Integritetsskydds myndigheten

Diskrimineringsombudsmannen

Diarienummer:
DI-2021-8354

Ert diarienummer:
LED 2021/488

Datum:
2025-04-23

Beslut efter tillsyn enligt dataskyddsförordningen mot Diskrimineringsombudsmannen

Innehåll

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Diskrimineringsombudsmannen har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1] genom att inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter vid användning av webbformuläret för tips och klagomål om diskriminering under perioden den 1 september 2020 till den 17 september 2021.

Integritetsskyddsmyndigheten beslutar med stöd av 6 kap. 2 § dataskyddslagen[2] och artiklarna 58.2 och 83 i dataskyddsförordningen att Diskrimineringsombudsmannen ska betala en administrativ sanktionsavgift på 100 000 (etthundratusen) kronor för överträdelse av artikel 32.1 i dataskyddsförordningen.

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY) beslutade den 6 oktober 2021 att inleda tillsyn mot Diskrimineringsombudsmannen (DO) med anledning av DO:s anmälan den 20 september 2021 av en personuppgiftsincident (IMY:s ärende PUI-2021-4142). Syftet med tillsynen är att granska DO:s behandling av personuppgifter i samband med myndighetens insamling och lagring av personuppgifter när enskilda använder DO:s webbformulär för tips eller klagomål om diskriminering. Tillsynen har bedrivits som en inspektion hos DO den 20 oktober 2021 och efterföljande skriftlig handläggning.

IMY:s prövning i ärendet har avgränsats till att bedöma om DO har efterlevt skyldigheten att vidta lämpliga säkerhetsåtgärder enligt artikel 32.1 i dataskyddsförordningen för personuppgifter som inhämtats via webbformuläret för tips och klagomål om diskriminering under tiden från den 1 september 2020 till den 17 september 2021.

Motivering av beslutet

Tillämpliga bestämmelser m.m.

Med personuppgiftsansvarig avses enligt artikel 4.7 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Behandling av personuppgifter ska följa de grundläggande principerna i artikel 5 i dataskyddsförordningen. Av artikel 5.2 framgår ansvarsskyldigheten, det vill säga att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna efterlevs.

---

[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] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Särskilda kategorier av personuppgifter räknas upp i artikel 9.1 i dataskyddsförordningen, så kallade känsliga personuppgifter. Dessa utgörs av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Enligt artikel 32.1 i dataskyddsförordningen ska både den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Vid bedömningen av vilka tekniska och organisatoriska åtgärder som är lämpliga ska den personuppgiftsansvarige och personuppgiftsbiträdet beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.

Enligt artikel 32.1 omfattar lämpliga skyddsåtgärder, när det är lämpligt,

a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Enligt artikel 32.2 i dataskyddsförordningen ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

I skäl 75 till dataskyddsförordningen anges att vid bedömningen av risken för fysiska personers rättigheter och friheter ska olika faktorer beaktas. Bland annat nämns personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade. I skäl 76 anges att hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är, bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs om behandlingen inbegriper en risk eller en hög risk.

Personuppgiftsansvar

DO har uppgett att myndigheten är personuppgiftsansvarig för de personuppgifter som samlats in via webbformuläret i enlighet med vad DO angett i anmälan av personuppgiftsincident.

Enligt IMY ger utredningen i ärendet stöd för att DO bestämmer ändamål och medel med den aktuella personuppgiftsbehandlingen. IMY delar därför DO:s bedömning att DO är personuppgiftsansvarig enligt artikel 4.7 i dataskyddsförordningen för

behandling av personuppgifter som har samlats in via DO:s webbformulär för tips eller klagomål om diskriminering.

Att DO är personuppgiftsansvarig innebär att myndigheten har ett ansvar för att säkerställa och kunna visa att personuppgifterna behandlas i enlighet med gällande dataskyddsbestämmelser, se artiklarna 5.1 och 5.2 i dataskyddsförordningen, den så kallade ansvarsskyldigheten.

