Sundsvalls kommun

Dataskyddsombuds granskningsrapport av dataskyddsarbete 2025.

Författad av
Camilla Eriksson
Dataskyddsombud

Med stöd av
Sofia Pinheiro Chipelo
Dataskyddssamordnare

Inledning

Dataskyddsombudet (DSO) har 2025 genomfört en granskning av dataskyddsarbete. Samtliga organisationer har granskats genom enkät skickat av dataskyddsombud.

Granskningen 2025 har fokuserat på nio olika huvudområden:

- Utbildning/medvetenhet/följsamhet och kultur
- Rätt till rättelse
- Rätt till radering
- Register över behandlingar
- Dataskyddsorganisation
- Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal
- Personuppgiftsbiträden och underbiträdens arbete med GDPR
- Tekniska och organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet

Detta har skett som en del av dataskyddsombudets övervakande arbete 2023 och med avsikt till 5års tillsynsplanen[1]. Granskningen har genomförts på liknande sätt hos Sundsvall, Timrå och Ånge kommuns nämnder, bolag och förbund som använder sig av DSO tillhandahållet av Sundsvalls kommun. Granskningsarbetets omfattning berodde naturligtvis på organisationens verksamhet, antal registrerade (anställda, kunder, medborgare), hur många personuppgifter som behandlas, hur stor andel som är känsliga eller skyddsvärda personuppgifter. På grund av det hade granskningen uppdelats på tre olike nivåer: liten, mellan och stor granskning. Granskningens syfte är att kontrollera hur Personuppgiftsansvariga (PUA) arbetar strategiskt med dataskyddsfrågor samt hur det systematiska arbetet med dataskydd är organiserat hos PUA. Dataskyddsombuds rekommendationer har som grund att GDPR ger dataskyddsombud befogenheten att informera samt ge råd till den personuppgiftsansvariga och de anställda som behandlar personuppgifter.

[1] Se ”Tillsynsplan Dataskyddsarbete 2023–2027”

Organisationer som ingick i tillsynen

Sundsvall

Organisation	Namn
Bolag	Mitthem
Bolag	MittSverige Vatten och Avfall AB
Bolag	Servanet
Bolag	SKIFU AB
Bolag	Stadsbacken AB
Bolag	Sundsvall Timrå Airport
Bolag	Sundsvalls Elnät AB
Bolag	Sundsvalls Energi AB
Bolag	Sundsvalls Hamn AB
Bolag	Sundsvalls Oljehamn AB
Förbund	Medelpads räddningsförbund
Nämnd	Barn och utbildningsnämnden
Nämnd	Individ och arbetsmarknadsnämnden
Nämnd	Kommunstyrelsen
Nämnd	Kultur och Fritidsnämnden
Nämnd	Lantmäterinämnden
Nämnd	Miljönämnden
Nämnd	Stadsbyggnadsnämnden
Nämnd	Valnämnden
Nämnd	Vård och omsorgsnämnden
Nämnd	Överförmyndarnämnden

Timrå

Organisation	Namn
Bolag	Timråbo
Nämnd	Barn och utbildningsnämnden
Nämnd	Kommunstyrelsen
Nämnd	Kultur och tekniknämnden
Nämnd	Miljö och byggnadsnämnden
Nämnd	Socialnämnden
Nämnd	Valnämnden

Ånge

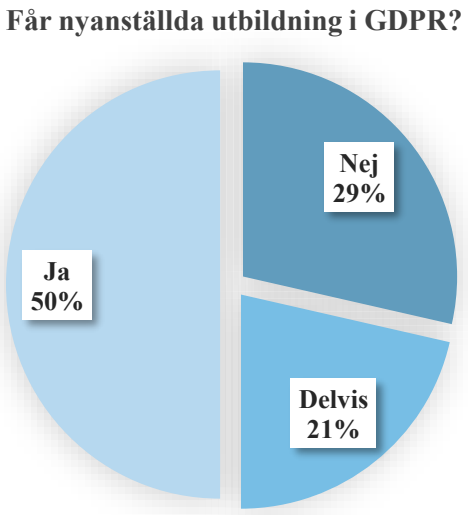
Organisation	Namn
Bolag	Ånge Energi AB
Bolag	Ånge Fastighets och Industri AB
Nämnd	Kommunstyrelsen
Nämnd	Myndighetsnämnden
Nämnd	Valnämnden

