Diarienummer:
IMY-2025-21177

Datum:
2026-09-22

Beslut efter tillsyn enligt dataskyddsförordningen – Miljödata i Karlskrona Aktiebolag

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Miljödata i Karlskrona Aktiebolag (556324-4036) har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.[1]

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Miljödata i Karlskrona Aktiebolag ska betala en administrativ sanktionsavgift på 1 800 000 kronor för överträdelsen av artikel 32.1 i dataskyddsförordningen.

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).

Sammanfattning

Miljödata i Karlskrona Aktiebolag (Miljödata) är en leverantör av digitala systemstöd inom personal- och arbetsmiljöhantering. Miljödata tillhandahåller webbaserade tjänster till kunder för hantering av bland annat sjukfrånvaro, rehabilitering och tillbud. I augusti 2025 utsattes bolaget för ett dataintrång av en extern angripare som tog del av information som den saknade behörighet till i tjänsterna (obehörig åtkomst). Intrånget upptäcktes av Miljödata som den 26 augusti 2025 anmälde personuppgiftsincidenten till IMY. Efter incidenten identifierade Miljödata att det fanns indikationer på att hotaktören extraherat data från systemen och den läckta informationen, som innehöll personuppgifter, publicerades kort tid därefter på Darknet.

IMY har granskat om Miljödata innan och vid tidpunkten för personuppgiftsincidenten hade vidtagit lämpliga tekniska och organisatoriska åtgärder enligt artikel 32.1 i dataskyddsförordningen för att skydda personuppgifterna som behandlas i tjänsterna. Granskningen visar att personuppgiftsbehandlingen har krävt en hög säkerhetsnivå och att Miljödata inte har vidtagit tillräckliga åtgärder för att säkerställa att personuppgifterna som behandlats i bolagets tjänster skyddats mot risken för obehörigt röjande eller obehörig åtkomst till följd av dataintrång. Bolaget har inte heller vidtagit tillräckliga säkerhetsåtgärder genom att inte ha automatisk realtidsövervakning för att identifiera hot i form av exempelvis misstänkt aktivitet och intrång eller intrångsförsök som kan leda till obehörig åtkomst.

IMY bedömer att Miljödata har varit oaktsamt i förhållande till den överträdelse av dataskyddsförordningen som konstaterats och att samtliga övriga förutsättningar för att påföra Miljödata en sanktionsavgift är uppfyllda. IMY beslutar att Miljödata ska betala en administrativ sanktionsavgift på 1 800 000 kronor för överträdelsen av artikel 32.1 i dataskyddsförordningen. Vid bestämmandet av sanktionsavgiftens storlek har överträdelsens höga allvarlighetsgrad och företagets omsättning beaktats. IMY bedömer att beloppet är effektivt, proportionerligt och avskräckande.

Redogörelse för tillsynsärendet

Bakgrund

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn mot Miljödata i Karlskrona Aktiebolag (Miljödata) med anledning av en personuppgiftsincident som inträffade den 20 augusti 2025 och anmäldes av Miljödata till IMY den 26 augusti 2025.

Miljödata är en leverantör av digitala systemstöd inom personal- och arbetsmiljöhantering. Bolaget tillhandahåller webbaserade tjänster (tjänsterna) i huvudsak för hantering av sjukfrånvaro, rehabilitering, tillbud och för arbetsmiljöarbete till såväl privata som offentliga kunder. Majoriteten av de registrerade i tjänsterna utgörs av anställda hos Miljödatas kunder.

Av Miljödatas anmälan om personuppgiftsincident framgår bland annat att bolaget har utsatts för ett dataintrång av en extern angripare (hotaktören) och att hotaktören har tagit del av information som den saknade behörighet till i tjänsterna (obehörig åtkomst). Intrånget upptäcktes den 23 augusti 2025 efter att ett tekniskt larm om fel i tjänsterna utlöstes i it-driften.

IMY:s prövning i ärendet gäller frågan om Miljödata innan och vid tidpunkten för personuppgiftsincidenten hade vidtagit lämpliga tekniska och organisatoriska åtgärder enligt artikel 32.1 i dataskyddsförordningen för att skydda personuppgifterna som behandlas i tjänsterna.

Vad Miljödata har uppgett

Miljödata anser att bolaget inte på något sätt har behandlat personuppgifter i strid med dataskyddsförordningen och har därutöver uppgett i huvudsak följande.

