

Swedavia AB

Diarienummer:
IMY-2023-7980

Datum:
2024-06-27

Beslut efter tillsyn enligt dataskyddsförordningen - Swedavia AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att utredningen i ärendet inte visar att Swedavia AB (556797-0801) har brutit i efterlevnaden av artikel 38.6 i dataskyddsförordningen.¹

Ärendet avslutas.

Redogörelse för tillsynsärendet

Bakgrund m.m.

Den europeiska dataskyddsstyrelsen (EDPB) har under 2023 genomfört en samordnad åtgärd² med syftet att undersöka om dataskyddsbuden har den roll samt de resurser som förutsätts enligt artiklarna 37–39 i dataskyddsförordningen. Integritetsskyddsmyndigheten (IMY) har deltagit i den samordnade åtgärden och genomfört den i form av tillsyn mot ett femtiotal personuppgiftsansvariga. Det är mot denna bakgrund som IMY har inlett tillsyn mot Swedavia AB (i fortsättningen "Swedavia" eller "bolaget").

Tillsynen har inledningsvis inneburit att Swedavia har besvarat ett trettiotal frågor om bland annat dataskyddsbudets kvalifikationer, uppgifter och ställning. Frågorna har sin grund i ett frågeformulär som EDPB har skapat inom ramen för den samordnade åtgärden.

Målet med en samordnad åtgärd som denna har varit att i bred mening underlätta gemensamma åtgärder på ett flexibelt men samordnat sätt, allt ifrån att öka den gemensamma medvetenheten och samla in information till att kontrollera verkställighet och utföra gemensamma utredningar. Detta möjliggör riktad uppföljning och åtgärder

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

¹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

² EDPB:s dokument om ram för samordnat genomförande enligt förordning 2016/679. Antaget den 20 oktober 2020.

både på nationell nivå och genom EDPB. Resultatet från granskningen har sammanställts i en rapport från EDPB.³

Av de tillsyner som IMY inlett inom ramen för den samordnade åtgärden har myndigheten gått vidare med ett mindre urval för att göra en fördjupad granskning av några frågeställningar. Denna tillsyn är ett av dessa ärenden där IMY sett anledning att ställa kompletterande frågor till Swedavia, såsom personuppgiftsansvarig, avseende artikel 38.6 i dataskyddsförordningen. Syftet har varit att utreda om det föreligger en intressekonflikt mellan rollen som dataskyddsombud och dataskyddsombudets övriga uppgifter och uppdrag inom organisationen. IMY har inte granskat huruvida Swedavia i övrigt uppfyller artiklarna 37–39 i dataskyddsförordningen utifrån tidigare lämnade svar.

Uppgifter från Swedavia

Swedavia har i huvudsak uppgett följande. Bolagets dataskyddsombud har även haft rollen som bolagets informationssäkerhetschef (CISO). I rollen som informationssäkerhetschef har det inte ingått att ha ansvar för fastställande av ändamålen och medlen för behandlingen av personuppgifter utan rollen har främst varit rådgivande och utbildande. Informationssäkerhetschefen ansvarar för normering, uppföljning, förvaltning, utveckling och kvalitetssäkring inom området Informationssäkerhet för Swedavias verksamhet och flygplatser. Det innebär bland annat att ha en övergripande kunskap om hot och risker samt omvärldsbevakning inom informationssäkerhet. Därtill har informationssäkerhetschefen haft en samverkande roll där denna har haft i uppgift att stötta verksamheten och i synnerhet IT samt dess IT-säkerhetsansvariga i arbetet med att efterleva ledningssystemet och tillämplig lagstiftning generellt. I rollen har även ingått att utforma krav och regler för hur Swedavia arbetar med informationssäkerhet, uppföljning och förvaltning av ledningssystem för Informationssäkerhet (LIS) samt att samordna arbetet inom Swedavia när det gäller informationssäkerhetsfrågor.