Säkerheten vid behandling av personuppgifter som inhämtats via DO:s webbformulär

DO:s uppgifter i incidentanmälan
I DO:s anmälan av personuppgiftincident den 20 september 2021 beskriver myndigheten incidenten som ett obehörigt röjande av personuppgifter om personer som lämnat in tips eller klagomål via ett webbformulär. Det anges att en utomstående eller registrerad informerade DO om incidenten. Antalet registrerade som påverkats av incidenten uppskattar DO till mellan 101 och 1 000.

DO:s uppgifter i tillsynsärendet m.m.
DO:s uppdrag regleras i lagen (2008:568) om Diskrimineringsombudsmannen, diskrimineringslagen (2008:567), föräldraledighetslagen (1995:584) och förordningen (2008:1401) med instruktion för Diskrimineringsombudsmannen. Det finns verksamhetsspecifik tystnadsplikt för DO:s verksamhet i 33 kap. 1 § offentlighets- och sekretesslagen (2009:400), OSL.

DO har den 22 september 2021 publicerat nyheten ”DO stänger ner webbformuläret för tips och klagomål” där det framgår att DO fått kännedom om ett säkerhetsproblem i sin webbmiljö.

På DO:s webbplats fanns ett webbformulär där enskilda har kunnat lämna tips eller klagomål om diskriminering. Formuläret fanns tillgängligt från den 1 september 2020 fram till att DO fick kännedom om att det kunde finnas ett säkerhetsproblem med koppling till formuläret. Formuläret stängdes den 17 september 2021.

När anmälaren hade fyllt i alla uppgifter kunde den se sina svar på en sammanfattningssida och sedan trycka på skicka. Uppgifterna i det ifyllda webbformuläret har, efter att den enskilde valt att skicka in uppgifterna, förts över krypterat till DO:s diarieföringssystem.

I september 2021 fick DO frågor från en person som hade använt webbformuläret. Frågorna indikerade att det kunde finnas ett säkerhetsproblem med formuläret. DO inledde därför direkt en undersökning för att komma fram till orsaken till det eventuella problemet. Undersökningen visade att det inte var något säkerhetsproblem med själva webbformuläret. Problemet orsakades av att en säkerhetsinställning – som maskerar uppgifter i fritextfält – i analysverktyget (se nedan) inte fungerade som DO utgick från i förhållande till sammanfattningssidan för webbformuläret.

Av nämnda formulär för tips eller klagomål om diskriminering framgick följande.

> ”Ditt tips eller klagomål är viktigt för vårt arbete mot diskriminering. Med hjälp av dina lämnade uppgifter kan vi identifiera problem inom olika samhällsområden där vi behöver agera för att driva på utvecklingen, ge vägledning och öka kunskapen om risker för diskriminering eller där vi behöver agera för att ändra

> lagstiftningen. Vi använder alltså informationen för att få fler att följa lagen och inte primärt för att lösa situationer för enskilda personer.
>
> Allt du rapporterar in här kommer att bli allmän handling som kan begäras ut av allmänheten och lämnas ut efter en sekretessprövning. Vi rekommenderar därför att du inte lämnar fler personuppgifter än vad som är nödvändigt i fritextfälten.”

Formuläret innehöll bland annat ett fritextfält där uppgiftslämnaren kan beskriva vad som hänt. Följande text fanns i anslutning till det fritextfältet.

> ”Beskriv den eller de händelser som gör att du lämnar ett tips eller klagomål till DO. Tala gärna om vilken roll den person som utsatt någon för diskriminering har (till exempel chef, lärare, sjuksköterska eller handläggare) samt om diskrimineringen har skett vid flera tillfällen. Ange inte personer vid namn.”

En obligatorisk uppgift i webbformuläret var att uppgiftslämnaren utifrån förvalda alternativ som rör diskriminering, skulle markera vilket eller vilka alternativ som stämmer överens med de händelser som uppgiftslämnaren beskrivit. Här fanns bland annat alternativen diskriminering som har samband med etnisk tillhörighet, funktionsnedsättning, könsöverskridande identitet och uttryck, religion eller annan trosuppfattning och sexuell läggning. En annan obligatorisk uppgift var att bland förvalda alternativ markera om tipset eller klagomålet handlar om trakasserier, sexuella trakasserier eller repressalier.