Sammanfattning av intrånget
Den 20 augusti 2025 inleddes en ransomware-attack mot Miljödata genom att hotaktören tillskansade sig tillgång till Miljödatas tjänster. Detta skedde genom att hotaktören utförde en så kallad SQL-injektion[2] mot en stödkomponent till en brandväggslösning som Miljödata installerat på en server i sin tekniska miljö. Genom SQL-injektionen fick hotaktören tillgång till Miljödatas server och kunde eskalera sina privilegier och tilldela sig högsta rättigheter i systemet. Natten till den 23 augusti 2025 påbörjade hotaktören kryptering av flera servrar och extraherade därefter informationen. På eftermiddagen den 23 augusti 2025 utlöstes tekniska larm om fel i tjänsten och Miljödata påbörjade omedelbart isolering av samtliga servrar. Den 2 september 2025 identifierade Miljödata genom sin utredning av incidenten att det fanns indikationer på att hotaktören extraherat data från systemen. Den 14 september 2025 publicerade hotaktören delar av den läckta informationen, som innehöll personuppgifter, på Darknet.

Orsak till intrånget och dess omfattning
Miljödatas forensiska utredning har visat att hotaktörens tillvägagångssätt bestod i ett utnyttjande av en sårbarhet i en stödkomponent till en brandväggslösning som Miljödata köpt från en välrenommerad leverantör av sådana produkter. På grund av

[2] IMY:s förklaring: En SQL-injektion är en metod för dataintrång som utnyttjar en sårbarhet i SQL. SQL är ett programmeringsspråk som används för att ställa frågor till relationsdatabaser och för att ändra och uppdatera databaser.

sårbarheten kunde hotaktören bereda sig tillträde till Miljödatas tekniska miljö genom en SQL-injektion.

Stödkomponenten till brandväggslösningen installerades på Miljödatas server cirka sju dagar före incidenten. Vid leverans av stödkomponenten försåg leverantören Miljödata med en utdaterad version av komponenten. När Miljödata gjorde beställningen på leverantörens webbplats, fanns ingen information om att det inte skulle vara den vid tidpunkten senaste versionen av komponenten. Miljödata fick inte heller vid nedladdningen av komponenten information om att det vid tillfället inte var den senaste versionen. Miljödata utförde installationen av stödkomponenten men godkände aldrig uttryckligen den installerade versionen och hade aldrig anledning att misstänka att bolaget försågs med en utdaterad version. Den version som installerades visade sig ha en känd sårbarhet som gjorde det möjligt för angripare att utnyttja detta för intrångsförsök. Leverantören hade på sin webbplats i början av 2024 publicerat information om den sårbarhet som fanns i den version som Miljödata tillhandahölls.

Det som möjliggjorde att hotaktören kunde röra sig inom systemet var de tekniska privilegier som hotaktören kunde tillskansa sig genom sårbarheten i brandväggslösningen. Hotaktören kunde eskalera sina rättigheter och röra sig lateralt i Miljödatas tekniska miljöer och fick tillgång till Miljödatas servrar. Detta skedde trots att Miljödata hade tvåfaktorsautentisering aktiverat på interna tjänster i sin tekniska miljö samt separata behörighetskonton för olika roller i bolaget innan och vid tidpunkten för incidenten.

Processen för installation av nya komponenter
Processen för installation och godkännande av nya komponenter eller system i Miljödatas infrastruktur genomförs av en systemadministratör och innefattar analyser av bland annat behov och tekniska beroenden samt påverkan på drift och säkerhet. Analysunderlaget granskas sedan i samråd med andra systemtekniker och beslut fattas tillsammans med överordnad, varvid eventuella tester och riskreducerande åtgärder fastställs innan komponenten integreras. Vid installation av den aktuella stödkomponenten hade Miljödata ingen anledning att misstänka att den installerade versionen inte var den senaste eftersom det var en kostsam produkt som levererades av en välkänd leverantör. Därmed uppkom aldrig någon fråga om att kontrollera versionen och om den hade kända sårbarheter eller att uppdatera den efter installation.

Övervakningssystem
Miljödata hade vid tidpunkten för incidenten en driftövervakning genom serverleverantören kompletterat med bolagets egna funktions- och driftövervakning. Miljödatas system för övervakning larmade inte om misstänkta aktiviteter i samband med intrånget den 20 augusti 2025 och framåt. Motståndskraften i den EDR-lösning[3] som bolaget använde visade sig vara otillräcklig.