Bolaget har haft en dokumenterad rollbeskrivning för de huvudsakliga arbetsuppgifter som åligger dataskyddsombudet för att förhindra att eventuella intressekonflikter uppstår. Informationssäkerhetschefen har inte fattat några beslut eftersom Swedavias organisation har varit strukturerad på ett sådant vis att informationssäkerhetschefen har haft en mer rådgivande roll där slutliga beslut fattas på en högre nivå. I de situationer där informationssäkerhetschefen/dataskyddsombudet misstänkt att en eventuell uppgift skulle kunna leda till en intressekonflikt har detta eskalerats till en högre nivå för att minska sådana risker. Därtill har Swedavia dataskyddskoordinatorer och en bolagsjurist som har arbetat med det löpande dataskyddsarbetet samt tar in externa konsulter vid behov.

Swedavia har i samband med sitt kompletterande svar inkommit med ett internt dokument daterat den 27 oktober 2021 gällande informationssäkerhetschefens befattningsbeskrivning samt en beskrivning av dataskyddsombudets roll som antogs den 29 november 2023.

Bolaget anför att de under 2023, som ett led i sitt dataskyddsarbete, beslutat att separera dataskyddsombudets och informationssäkerhetschefens roller.

³ EDPB:s rapport "2023 Coordinated Enforcement Action, Designation and Position of Data Protection Officers", antagen den 16 januari 2024.

Motivering av beslutet

Tillämpliga bestämmelser m.m.

Rollen som dataskyddsbud regleras i artiklarna 37–39 i dataskyddsförordningen. Dataskyddsbudet ska bland annat informera och ge råd inom organisationen om tillämplig dataskyddslagstiftning, övervaka organisationens efterlevnad av dataskyddslagstiftningen och interna styrdokument, ge råd om konsekvensbedömningar samt vara kontaktperson för tillsynsmyndigheten. Dataskyddsbudet ska vara oberoende och självständig i utförandet av sina arbetsuppgifter.

Dataskyddsbudet får enligt artikel 38.6 i dataskyddsförordningen fullgöra andra uppgifter och uppdrag utöver rollen som dataskyddsbud. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter inte leder till en intressekonflikt.

Av artikel 29-gruppens riktlinjer om dataskyddsbud framgår följande om artikeln:

Kravet att det inte får föreligga intressekonflikter är nära kopplat till kravet att dataskyddsbuden ska kunna agera på ett oberoende sätt. Även om dataskyddsbud får ha andra funktioner, kan de anförtros andra uppgifter och uppdrag endast på villkor att de inte ger upphov till intressekonflikter. Det innebär särskilt att dataskyddsbudet inte kan inneha en sådan tjänst inom organisationen som innebär att han eller hon fastställer ändamålen med och medlen för behandlingen av personuppgifter. Detta måste avgöras från fall till fall beroende på hur organisationen är strukturerad.

Som en tumregel kan motstridiga befattningar inom organisationen vara befattningar i högsta ledningen (t.ex. verkställande direktör, högste verkställande beslutsfattare, finansdirektör, chefsläkare, marknadsföringschef, personalchef eller it-chef), men även andra funktioner lägre i organisationsstrukturen, om sådana befattningar eller funktioner innebär att dataskyddsbudet fastställer ändamålen med och medlen för behandlingen av personuppgifter.⁴

EU-domstolen har i målet X-FAB Dresden förtydligat att dataskyddsbudet inte kan anförtros uppgifter och uppdrag som kan skada fullgörandet av de uppgifter som han eller hon utför i egenskap av dataskyddsbud. Detta eftersom artikel 38.6 i dataskyddsförordningen syftar till att bevara dataskyddsbudets funktionella oberoende och därmed säkerställa effektiviteten hos bestämmelserna i dataskyddsförordningen. Bedömningen av om ett visst uppdrag riskerar att leda till en intressekonflikt med uppdraget som DSO ska göras utifrån relevanta omständigheter i det enskilda fallet, bland annat mot bakgrund av den personuppgiftsansvariges eller personuppgiftsbiträdes organisatoriska struktur och dess interna regler/policys.⁵

Integritetsskyddsmyndighetens bedömning

Den fråga som IMY ska ta ställning till är om det föreligger en intressekonflikt mellan rollen som dataskyddsbud för Swedavia och rollen som bolagets informationssäkerhetschef.