I formuläret fanns också ett fritextfält för övrig information eller kommentarer med anvisningen att här kan anges annan relevant information som inte lämnats tidigare i formuläret. Under ”Dina kontaktuppgifter” i formuläret framgick att det är frivilligt att fylla i personuppgifter i formuläret, att uppgiftslämnaren inte behöver lämna sina kontaktuppgifter eller andra personuppgifter för att DO ska kunna ta emot och ha användning av tipset eller klagomålet. Uppgiftslämnaren kunde ange e-post eller telefonnummer eller vara anonym. Det var obligatoriskt att ange om tipset eller klagomålet handlar om händelser som uppgiftslämnaren personligen har blivit utsatt för eller om tipset eller klagomålet handlar om händelser som andra utsatts för.

Vidare fanns en anvisning för ifyllande av webbformuläret där ingivaren rekommenderades att inte lämna fler personuppgifter än vad som är nödvändigt i fritextfälten.

Ändamålet med insamlingen av personuppgifter i webbformuläret var att DO skulle få in underlag för att bedriva tillsyn i enlighet med DO:s uppdrag och att bedriva kunskapsinhämtning som en del av uppdraget.

Anmälningarna kunde innehålla känsliga personuppgifter, men DO hade inför lanseringen av webbformuläret arbetat i ett utvecklingsuppdrag med att minska antalet personuppgifter, vilket framgår i DO:s Uppdragsdirektiv för översyn av användandet av begreppet anmälningar i DO:s verksamhet, daterat den 20 januari 2020. DO arbetade med att utforma frågorna i webbformuläret på ett sätt som gör att myndigheten efterfrågar så få personuppgifter, och framför allt känsliga personuppgifter, som möjligt utifrån principen om uppgiftsminimering.

På DO:s webbplats har ett analysverktyg från ett företag, ett personuppgiftsbiträde, varit installerat. Det fanns ett personuppgiftsbiträdesavtal. När webbformuläret infördes

fanns redan analysverktyget. Verktyget spelade in och sparade olika mätpunkter om användarens session vid besöket på webbplatsen (så kallade ”inspelningar”), till exempel hur en användare navigerar på webbplatsen. På det sättet kunde DO analysera hur webbplatsen användes. Syftet med analysen har varit att optimera och förbättra funktionaliteten på webbplatsen. Verktyget har funnits på hela DO:s webbplats, inklusive på sidan med webbformuläret. Analysverktyget fungerade så att ett slumpmässigt urval besök eller sessioner spridda över dagen spelades in (25 procent av trafiken på webbplatsen).

DO har använt en säkerhetsinställning i analysverktyget som gjorde att information som skrivits i fritextfälten bytts mot asterisker, dvs. stjärntecken. Avsikten med inställningen var att de uppgifter som skrevs in i webbformuläret inte skulle ses i klartext i analysverktyget. Säkerhetsinställningen har fungerat korrekt i webbformulärets alla fritextfält. Däremot har den inte fungerat på formulärets sammanfattningssida, med undantag för rutan för telefonnummer eller mejladress. DO:s undersökning visade att detta berodde på att analysverktyget uppfattade sammanfattningssidan som vilken webbsida som helst. Det kan inte uteslutas att den som lämnat uppgifterna har skrivit uppgifter om mejladress och/eller telefonnummer i något annat fritextfält.

Med anledning av att den funktion som DO använt sig av inte har fungerat för sammanfattningssidan har personuppgifter från det aktuella formuläret förts över och lagrats hos personuppgiftsbiträdet, vilket inte var avsikten.

Personuppgiftsbiträdet har uppgett för DO att all kommunikation mellan analysverktyget och lagringsytan var krypterad med TLS 1.2. Lagringen var krypterad med AES-256.

Internt på DO har det enbart varit en behörig person som hade inloggningsuppgifter till analysverktyget. Exempel på andra åtgärder hos DO var att kryptering har använts både för formuläret och för överföring till DO:s registratorsfunktion. Formuläret var placerat på DO:s egna servar och bakom brandvägg.

Under den aktuella 12-månadersperioden inkom cirka 5 400 tips och klagomål till DO, av vilka merparten inkom via webbformuläret. DO:s bedömning är att analysverktyget förde över cirka 500 tips och klagomål som kunnat innehålla personuppgifter. En person kunde skriva allt ifrån en sida fritext till 40 sidor fritext. Personuppgifter om barn under 18 år kunde förekomma, exempelvis namn på elever. Andra exempel var namn på anställda på viss arbetsplats.