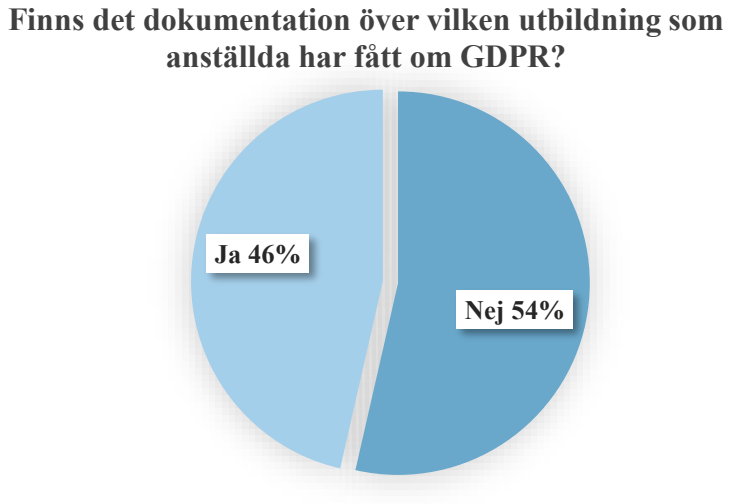
Utbildning/medvetenhet/följsamhet och kultur

Utöver formalia med dokumenterade och beslutade styrdokument och processer är en förutsättning till regelefterlevnad att kunskapsnivån om dataskyddslagstiftningen och interna arbetssätt är tillräckligt hög. Genom att öka medvetenhet och kunskap om personuppgiftshantering så kommer riskerna som finns med hanteringen troligtvis att minska, efterlevnad av regler blir bättre, och acceptansen och förståelsen för dataskyddsfrågor i stort öka.

PUA ska därför skapa relevanta, uppdaterade utbildningar för medarbetare, beroende på roll och arbetsuppgifter samt säkerställa att de har den kompetens och kunskap som krävs för sina arbetsuppgifter.

Av granskningen framgår det att introduktion i dataskydd för nyanställda är begränsad samt ett dåligt resultat på dokumentation av utbildningsinsatser.





Dataskyddsombudets rekommendation

Kommunstyrelsen rekommenderas vidare att säkerställa att utbildning, medvetenhet och följsamhet inom dataskydd bedrivs strukturerat och återkommande. Av granskningen framgår att det saknas dokumentation över genomförda utbildningsinsatser, att introduktion av nyanställda i dataskyddsfrågor inte är likvärdig och att kunskapsnivån varierar mellan verksamheter. För att minska risken för felaktig personuppgiftshantering bör kommunstyrelsen säkerställa att det finns en tydlig kommunövergripande modell för grundläggande och rollanpassad utbildning i dataskydd, att denna genomförs regelbundet samt att deltagande dokumenteras och följs upp.

Det finns även en nyligen framtagen ”5-årig utbildningsplan för informationssäkerhet, cybersäkerhet och dataskydd” som kan också användas som stöd i planeringen för att höja kunskapsnivån i förvaltningen.

Rätt till rättelse

Den registrerades rättigheter regleras av GDPR och omfattar lagstadgade rättigheter som individen kan åberopa gentemot personuppgiftsansvarig (PUA). Rätten till rättelse innebär att den registrerade, under vissa förutsättningar, har rätt att få felaktiga personuppgifter korrigerade samt att få ofullständiga uppgifter kompletterade. Organisationer är skyldiga att möjliggöra detta på ett enkelt och kostnadsfritt sätt, utan onödigt dröjsmål.