Miljödata upptäckte intrånget när tekniska larm utlöstes avseende fel i tjänst den 23 augusti 2025. Samtliga servrar isolerades av Miljödata och ett externt incidentresponsteam aktiverades av Miljödata samma kväll. Efter incidenten har EDR-lösning och SOC-övervakning införts dygnet runt.

[3] IMY:s förklaring: EDR-lösning (Endpoint detection and response) är ett säkerhetsprogram som övervakar nätverkets ändpunkter för att upptäcka misstänkt aktivitet.

Riskbedömningar och vidtagna säkerhetsåtgärder
Miljödata bedriver ett kontinuerligt och strukturerat säkerhetsarbete och hade vid tiden för incidenten relevanta organisatoriska och tekniska skyddsåtgärder på plats, såsom flerlagersskydd, åtkomst- och behörighetsstyrning, loggning, övervakning samt incidentberedskap. Riskbedömningar genomförs vid strategimöten och styrelsemöten men också löpande vid behov.

Riskerna i samband med behandling av personuppgifter i tjänsterna har på en övergripande nivå bedömts som låga. Bedömningen har skett inom ramen för Miljödatas systematiska informationssäkerhets- och riskhanteringsarbete och grundar sig i en kartläggning av behandlingsaktiviteter, klassificering av personuppgifter samt en sammanvägd hot- och sårbarhetsanalys. I hot- och sårbarhetsanalysen har risken för cyberangrepp särskilt beaktats och sannolikheten för cyberangrepp bedömdes som relativt låg, bland annat mot bakgrund av Miljödatas begränsade offentliga profil. Konsekvenserna för de registrerades fri- och rättigheter av ett eventuellt angrepp bedömdes som stora.

I hot- och sårbarhetsanalysen som Miljödata utförde avseende behandlingen i tjänsterna identifierades bland annat risker för obehörig åtkomst och kontoövertagande, felaktig behörighetstilldelning, skadlig kod samt drift- och leverantörsrelaterade risker. Efter införlivande av förebyggande tekniska och organisatoriska åtgärder bedömdes dock riskerna som låga. Risker har identifierats och hanterats löpande, bland annat i samband med design, utveckling och vidareutveckling av system. Systemen har utformats med utgångspunkt i genomgående höga säkerhetsnivåer och med tillämpning av principerna om inbyggt dataskydd och dataskydd som standard.

I tjänsterna skedde behandling av känsliga personuppgifter i form av bland annat sjukfrånvaro, rehabiliteringsdokumentation och personalanteckningar. Konsekvensen av obehörig åtkomst liksom behovet av skyddsåtgärder bedömdes vara större för denna typ av uppgifter. Åtgärder vidtogs i form av att bilagor och uppgifter i fritextfält krypterades av Miljödata i tjänsterna.

Personuppgifterna i tjänsterna och personuppgiftsansvar
Personuppgiftsincidenten omfattade cirka 2 200 000 fysiska personer. Incidenten omfattar personnummer, kontaktuppgifter, anställnings- och organisationsuppgifter samt frånvarodata. I begränsad omfattning förekommer barn bland de registrerade som drabbats av incidenten i de fall de innehaft en anställning hos någon av kunderna eller ingått i ärenden om elevhändelser som registreras i tjänsterna.

Bland de personuppgifter som behandlas i tjänsterna förekommer även känsliga personuppgifter, bland annat sjukfrånvarodata, dokumentation vid elevhändelser, rehabiliteringsdokumentation och personalanteckningar. I viss omfattning har skyddade personuppgifter behandlats i tjänsterna även om utgångspunkten har varit att sådana uppgifter inte var avsedda att behandlas i tjänsterna.

Miljödata är personuppgiftsbiträde för den behandling av personuppgifter som sker i tjänsterna för kundernas räkning. I de fall tjänsterna levereras till kunder via trepartsavtal med andra leverantörer är Miljödata underbiträde. Utöver detta är Miljödata i begränsad omfattning personuppgiftsansvarig för den behandling som avser Miljödatas egna personal samt viss kund-, system-, och leverantörsadministration som innefattar personuppgifter.