Personuppgiftsbiträdet har till DO skriftligen bekräftat att de inte har tagit del av personuppgifter eller annan information på sammanfattningssidan. De har även informerat om att det enligt deras policy för dataklassificering endast är personal hos dem som har ett reellt och faktiskt verksamhetsbehov som kan komma åt sådan information som genereras av verktyget och endast för support och underhåll. Åtkomst ges baserat på en så kallad "Change Request" och granskas och godkänns beroende på roll.

Vid tidpunkten för incidenten hade DO styrdokumenten *Informationssäkerhetspolicy* och *Rutin för registrering av system som innehåller personuppgifter*. Sist nämnda dokument har 2023 ersatts av *Rutin för hantering av personuppgifter vid inköp*. Numera finns också *Riktlinjer för dataskydd*, som kodifierat och tydliggjort hur DO ska arbeta med dataskydd. Innan lanseringen av webbformuläret gjorde DO en riskanalys i

enlighet med gällande rutin och det konstaterades innan lanseringen bland annat att säkerhetsinställningen i analysverktyget behövde vara aktiverad.

För att säkerställa att de tekniska och organisatoriska säkerhetsåtgärder som beslutas också genomförs, har DO ett antal rutiner som bidrar till uppföljning. Avtalsansvariga följer löpande upp sina avtal och för en dialog med leverantören om det uppkommer frågor som behöver lösas, t.ex. avseende personuppgiftsbehandling. Dataskyddsombudet gör årligen en uppföljning av myndighetens dataskyddsarbete där det uppmärksammas om det finns något område eller någon fråga som DO måste arbeta med för att ytterligare förbättra sitt arbete med dataskydd. DO:s medarbetare känner till de rutiner som finns på myndigheten och flaggar upp om något sker som inte är i enlighet med dessa rutiner. Till exempel agerade DO direkt när en medarbetare fick frågor som indikerade att det kunde finnas ett problem med webbformuläret. Detta visar att rutinerna för uppföljning har fungerat även vad gäller webbformuläret.

Efter att filerna hade exporterats krypterat från personuppgiftsbiträdet till DO gav DO ytterligare instruktion till biträdet att filerna skulle raderas hos biträdet. Den 15 december 2021 har biträdet bekräftat att de har raderat filerna i enlighet med DO:s instruktion. Filerna som har funnits hos personuppgiftsbiträdet får enligt DO därmed anses vara gallrade vid denna tidpunkt. Innehåll i analysverktyget har gallrats manuellt av en medarbetare på DO. Samtliga gallringsåtgärder var klara den 21 december 2021. DO sade upp avtalet med personuppgiftsbiträdet den 15 februari 2022. Verktyget avaktiverades dock redan den 18 september 2021.

IMY:s bedömning

Behandlingen har krävt en hög säkerhetsnivå
Av utredningen framgår att DO utifrån myndighetens uppdrag gällande diskriminering har använt ett webbformulär för att samla in personuppgifter som relaterar till diskriminering i form av tips och klagomål. Detta har skett genom att uppgiftslämnaren har kunnat beskriva vad som har hänt i fritextfält och som obligatorisk uppgift genom förvalda alternativ ange vilken typ av diskriminering som avses. Här fanns bland annat alternativen diskriminering som har samband med etnisk tillhörighet, funktionsnedsättning, könsöverskridande identitet och uttryck, religion eller annan trosuppfattning och sexuell läggning. Uppgiftslämnaren av ett tips eller klagomål har kunnat uppge sin e-postadress eller namn. Personuppgifter om barn kunde förekomma, exempelvis namn på elever. Andra exempel på personuppgifter var namn på anställda på viss arbetsplats. Tips och klagomål kunde handla om händelser som andra än ingivaren av webbformuläret blivit utsatta för. Uppgifterna kunde omfattas av lagstadgad tystnadsplikt enligt 33 kap. 1 § OSL.

DO är i egenskap av personuppgiftsansvarig skyldig att vidta lämpliga säkerhetsåtgärder. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, se artikel 32.1 och 32.2 i dataskyddsförordningen. Att säkerställa en lämplig säkerhet innebär att säkerhetsnivån måste anpassas till riskerna med den aktuella behandlingen.