Rätt till radering

Rätten till radering, eller ”rätten att bli bortglömd” innebär att registrerade, utifrån vissa förutsättningar, har rätt att få sina personuppgifter raderade. Organisationer behöver dock inte radera personuppgifter om uppgifterna behövs för att fullfölja avtal eller avsluta ett ärende med den registrerade.

Personuppgifterna får inte heller raderas om det finns lagar, förordningar, föreskrifter eller andra offentliga förlägganden som föreskriver annat. Varje registrerad ska underrättas i samband med att deras personuppgifter raderas eller anonymiseras.

Dataskyddsombudets rekommendation

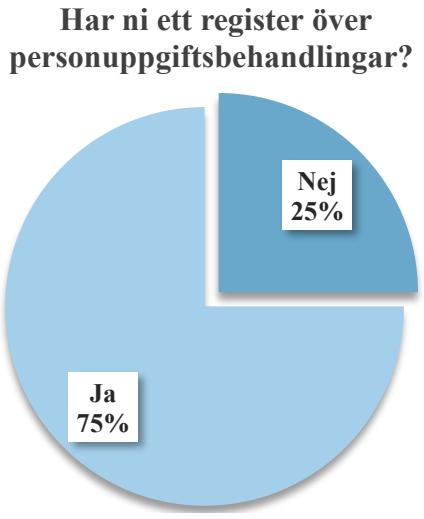
Av resultaten kan det konstateras en avsaknad av fastställda rutiner för hantering av begäran av både rätt till rättelse och radering.

Dataskyddsombud rekommenderar att ett förslag på en skriftlig rutin tas fram på central nivå. Rutinen bör tydliggöra hur en sådan begäran tas emot och handläggas, tidsfrister, bedömning av undantag och hur en sådan begäran dokumenteras. Förvaltningen bör då tillse vem som tar emot och hantera begäran hos sig.

Register över personuppgiftsbehandlingar

Att PUA ska ha en registerförteckning över personuppgiftsbehandlingar är en skyldighet enligt GDPR. En fullständig registerförteckning är en förutsättning för ett godkänt dataskyddsarbete.

Av resultaten framgår att de flesta har en registerförteckning, men att några verksamheter fortfarande behöver arbeta vidare med frågan.



Dataskyddsombudets rekommendation

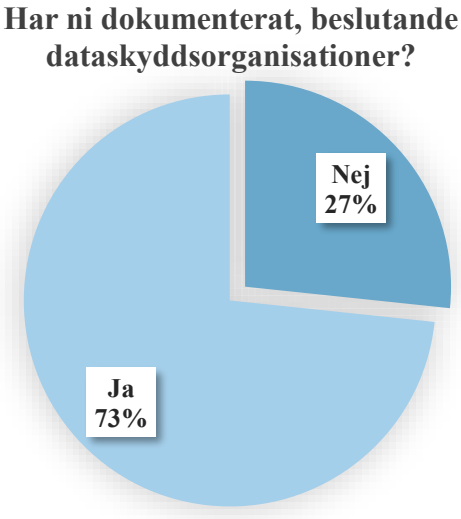
Det rekommenderas att kommunstyrelsen prioriterar färdigställande och löpande förvaltning av registret över personuppgiftsbehandlingar. Registret

är en grundförutsättning för ett fungerande dataskyddsarbete och för att kunna tillgodose registrerades rättigheter. Kommunstyrelsen bör säkerställa att samtliga avdelningar har identifierat och dokumenterat sina behandlingar, att registret hålls aktuellt och att det används aktivt som underlag för riskbedömningar, konsekvensbedömningar och tillsyn.