Åtgärder som vidtagits med anledning av incidenten
Miljödata isolerade samtliga servrar cirka en timme efter att incidenten upptäcktes den 23 augusti 2025. Ett externt incidentresponsteam och en intern arbetsgrupp aktiverades av Miljödata och incidenthanteringen innefattade omedelbar isolering, en forensisk utredning och sanering av kompromitterade system följt av återställning av krypterade servrar. Vidare innefattade hanteringen bland annat att påverkade domänkontrollanter[4] byggdes om för att återställa en betrodd identitetsinfrastruktur och åtgärder vidtogs i syfte att förhindra hotaktörens fortsatta eller ytterligare åtkomst. En total rensningsprocess genomfördes för att säkerställa att miljön var fri från kvarvarande skadlig kod. Säkerhetslösningar avvecklades och ersattes med nya och ytterligare säkerhetsåtgärder infördes i miljön i form av EDR- och SOC-övervakning[5] dygnet runt för att stärka förmågan kring detektion och respons.

Parallellt med den tekniska incidenthanteringen gjordes anmälningar till IMY och Polismyndigheten och kontakter togs med berörda myndigheter. Strukturerade kontaktvägar etablerades till samtliga kunder och Miljödata arbetade intensivt för att föra direkt dialog med varje berörd aktör. Samtliga personuppgiftsansvariga försågs löpande med underlag för incidentrapportering inklusive kompletteringar i takt med att nya forensiska fynd verifierades. För att säkerställa transparens och samordning genomfördes ett informationsmöte med Myndigheten för civilt försvar och dess funktioner, genomgångar med Sveriges Kommuner och Regioner som var öppna för offentliga organisationer och privata kunder samt ett separat informationsmöte öppet för alla Miljödatas kunder.

Motivering av beslutet

Tillämpliga bestämmelser m.m.

Personuppgiftsansvar
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.

Med personuppgiftsbiträde avses enligt artikel 4.8 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

En leverantör som tillhandahåller standardiserade tjänster kan agera som personuppgiftsbiträde medan dess användare agerar personuppgiftsansvariga i den mån de sistnämnda bestämt ändamålet för behandlingen och i vart fall utövar ett väsentligt inflytande över metoderna för behandlingen.[6] Det ska dock noteras att en sådan tjänsteleverantör kan fungera som personuppgiftsansvarig för viss behandlingsaktivitet och som personuppgiftsbiträde för annan aktivitet. För att avgöra

[4] IMY:s förklaring: En domänkontrollant är en server som i en domän i ett Windows-nätverk hanterar frågor om inloggning, autentisering och behörighet.
[5] IMY:s förklaring: SOC-övervakning (Security Operations Center) innebär kontinuerlig realtidsanalys av en organisations it-miljö för att identifiera, bedöma och avvärja säkerhetsincidenter.
[6] Se Europeiska dataskyddsstyrelens (EDPB) riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, p. 85.

hur personuppgiftsansvaret fördelar sig krävs att det för respektive aktivitet görs en analys av vilken grad av inflytande respektive aktör har haft för att det ska gå att avgöra vem som bestämt ändamål och medel för den aktuella behandlingen.[7]

Kravet på att vidta lämpliga säkerhetsåtgärder
Enligt artikel 32.1 i dataskyddsförordningen ska både personuppgiftsansvariga och personuppgiftsbiträden 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 senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter beaktas.

Enligt artikel 32.1 i förordningen omfattar lämpliga säkerhetsåtgärder, 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,
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.

EU-domstolen har uttalat att hänvisningen i artikel 32 till en ”säkerhetsnivå som är lämplig i förhållande till risken” respektive ”lämplig säkerhetsnivå” visar att det genom förordningen inrättats ett riskhanteringssystem och att ambitionen med förordningen inte på något sätt är att eliminera riskerna för personuppgiftsincidenter. Bestämmelsens ordalydelse innebär endast en skyldighet för den personuppgifts-ansvarige att vidta tekniska och organisatoriska åtgärder för att i möjligaste mån undvika personuppgiftsincidenter. Bedömningen av om sådana åtgärder är lämpliga ska ske utifrån de konkreta omständigheterna i det enskilda fallet.[8]

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 till dataskyddsförordningen 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

[7] Se EDPB:s riktlinjer 07/2020, p. 80.
[8] Se EU-domstolens dom den 14 december 2023, Natsionalna agentsia za prihodite, C-340/21, EU:C:2023:986, p. 29 och 30.

grundval av en objektiv bedömning, genom vilken det fastställs om behandlingen inbegriper en risk eller en hög risk.

Känsliga personuppgifter och personuppgifter som förtjänar särskilt skydd
Uppgifter om hälsa tillhör de särskilda kategorier av personuppgifter, så kallade känsliga personuppgifter, som ges ett särskilt starkt skydd enligt dataskyddsförordningen. Det är förbjudet att behandla sådana personuppgifter enligt artikel 9.1 i dataskyddsförordningen, om inte behandlingen omfattas av något av undantagen i artikel 9.2 i förordningen.