IMY konstaterar att känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen bland annat utgörs av personuppgifter som avslöjar ras eller etniskt ursprung, religiös eller filosofisk övertygelse, uppgifter om hälsa och uppgifter om en fysisk persons

sexualliv eller sexuella läggning. Webbformuläret kunde användas för tips eller klagomål om diskrimineringsgrunderna som bland annat omfattar könsöverskridande identitet eller uttryck, etnisk tillhörighet, religion eller annan trosuppfattning, funktionsnedsättning och sexuell läggning.[3] Personuppgifter kopplade till diskrimineringsgrunderna utgör därmed många gånger även känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen. Behandling som omfattar känsliga personuppgifter medför normalt sett högre risker. Vidare förtjänar barns personuppgifter särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter.[4]

IMY konstaterar att DO har samlat in personuppgifter, även känsliga personuppgifter, som kan omfattas av tystnadsplikt. Under den aktuella tidsperioden inkom cirka 5 400 tips eller klagomål där merparten inkom via webbformuläret. Ingivaren av formuläret kunde skriva upp till 40 sidor fritext och därvid även beskriva händelser som avsåg andra personer än ingivaren själv. Uppgiftslämnare som använt webbformuläret eller andra enskilda som omnämnts i webbformuläret får anses ha en hög förväntan på att obehöriga inte ska kunna få del av deras personuppgifter.

Sammanfattningsvis bedömer IMY att personuppgiftsbehandlingens art, omfattning och sammanhang inneburit sådana risker att höga krav måste ställas på de säkerhetsåtgärder som behöver vidtas enligt artikel 32.1 i dataskyddsförordningen avseende behandlingen av personuppgifter som samlas in via webbformuläret.

DO har inte vidtagit tillräckliga åtgärder för att skydda uppgifterna
IMY konstaterar att det under tiden från den 1 september 2020 till den 17 september 2021 saknades en säkerhetsinställning som skyddade personuppgifter i webbformulärets sammanfattningssida, med undantag för fälten för telefonnummer och mejladress. Det ledde till att personuppgifter från webbformulärets sammanfattningssida överfördes till personuppgiftsbiträdet.

Enligt IMY innebär redan det förhållande att DO oavsiktligt överfört de aktuella uppgifterna till personuppgiftsbiträdet att uppgifterna rent faktiskt inte har skyddats mot obehörigt röjande. DO har också i sin anmälan om personuppgiftsincident angett att säkerhetsincidenten bestått i ett obehörigt röjande.

Av utredningen i ärendet framgår att DO haft rutiner för bland annat registrering av system som innehåller personuppgifter och att DO inför lanseringen av webbformuläret beslutade att vidta ett antal åtgärder för att skydda personuppgifter som samlades in via webbformuläret. Innan lanseringen konstaterade DO bland annat att säkerhetsinställningen i analysverktyget behövde vara aktiverad. Det säkerställdes dock inte att inställningen fungerade fullt ut. De åtgärder som DO vidtog var därför inte tillräckliga för att skydda personuppgifterna från att röjas för personuppgiftsbiträdet.

Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och -tjänster är enligt artikel 32.1 b i dataskyddsförordningen en åtgärd som kan vara lämplig när det gäller att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. En annan åtgärd som kan vara lämplig när det gäller att säkerställa en säkerhetsnivå som är lämplig i förhållande

[3] Diskrimineringslagen (2008:567) har till ändamål att motverka diskriminering och på andra sätt främja lika rättigheter och möjligheter oavsett kön, könsöverskridande identitet eller uttryck, etnisk tillhörighet, religion eller annan trosuppfattning, funktionsnedsättning, sexuell läggning eller ålder.
[4] Skäl 38 till dataskyddsförordningen.

till risken är enligt artikel 32.1 d i dataskyddsförordningen ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

IMY konstaterar att DO vidtog utredningsåtgärder när DO fick frågor från en utomstående som indikerade att det kunde finnas ett säkerhetsproblem med webbformuläret. DO har visserligen uppgett att myndigheten har rutiner för uppföljning av säkerhetsåtgärder. Dessa rutiner har dock inte varit tillräckliga för att DO skulle kunna upptäcka och åtgärda säkerhetsbristen under den aktuella tiden. Enligt IMY:s bedömning har DO därmed under tiden från den 1 september 2020 till den 17 september 2021 saknat ett effektivt systematiskt säkerhetsarbete som gjort det möjligt att upptäcka säkerhetsbristen och det obehöriga röjandet.