Dataskyddsorganisation

Enligt dataskyddsförordningen ska den personuppgiftsansvarige tillhandahålla dataskyddsombudet de resurser som krävs för att fullgöra dataskyddsombudets uppgifter. Varje personuppgiftsansvarige bör därför utse personer inom den dagliga verksamheten som ansvarar för dataskyddsarbetet samt organisera deras arbete på ett sådant sätt att krav i dataskyddsförordningen ska uppfyllas.

Av resultaten framgår att de flesta har en dataskyddsorganisation på plats, men att tydlighet saknas när det gäller resurser i form av avsatt tid och ansvarsfördelning.



Dataskyddsombudets rekommendation

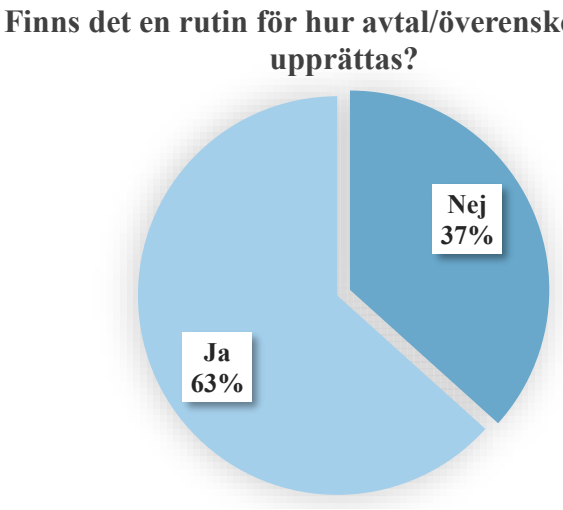
Kommunstyrelsen rekommenderas även att tydliggöra dataskyddsorganisationen genom att dokumentera roller, ansvar och förväntningar kopplat till dataskyddsarbetet. Även om samordnare finns utsedda saknas formella beslut och en samlad beskrivning av hur dataskyddsarbetet ska bedrivas, följas upp och rapporteras.

Reglera personuppgiftsansvar och personuppgiftsbiträdesavtal

PUA och personuppgiftsbiträden ska upprätta ett så kallat personuppgiftsbiträdesavtal om biträden behandlar personuppgifter för PUA:s räkning. GDPR räknar upp vad ett sådant biträdes ska innehålla.

Vid gemensamt personuppgiftsansvar ska ett datadelningsavtal upprättas och inom kommunkoncernen ska personuppgiftsbiträdesavtal benämnas överenskommelser. Alla personuppgiftsbiträdesavtal, datadelningsavtal och överenskommelser ska dokumenteras och vara sökbara.

Av resultaten framgår att vissa verksamheter saknar rutiner för hur ett PUB-avtal ska upprättas samt hur det ska förvaras.