⁴ Artikel 29-gruppens riktlinjer om dataskyddsbud, WP 243 rev. 01, senast granskade och antagna den 5 april 2017, sida 19.

⁵ EU-domstolens dom den 9 februari 2023, X-FAB Dresden, C-453/21, EU:C:2023:79, punkterna 41–42 samt 46.

Enligt vad som framgår ovan kan funktioner som innebär ledande befattningar typiskt sett ge upphov till intressekonflikt med rollen som dataskyddsbud, eftersom det ofta innebär att denne är delaktig i beslut rörande personuppgiftbehandlingar på ett sådant sätt att dataskyddsbudets oberoende kan ifrågasättas. Även andra rollfördelningar som medför att en och samma person tvingas driva frågor med motstridiga intressen och i egenskap av dataskyddsbud granska sitt egna arbete kan, enligt IMY, innebära en intressekonflikt enligt artikel 38.6 i dataskyddsförordningen.

En av dataskyddsbudets viktiga uppgifter är att övervaka efterlevnaden av dataskyddsreglerna. En informationssäkerhetschef är å sin sida vanligtvis ansvarig för att skapa säkerhetsstrategier med särskilda prioriteringar och att skydda organisationens information. Den skyddsvärda informationen kan omfatta personuppgifter. De säkerhetslösningar som organisationen efterfrågar kan stå i motsats till det som skyddet för personuppgifter kräver. De dubbla rollerna kan därför innebära en intressekonflikt i enskilda frågor, men även en risk för att man kan komma att behöva granska sitt egna säkerhetsarbete ur ett dataskyddsperspektiv. Beroende på informationssäkerhetschefens arbetsbeskrivning och typen av verksamhet som det rör sig om, kan rollen som informationssäkerhetschef därför i många fall vara oförenlig med rollen som dataskyddsbud.

Swedavia har uppgett att deras informationssäkerhetschef inte har varit delaktig i fastställande av ändamålen och medlen för behandlingen av personuppgifter och att rollen främst är rådgivande och utbildande. Samtidigt har det av utredningen framkommit att det i informationssäkerhetschefens uppdrag också har ingått att utforma krav och regler för hur bolaget arbetar med informationssäkerhet vilket till viss del talar för att denne varit med och bestämt hur personuppgifter ska behandlas.

Vid en sammantagen bedömning anser dock IMY att det som framkommit i utredningen inte är tillräckligt för att konstatera att det, före det att Swedavia beslutat att separera rollerna, förelegat en intressekonflikt mellan rollen som dataskyddsbud och rollen som informationssäkerhetschef. IMY har särskilt beaktat att Swedavia har haft rutiner och mekanismer för att minska risken för intressekonflikter och extra resurser i form av dataskyddskoordinatorer och en bolagsjurist som löpande arbetat med dataskyddsfrågor.

Ärendet avslutas.

Detta beslut har fattats av enhetschefen Jonas Agnvall efter föredragning av juristen Lucia Trenkler. Vid den slutliga handläggningen har även tillförordnade rättschefen Cecilia Agnehall deltagit

Jonas Agnvall, 2024-06-27 (Det här är en elektronisk signatur)

Kopia till
Dataskyddsbudet

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till IMY. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till IMY inom tre veckor från den dag ni fick del av beslutet. Om ni är en part som företräder det allmänna ska överklagandet dock ha kommit in inom tre veckor från den dag då beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder IMY det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till IMY om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.