DO har således behandlat personuppgifter i tips eller klagomål om diskriminering i webbformulärets sammanfattningssida utan att i tillräcklig utsträckning skydda personuppgifterna mot obehörigt röjande under den aktuella tiden. DO har därför inte iakttagit sin skyldighet som personuppgiftsansvarig att vidta lämpliga tekniska och organisatoriska åtgärder som säkerställt en säkerhetsnivå som är lämplig i förhållande till risken i enlighet med artikel 32.1 i dataskyddsförordningen.

Val av ingripande

Tillämpliga bestämmelser m.m.

Vid överträdelser av dataskyddsförordningen har IMY ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen, bland annat reprimand, föreläggande och sanktionsavgifter. Av artikel 83.2 framgår att IMY ska påföra administrativa sanktionsavgifter utöver eller i stället för de andra åtgärder som avses i artikel 58.2 beroende på omständigheterna i det enskilda fallet.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 i dataskyddsförordningen.

Medlemsstaterna får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter. Det framgår av artikel 83.7 i dataskyddsförordningen. Av 6 kap. 2 § dataskyddslagen framgår att IMY får ta ut sanktionsavgifter av myndigheter vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i dataskyddsförordningen och att artikel 83.1, 83.2 och 83.3 i förordningen då ska tillämpas.

I artikel 83.2 i dataskyddsförordningen anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras och vad som kan påverka sanktionsavgiftens storlek. Av betydelse för bedömningen av överträdelsens allvar är bland annat dess karaktär, svårighetsgrad och varaktighet. EDPB har antagit riktlinjer om beräkning av administrativa sanktionsavgifter enligt dataskyddsförordningen som syftar till att skapa en harmoniserad metod och principer för beräkning av sanktionsavgifter.[5] Riktlinjerna kan tillämpas på beräkningen av sanktionsavgifter som ska åläggas offentliga myndigheter och organ.[6]

[5] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR.
[6] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 10.

Om det är fråga om en mindre överträdelse får IMY enligt skäl 148 till dataskyddsförordningen i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 52.2 b i förordningen.

DO:s uppgifter

DO har i huvudsak uppgett följande avseende korrigerande åtgärder.

Behandlingen har inte inneburit någon risk för obehörigt röjande eller obehörig åtkomst till de aktuella uppgifterna. Uppgifterna har överförts krypterat till personuppgiftsbiträdet och har lagrats krypterat i databasen. Informationen i databasen är endast datapunkter som har samlats in från användarens webbläsarsession. För att kunna ta del av uppgifterna krävs att informationen spelas upp i verktyget, vilket förutsätter en aktiv koppling mellan webbläsaren och databasen. Uppgifterna har därför inte lagrats i läsbart skick och har inte heller varit sökbara. Personuppgiftsbiträdet har dessutom bekräftat till DO att ingen personal hos dem har haft åtkomst till de aktuella uppgifterna.

Behandlingen har inte heller inneburit att någon extern mottagare, som agerar som personuppgiftsansvarig, har fått del av uppgifterna för sin egen efterföljande behandling för egna ändamål. Detta eftersom personuppgiftsbiträdet har behandlat uppgifterna som ett personuppgiftsbiträde på uppdrag av DO inom ramen för DO:s personuppgiftsansvar och endast enligt DO:s instruktioner. Det kan således konstateras att det i detta fall inte har varit fråga om ett okontrollerat röjande av uppgifter med många mottagare eller publik spridning.

Behandlingen har varit begränsad i sin omfattning och endast berört ett fåtal registrerade individer. Det aktuella formuläret fanns på DO:s webbplats under en förhållandevis begränsad tid.