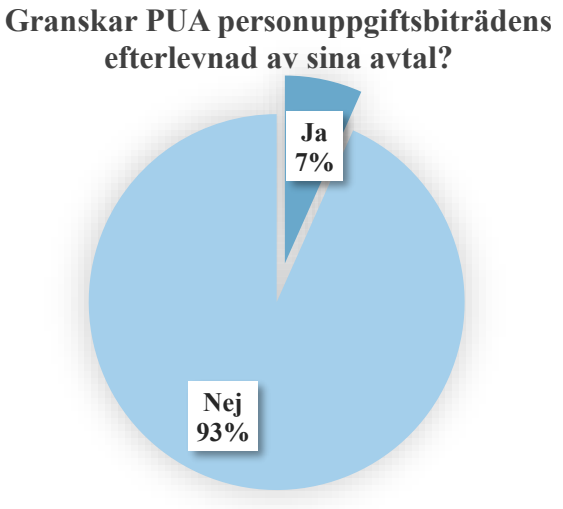
Dataskyddsombudets rekommendation

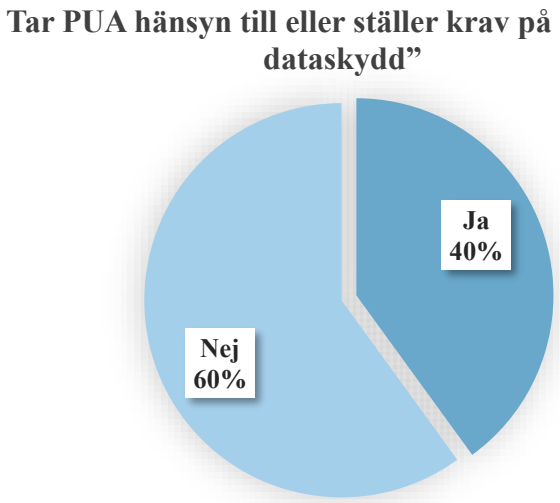
Det finns mallar för personuppgiftsbiträdesavtal tillgängliga på intranätet. Avtal tecknas enligt delegationsordning och sker i samverkan med informationssäkerhets- och dataskyddssamordnare och sparas tillsammans med huvudavtalet. Dataskyddsombud bedömer detta som tillräckligt.

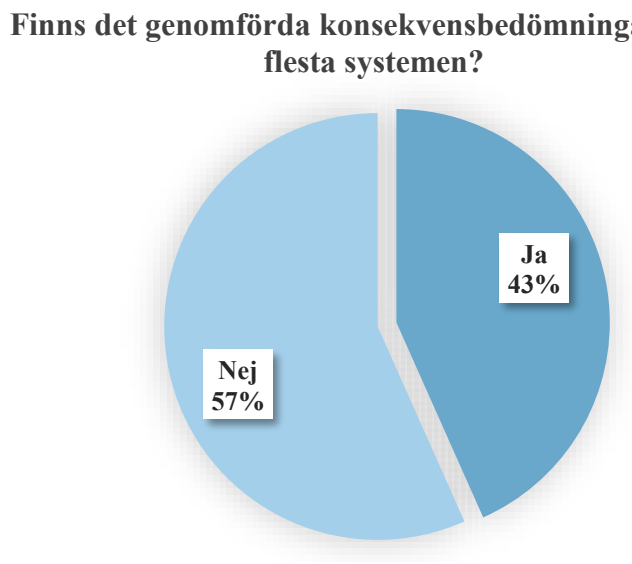
Personuppgiftsbiträden och underbiträden och underbiträdens arbete med GDPR

Enligt GDPR ska PUA enbart anlita personuppgiftsbiträden som kan lämna tillräckliga garantier för att de genomför tekniska och organisatoriska åtgärder som lever upp till kraven i GDPR. PUA ska följa upp att deras personuppgiftsbiträden och underbiträden efterlever de personuppgiftsbiträdesavtal som har ingåtts och kunna vis att kontroller genomförts.

Av resultaten framgår att utfallet av granskningen av personuppgiftsbiträdens efterlevnad av sina avtal är svagt, men att resultaten för genomförda konsekvensbedömningar har förbättrats jämfört med tidigare år.







Dataskyddsombudets rekommendation

Granskningen visar att krav ställs vid upphandling men att efterlevnaden därefter sällan följs upp. Dataskyddsombudet rekommenderar att en dokumenterad och riskbaserad rutin för uppföljning av personuppgiftsbiträden tas fram. Arbetet kan med fördel integreras i befintliga processer för upphandling, systemförvaltning och informationssäkerhet. Vidare bör identifiering av högriskbehandlingar och genomförande av konsekvensbedömningar prioriteras enligt verksamhetsplanen.

