förebygga, åtgärda och utveckla verksamheten.

Rättighetsbegäranden och klagomål

Det har under 2025 inkommit totalt tio ärenden i den e-tjänst som den personuppgiftsansvarige använder sig av som en digital ingång vid begäran av registerutdrag. Endast en av dessa tio begäranden utgjorde en rättighetsbegäran enligt artikel 15. Resterande nio begäranden avsåg andra typer av ärenden, såsom begäran om handlingar avseende egna individärenden (till exempel betygsdokument eller intyg).

Den begäran som avsåg utövande av rätten till tillgång (registerutdrag) besvarades inom den angivna tidsfristen.

Det har vidare inte inkommit några ytterligare rättighetsbegäranden under 2025. Det har inte heller inkommit några klagomål till den personuppgiftsansvarige. Inte heller har den personuppgiftsansvarige varit föremål för något tillsynsärende hos IMY under 2025.

Identifierade risker utifrån rättighetsbegäranden och klagomål

Det låga antalet inkomna rättighetsbegäranden kan bero på att invånare inte känner till sina rättigheter, vilket i sin tur kan bero på att informationen om detta kan vara bristfällig eller otillgänglig.

En ytterligare potentiell risk är att det i vissa fall kan finnas begränsad kännedom om hur rättighetsbegäranden ska identifieras, särskilt då de kan inkomma via olika kanaler och vara utformade på olika vis. Detta kan leda till att begäranden förbises eller hanteras felaktigt, vilket i sin tur riskerar att fördröja handläggning, brista i regel efterlevnad samt påverka de registrerade negativt. Dataskyddsombudet vill

dock vara tydlig med att denna iakttagelse inte nödvändigtvis avser en konstaterad brist i hanteringen, utan en identifierad risk.

Dataskyddsombudet kan även konstatera att det saknas rutiner för hantering av samtliga rättigheter. Den vanligast rättighetsbegäran som inkommer är begäran om registerutdrag (rätten till tillgång) och i detta avseende arbetar dataskydds- och informationssäkerhetssamordnare inom kommunstyrelseförvaltningen med framtagande av rutin som ska fungera på en kommunövergripande nivå.

Dataskyddsombudets löpande arbete

Dataskyddsombudet har löpande under året arbetat med bland annat:

- Bevaka funktionsbrevlåda (dataskyddsombud@huddinge.se) och besvarat inkomna dataskyddsfrågor.
- Gett stöd vid och i vissa fall hanterat personuppgiftsincidenter.
- Deltagit och gett stöd vid konsekvensbedömningar och lämnat synpunkter.
- Deltagit vid diverse möten för att bevaka och ge råd avseende dataskydd.
- Omvärldsbevakning.
- Deltagande vid och samordning av nätverk.
- Deltagit vid konferenser och webinarium.
- Varit kontaktperson gentemot externa registrerade.

Omvärldsbevakning

Utifrån ett dataskyddsperspektiv har 2025 varit ett mycket händelsefullt år. Nedan följer ett urval av de viktigaste händelserna från 2025.

Nya regler om kamerabevakning

Den 1 april 2025 infördes nya regler om kamerabevakning. De nya reglerna innebär i korthet att den som vill bedriva kamerabevakning inte längre behöver ansöka om tillstånd för att bedriva kamerabevakning hos IMY. Den som tidigare behövt ansöka om tillstånd ska själva göra en intresseavvägning mellan bevakningsintresset och den enskildes intresse av att inte bli bevakad.

Intresseavvägningen ska dokumenteras och den som bevakar ska även ha en förteckning med vissa uppgifter om den kamerabevakning som bedrivs (samt den bevakning som har upphört fem år tillbaka i tiden). Den skillnad som de nya reglerna i praktiken innebär är att IMY inte längre bedömer om en bevakning ska tillåtas eller inte i förväg. Det råder samma strikta krav som tidigare – bevakningsintresset måste fortsatt väga tyngre för att bevakningen ska vara tillåten.

Det är även viktigt att ha i åtanke att kamerabevakning utgör en personuppgiftsbehandling som sannolikt kan leda till hög risk för de registrerade. I dessa fall ska även en konsekvensbedömning avseende dataskydd utföras innan ny personuppgiftsbehandling (i detta fall ny kamerabevakning) påbörjas.

EU-kommissionens förslag om ändringar av dataskyddsförordningen

Den 19 november 2025 presenterades EU-kommissionens nya förslag till ”Digital Omnibus”. Detta är ett förslag som kortfattat presenterar ett antal förslag för regellättnader till dagen digitala ramverk, där inkluderat dataskyddsförordningen, AI-förordningen och NIS2. Förslaget innehåller en rad förslag, varav ett urval presenteras nedan.