DO har vidtagit skyddsåtgärder för att säkerställa de registrerades fri- och rättigheter innan webbformuläret för tips och klagomål lanserades. Så snart det blev känt att fler uppgifter än avsett fördes över till personuppgiftsbiträdet tog DO bort verktyget. DO säkerställde också att uppgifterna togs bort av personuppgiftsbiträdet.

Om IMY bedömer att DO inte uppfyllt kraven i artikel 32.1 i dataskyddsförordningen ska överträdelsen ses som en mindre överträdelse där reprimand är en tillräcklig korrigerande åtgärd. Detta särskilt mot bakgrund av att behandlingen i praktiken inte har inneburit någon risk för berörda registrerade individer och att DO har vidtagit flera åtgärder med anledning av det inträffade.

Om IMY ändå skulle bedöma att en sanktionsavgift ska påföras ska en eventuell överträdelse av kraven i artikel 32.1 i dataskyddsförordningen under alla förhållanden anses ha en mycket låg allvarlighetsgrad av de skäl som har angivits ovan.

IMY:s bedömning

Sanktionsavgift ska påföras
IMY har bedömt att DO har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Överträdelsen har skett genom att DO har behandlat personuppgifter under drygt ett års tid med en otillräcklig säkerhetsnivå. Den otillräckliga säkerhetsnivån har lett till

obehörigt röjande av personuppgifter som kunde vara känsliga eller omfattas av tystnadsplikt. DO har under denna tid saknat förmåga att upptäcka det pågående röjandet av personuppgifterna. IMY bedömer att det inte rör sig om sådana mindre överträdelser som avses i skäl 148 till dataskyddsförordningen.

EU-domstolen har klargjort att det krävs att den personuppgiftsansvarige har begått en överträdelse uppsåtligen eller av oaktsamhet för att administrativa sanktionsavgifter ska kunna påföras enligt dataskyddsförordningen. EU-domstolen har uttalat att personuppgiftsansvariga kan påföras sanktionsavgifter för ageranden om de inte kan anses ha varit okunniga om att agerandet utgjorde en överträdelse, oavsett om de varit medvetna om att de åsidosatte bestämmelserna i dataskyddsförordningen.[7]

Enligt principen om ansvarsskyldighet som bland annat kommer till uttryck i artikel 5.2 i dataskyddsförordningen ska den som ansvarar för behandlingen av personuppgifter säkerställa och kunna visa att behandlingen är förenlig med dataskyddsförordningen. IMY konstaterar att DO ansvarar för att personuppgifter som samlats in i verksamheten behandlas på ett sätt som säkerställer en lämplig säkerhetsnivå. IMY har vid sin prövning konstaterat att DO inte levt upp till de krav som dataskyddsförordningen ställer i dessa avseenden. DO kan inte anses ha varit okunnig om att myndighetens agerande inneburit överträdelser av förordningen. Det föreligger därmed förutsättningar för att påföra DO en administrativ sanktionsavgift.[8]

Sanktionsavgiftens storlek
Av 6 kap. 2 § dataskyddslagen framgår att sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen och till högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5 och 83.6. Överträdelser av artikel 32 omfattas av den lägre sanktionsavgiften.

Av EDPB:s riktlinjer framgår att tillsynsmyndigheten ska bedöma om överträdelsen är av låg, medelhög eller hög allvarlighetsgrad enligt artikel 83.2 a, b och g i dataskyddsförordningen.[9] Vid bedömningen av överträdelsens allvarlighetsgrad tar IMY hänsyn till följande omständigheter.

Att det saknades en säkerhetsinställning för sammanställningen av fritextfälten och att DO saknat förmågan att upptäcka överföringen av uppgifterna ledde till en personuppgiftsincident som pågick under cirka ett års tid, dvs. under en längre tid. Som framkommit ovan bedömer IMY att redan det förhållande att personuppgifterna överförts till personuppgiftsbiträdet innebär att det skett ett obehörigt röjande. Att det varit fråga om överföring till ett personuppgiftsbiträde förändrar inte detta förhållande, i synnerhet med beaktande av att DO:s avsikt aldrig var att uppgifterna skulle föras över till det personuppgiftsbiträdet. Personuppgiftsbehandlingen innefattade beskrivningar av händelser om diskriminering som förknippas med någon eller några av diskrimineringsgrunderna. Behandlingen har omfattat cirka 500 tips och klagomål som kunde innehålla personuppgifter och det gick att skriva 40 sidor fritext i webbformuläret. Beskrivningar av händelser som rör diskriminering är av personlig karaktär. Det har varit fråga om känsliga personuppgifter i en verksamhet där uppgifterna också kan omfattas av tystnadsplikt.