Uppgifter om hälsa definieras i artikel 4.15 i dataskyddsförordningen som personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa vilka ger information om dennes hälsostatus. I skäl 35 till dataskyddsförordningen anges att personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd.

I skäl 38 till dataskyddsförordningen anges att barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Av artikel 87 i dataskyddsförordningen och 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning följer att personnummer och samordningsnummer ges ett särskilt skydd.

IMY:s bedömning

Personuppgiftsansvar
Av utredningen i ärendet framgår att Miljödata i huvudsak agerar som personuppgiftsbiträde för personuppgifterna som behandlas i tjänsterna. I begränsad omfattning agerar Miljödata som personuppgiftsansvarig för personuppgifterna i tjänsterna. Eftersom skyldigheten att vidta lämpliga åtgärder enligt artikel 32 i dataskyddsförordningen gäller för både personuppgiftsansvariga och personuppgiftsbiträden kommer IMY inte att närmare bedöma vilken roll som bolaget har haft i förhållande till respektive behandlingsaktivitet.

Behandlingen har krävt en hög säkerhetsnivå
Miljödata har enligt artikel 32 i dataskyddsförordningen haft en skyldighet att vidta lämpliga säkerhetsåtgärder för att skydda personuppgifterna som behandlas i tjänsterna. Av utredningen framgår att det är Miljödata som utformar och tillhandahåller de aktuella tjänsterna och som därmed har haft den faktiska möjligheten att implementera sådana åtgärder. Vid bedömningen av vilka åtgärder som varit lämpliga och vilken säkerhetsnivå som behandlingen har krävt i det aktuella fallet beaktar IMY följande.

I tjänsterna har behandlingen av personuppgifter varit omfattande. Miljödata har uppgett att cirka 2 200 000 fysiska personer har varit registrerade i tjänsterna och omfattats av personuppgiftsincidenten. Bolaget har över 300 kunder i hela Sverige, varav en stor del av kunderna utgörs av kommuner, regioner och andra offentliga aktörer. Tjänsterna har innehållit cirka 20 personuppgifter om varje registrerad, såsom uppgifter om namn, kontaktuppgifter, personnummer samt anställnings- och organisationsuppgifter. IMY bedömer att det genom tillgång till informationen varit möjligt att direkt utläsa ett stort antal uppgifter om varje registrerad, vilket gjort behandlingen särskilt integritetskänslig.

IMY anser vidare att de personuppgifter som behandlats i tjänsterna har varit av sådan karaktär att behandlingen inneburit höga risker för de registrerades rättigheter och friheter. Tjänsterna som Miljödata erbjudit till kunderna har i huvudsak avsett hantering av bland annat sjukfrånvaro, rehabilitering, arbetsskador och tillbud. Detta har således inneburit en omfattande behandling av känsliga personuppgifter om hälsa, såsom uppgifter om sjukfrånvaro, uppgifter i rehabiliteringsdokument och i sjukintyg. Behandling av sådana uppgifter kan utgöra ett synnerligen allvarligt ingrepp i de grundläggande rättigheterna avseende respekt för privatlivet och skydd för personuppgifter.[9] I tjänsterna har det även behandlats personuppgifter om barn som är särskilt skyddsvärda enligt dataskyddsförordningen och andra särskilt skyddsvärda personuppgifter i form av personnummer och skyddade personuppgifter.

IMY konstaterar sammanfattningsvis att det har varit fråga om en omfattande behandling av personuppgifter sett till både antalet berörda registrerade och antalet uppgifter om varje registrerad. Detta i kombination med uppgifternas karaktär, som i stor utsträckning avsett känsliga personuppgifter liksom särskilt skyddsvärda uppgifter om bland annat barn, har medfört en hög risk för fysiska personers fri- och rättigheter. Obehörigt röjande eller obehörig åtkomst till personuppgifterna har kunnat leda till allvarliga konsekvenser för de berörda personerna. Det har ställt krav på en hög säkerhetsnivå för behandlingen i form av tillräckliga säkerhetsåtgärder för att säkerställa motståndskraft i tjänsterna och effektiviteten hos de tekniska och organisatoriska åtgärder som bolaget vidtagit för att upprätthålla behandlingens säkerhet.