Avseende dataskyddsförordningen ges förslag om att förtydliga definitionen av ”personuppgift” och vad som faktiskt avses med begreppet. EU-kommissionen hänvisar här också till beslutet i EDPS vs SRB (CJEU, mål C-413/23 EDPS v SRB) och föreslår att det bör förtydligas i vilka fall uppgifter inte ska ses som personuppgifter i sammanhanget där innehavaren av uppgifterna inte kan identifiera en individ.

Det ges även förslag om ändrade tidsfrister inom vilken en personuppgiftsincident ska anmälas till tillsynsmyndighet, där EU-kommissionen vill ändra från dagens 72 timmars frist till 96 timmars frist.

Vidare presenteras förslag rörande konsekvensbedömningar där man bland annat anser att Europeiska dataskyddsstyrelsen (EDPB) ska upprätta och överlämna förslag till lista över vilka behandlingsaktiviteter som kräver och som inte kräver att en konsekvensbedömning genomförs. EDPB föreslås även ta fram en gemensam mall och gemensam metodik för genomförandet av konsekvensbedömningar avseende dataskydd.

Förslaget innebär även ändringar i de registrerades rättigheter, främst rätten till information och tillgång (registerutdrag). EU-kommissionen föreslår bland annat att den personuppgiftsansvarige ska få antingen ta ut en rimlig avgift med hänsyn till de administrativa kostnader för tillhandahållande av information alternativt vägra att agera på en begäran om registerutdrag. Dock ska det vara fråga om att en begäran uppenbart saknar grund, är överdriven eller med beaktande av begäran som sker med repetitiv karaktär.

Observera att ovan inte är en uttömmande redogörelse för förslagen. Det är många aktörer som har uttalat sig om förslagen. IMY till exempel finner både styrkor och risker i förslaget om ändringarna som presenteras avseende dataskyddsförordningen. Det IMY ser som styrkor är bland annat de delar som de kan leda till ökad harmonisering, rättssäkerhet och borttagande av onödig administration, i syfte att stärka EU:s konkurrenskraft. Som exempel välkomnar man kommissionens förslag om möjligheter att behandla biometrisk data för verifiering och en höjning av gränsen för när personuppgiftsincidenter ska anmälas. Samtidigt framförs stark kritik mot förslaget till ändring i definitionen av begreppet personuppgift. Man menar att förslaget inskränker begreppet personuppgift på ett sätt som riskerar att undanta personuppgiftsbehandling från dataskyddsförordningens tillämpningsområde och som går utöver EU-domstolens praxis.

Personuppgiftsincident Miljödata

En leverantör till Huddinge kommun (det är dock inte gymnasie- och arbetsmarknadsnämnden som är personuppgiftsansvarig) drabbades under året av ett antagonistiskt angrepp. Leverantören, Miljödata, tillhandahåller två system till

Huddinge kommun som berördes av attacken. Angriparna tog sig in i leverantörens IT-miljö och tillskansade sig en omfattande mängd information som till slut publicerades på Darknet.

Det ena systemet hanterar disciplinärenden och det andra systemet hanterar sjukfrånvaro och rehabilitering. Det kan dock konstateras att det inte har röjts några känsliga personuppgifter, sett till vad som kan förekomma i systemen såsom läkarintyg. Det som däremot kan konstateras är att det har funnits personer med skyddad identitet inom de läckta uppgifterna. Incidenten berörde cirka 30 000 personer, både nuvarande och tidigare anställda inom Huddinge kommun.

Den tredje november 2025 beslutade IMY att inleda ett flertal granskningar med anledning av IT-angreppet mot Miljödata och de personuppgifter som då läckte. Granskning görs dels mot bolaget Miljödata, dels mot två kommuner och en region.

Granskningen mot Miljödata gäller främst säkerhetsfrågor kopplade till dataintrånget. Granskningen av kommunerna och regionen fokuserar på dess behandling av personuppgifter i Miljödatas system, särskilt gällande vilken typ av uppgifter som behandlats och om vilka personer (exempelvis personer med skyddade personuppgifter, uppgifter om barn samt uppgifter om anställda som sedan länge avslutat sin anställning).

Inom Huddinge kommun arbetas det även med en intern rapport rörande incidenten, dels för att dokumentera det inträffade enligt lagkrav, dels för att lära av det inträffade och utveckla verksamheten.

Rapportering

Återrapportering av genomförda aktiviteter och resultat för arbetet 2026 kommer att ingå i dataskyddsombudets årsrapport för 2026 som presenteras 2027.

Dataskyddsombudet vill avslutningsvis tacka för ett gott samarbete.