---

[7] EU-domstolens dom i mål C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos mot Valstybinė duomenų apsaugos inspekcija av den 5 december 2023, punkt 81 och dom i mål C-807/21 Deutsche Wohnen av den 5 december 2023, punkt 76.
[8] Se för bedömningen av oaktsamhet även Kammarrätten i Stockholms dom den 11 mars 2024 i mål 2829-23 s.12.
[9] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 60.

Enskilda personer som utsatts för diskriminering som exempelvis barn och arbetstagare, får anses ha en berättigad förväntan på hög konfidentialitet och på att deras personuppgifter inte röjs.

Överträdelsen i form av bristande tekniska och organisatoriska åtgärder har inneburit en risk för att obehöriga tar del av de registrerades personuppgifter.

IMY bedömer sammanfattningsvis att överträdelsen ska betraktas som mer allvarlig än om ovanstående omständigheter inte förelegat. I ärendet har dock även framkommit omständigheter som talar för att överträdelsen ska bedömas som mindre allvarlig.

IMY konstaterar att DO vid tidpunkten för överträdelsen hade vidtagit ett antal lämpliga tekniska och organisatoriska åtgärder, exempelvis skedde överföringen av uppgifter från webbformuläret till personuppgiftsbiträdet genom krypterad överföring. Det rörde sig därmed inte om ett okontrollerat röjande där uppgifterna exempelvis var åtkomliga via internet. Det kan också konstateras att det i ärendet är fråga om överföringar som skett till en aktör som behandlar uppgifterna i egenskap av personuppgiftsbiträde i förhållande till DO.

Vidare hade DO i anvisning för ifyllande av webbformuläret rekommenderat ingivaren att inte lämna fler personuppgifter än vad som är nödvändigt i fritextfälten. DO hade också i arbetet inför lanseringen av webbformuläret identifierat säkerhetsinställningen i analysverktyget som en lämplig säkerhetsåtgärd och aktiverade denna med avsikten att den skulle fungera även avseende sammanfattningssidan.

Det har inte heller framkommit att personuppgiftsbiträdet faktiskt tagit del av personuppgifterna som överförts.

Vid en samlad bedömning mot bakgrund av ovanstående omständigheter bedömer IMY att det rör sig om en överträdelse av artikel 32.1 i dataskyddsförordningen av låg allvarlighetsgrad.

IMY ska också bedöma om det föreligger några försvårande eller förmildrande omständigheter som får betydelse för sanktionsavgiftens storlek.

IMY konstaterar att DO efter incidenten vidtog åtgärder genom att upphöra med insamlingen av personuppgifter via webbformuläret för tips och klagomål och genom att kontakta personuppgiftsbiträdet för att utreda incidenten. DO säkerställde även att biträdet upphörde med behandlingen av personuppgifterna. Information om incidenten lämnades genom att DO publicerade en nyhet på myndighetens webbplats. IMY bedömer att dessa åtgärder inte kan anses gå utöver vad som förväntas av DO i det aktuella fallet. De vidtagna åtgärderna utgör därför enligt IMY inte någon förmildrande faktor.

IMY bedömer att det, utöver de omständigheter som beaktats ovan, saknas försvårande eller förmildrande omständigheter som påverkar sanktionsavgiften.

Mot bakgrund av överträdelsernas allvar bestämmer IMY den administrativa sanktionsavgiften till 100 000 kronor för överträdelsen. IMY bedömer att detta belopp är effektivt, proportionerligt och avskräckande.

Detta beslut har fattats av enhetschefen Linn Sandmark efter föredragning av avdelningsdirektören Suzanne Isberg. Vid den slutliga handläggningen har även it- och informationssäkerhetsspecialisten Petter Flink och avdelningsjuristen Andreas Persson medverkat.

Linn Sandmark

Bilaga
Information om betalning av sanktionsavgift

Kopia till
dataskyddsombud@do.se

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.