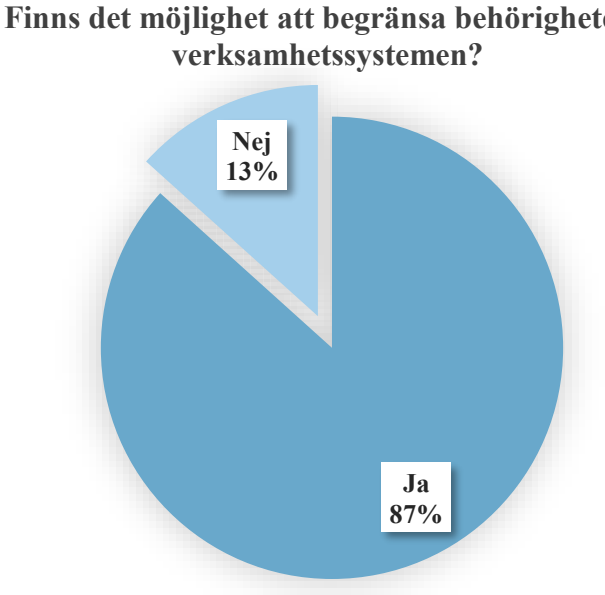
Tekniska och organisatoriska säkerhetsåtgärder, säkerhet och proportionalitet

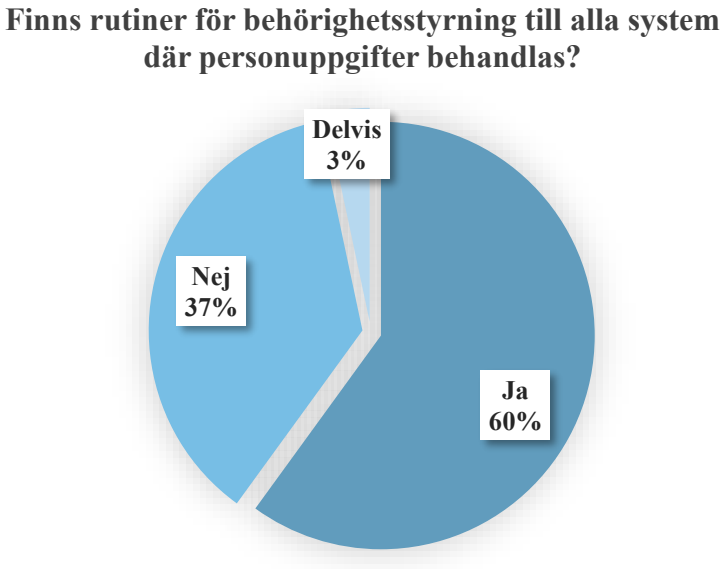
Enligt GDPR ska personuppgifter skyddas med lämpliga tekniska och organisatoriska åtgärder så att de inte blir åtkomliga för obehöriga. Det är PUA:s ansvar att genomföra dessa tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med GDPR.

Den personuppgiftsansvariga ska även se över åtgärder och uppdatera dem vid behov. Exempelvis bör det finnas rutiner för hur behörigheter tilldelas och avslutas och det bör ställas krav på verksamhetssystem att det finns möjlighet att styra behörigheter i dem.

Det ska även finnas en förmåga att fortlöpande säkerställa konfidentialitet, riktighet, tillgänglighet och spårbarhet i behandlingsystem och tjänsterna. Det vill säga att bland annat säkerställa redundans, upprätta brandväggar & antivirus och ha en förmåga att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.

Resultaten av behörighetsstyrningsfrågorna ser överlag positiva ut.





Dataskyddsombudets rekommendation

Det finns rutiner för tilldelning och avslut av behörigheter vid anställning, avslut eller byte av tjänst, men dessa behöver revideras. Verksamhetssystemen ger i huvudsak möjlighet att begränsa behörigheter i de mest kritiska systemen. Där tekniska begränsningar finns kompletteras detta med organisatoriska åtgärder. Rutiner för beställning av behörigheter finns, medan rutiner för uppföljning och avbeställning behöver revideras eller upprättas.

Dataskyddsombudet rekommenderar fortsatt arbete med behörighetsrutiner. Tydliga, dokumenterade rutiner ska säkerställas för samtliga system där personuppgifter behandlas. Uppföljning av behörigheter bör ske regelbundet och dokumenterat.

Dataskyddsombudets uppföljning av fjolårets tillsyn

Enligt GDPR ska Dataskyddsombudet övervaka efterlevnaden av dataskyddsförordningen. Det kan till exempel innebära att dataskyddsombudet samlar in information om hur personuppgifter behandlas i organisationen och utfärdar rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.

Dataskyddsombudets rekommendation

Kommunstyrelsen rekommenderas att fortsatt följa upp och prioritera de åtgärder som kvarstår efter tidigare tillsyner från dataskyddsombudet,

särskilt avseende rättslig grund för behandling, hantering av personuppgiftsincidenter, rätten till information samt behovet av utbildningsinsatser. Ett mer strukturerat arbetssätt för uppföljning av rekommendationer bedöms vara nödvändigt för att säkerställa långsiktig regelefterlevnad och minska risken för brister i hanteringen av personuppgifter inom kommunstyrelsens ansvarsområde.

Reflektioner från Dataskyddsombud

Under 2025 låg fokus på att stärka och effektivisera GDPR-tillämpningen inom EU, bland annat genom nya regler för snabbare hantering av gränsöverskridande ärenden. Flera stora beslut har fattats och mycket höga sanktionsavgifter utfärdats mot stora teknikbolag bekräftade en striktare tillsyn, särskilt kring internationella dataöverföringar och användning av personuppgifter för AI-träning.

Incidenter och tillsyn

I Sverige utfärdade IMY en administrativ sanktionsavgift på 58 miljoner kronor mot Spotify inte gett tillräcklig information om hur personuppgifter hanteras och delats utanför EU när enskilda begär att få tillgång till sina personuppgifter. Den 12 juni 2025 bifaller Kammarrätten överklagan och fastställer sanktionsavgift.

I slutet av augusti 2025 utsattes IT-leverantören Miljödata, som levererar bl.a. systemen Adato, Novi och Stella till många kommuner, regioner och universiteten, för en stor cyberattack. Efteråt publicerades personuppgifter för över 1,5 miljoner personer på Darknet, inklusive namn, personnummer, kontaktuppgifter, hälsodata och andra uppgifter kopplad till anställningen. Flera svenska myndigheter och lärosäten bekräftade att personuppgifter från anställda, tidigare anställda och även barn läckt efter intrånget, och både IMY och polisen utreder händelsen.

IMY och vägledning

Den 18 februari 2025 publicerade IMY vägledning vid konsekvensbedömningar för verksamheter som behandlar personuppgifter. Nya mallar baserade på IMYs vägledning har tagits fram hos oss.

Även en ny rutin, checklista och mall för hantering av begäran av rätt till tillgång har tagits fram hos Sundsvalls Kommun som kan med fördel användas av andra verksamheter.

Från och med den 1 januari 2026 är IMY:s operativa verksamhet indelad i avdelningen för tillsyn och klagomål och avdelningen för vägledning,

innovation och teknik. De nya avdelningarna ska bidra till bl.a. effektivare hantering av klagomål och förstärkning av myndighetens förmåga att ge vägledning och genomföra riskbaserad tillsyn.

Kommissionens förslag om ändringar i GDPR

Den 19 november presenterade den Europeiska kommissionen förslag till ändringar av dataskyddsförordningen, GDPR. De föreslagna ändringarna läggs fram inom ramen för ett bredare paket av ändringar på det digitala området, den digitala omnibussen. Bland förslaget finns det tydligare och mer flexibla regler för användning av personuppgifter i AI-sammanhang, samt enklare hantering av cookies och samtycke. Begreppet av personuppgifter kan uppdateras för att inkludera vissa typer av psedonymiserade data som personuppgifter endast om de kan återidentifieras med rimliga medel. Förslaget innehåller också bättre samordning av incidentrapportering mellan GDPR och andra cybersäkerhetsregler. Målet är att minska administrativ börda utan att formellt sänka integritetsskyddsnivån.