Miljödata har inte vidtagit tillräckliga säkerhetsåtgärder
IMY ska därefter bedöma om Miljödata har vidtagit de tekniska och organisatoriska åtgärder som, med hänsyn till de höga risker som förelegat, varit lämpliga för att skydda personuppgifterna i tjänsten.

Bristande åtgärder för att förhindra intrånget

Av utredningen i ärendet framgår att Miljödata ungefär en vecka före incidenten installerade en stödkomponent till en brandväggslösning på en server hos Miljödata. Stödkomponenten levererades av en välkänd leverantör. Installationen av stödkomponenten utfördes av Miljödata. Den version som leverantören tillhandahöll Miljödata var dock utdaterad och innehöll en kritisk sårbarhet som var känd. Information om sårbarheten var tillgänglig på leverantörens hemsida mer än ett år innan installationen hos Miljödata genomfördes. Miljödata har uppgett att hotaktören utnyttjade sårbarheten i stödkomponenten genom en SQL-injektion och tog sig på så sätt in i Miljödatas tekniska miljö. IMY saknar anledning att ifrågasätta denna uppgift.

IMY konstaterar att ansvaret enligt artikel 32.1 i dataskyddsförordningen omfattar bland annat förmågan att fortlöpande säkerställa motståndskraften hos tjänsterna, samt regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet. I ärendet har det framkommit att Miljödata har en process vid installation och godkännande av nya komponenter innefattande bland annat en behovsanalys och en bedömning av påverkan på drift och säkerhet. Miljödata har dock uppgett att bolaget inte fann anledning att kontrollera att bolaget fått förväntad version av stödkomponenten från

[9] Se EU-domstolens dom den 1 augusti 2022, C-184/20, Vyriausioji tarnybinės etikos komisija, EU:C:2019:773, p. 126.

leverantören, bland annat eftersom det var en kostsam produkt från en välkänd leverantör.

IMY konstaterar att Miljödata har haft ansvaret för att säkerställa ett tillräckligt skydd för personuppgifterna i tjänsterna. Som framgår ovan har personuppgifts-behandlingens art och omfattning krävt en hög skyddsnivå. Vidare installerades den aktuella stödkomponenten på en server som var exponerad mot internet, vilket i sig innebär en förhöjd risk för intrång och därmed ställt krav på en hög säkerhetsnivå för behandlingen. När det som i detta fall var fråga om en ny mjukvara som inte genomgår tester i en testmiljö innan den integreras i ett it-system var det särskilt viktigt att rätt version av säkerhetskomponenten installerades. IMY konstaterar vidare att bristerna i den utdaterade versionen var kända.

Mot denna bakgrund bedömer IMY att det var en grundläggande säkerhetsåtgärd att kontrollera att rätt version av komponenten installerades. Miljödata borde således ha gjort en sådan kontroll innan komponenten integrerades i bolagets it-system. Genom att underlåta att göra en sådan kontroll installerade Miljödata en version av stöd-komponenten med en kritisk sårbarhet som sedan utnyttjades av hotaktören.

Genom att inte vidta sådana säkerhetsåtgärder bedömer IMY att Miljödata inte vidtagit tillräckliga tekniska och organisatoriska åtgärder i förhållande till risken för obehörigt röjande och obehörig åtkomst.

Bristande åtgärder för att upptäcka intrång eller intrångsförsök och begränsa omfattningen av intrånget

Av utredningen i ärendet framgår att intrånget påbörjats den 20 augusti 2025 och att tekniska larm om fel i tjänsten utlöstes den 23 augusti 2025. Hotaktören befann sig således i Miljödatas tekniska miljö under tre dygn och kunde röra sig lateralt mellan servrar i Miljödatas tekniska miljö samt påbörja kryptering av bolagets servrar innan Miljödatas övervakningssystem larmade. Enligt Miljödata var övervakningssystemet, som skulle upptäcka intrångsförsök, inte tillräckligt motståndskraftigt. Av utredningen framgår att Miljödata efter incidenten införde realtidsövervakning (SOC-övervakning) dygnet runt.

IMY konstaterar att de övervakningssystem som Miljödata använde främst var inriktade på att övervaka prestanda och tillgänglighet i systemen. De tekniska och organisatoriska säkerhetsåtgärder som Miljödata vidtagit för att övervaka säkerhetsrelaterade händelser har därmed inte varit tillräckliga för att upptäcka eller varna för de initiala intrångsförsöken, hotaktörens rörelse i systemen, krypteringen eller överföringen av personuppgifter. Hotaktören kunde således kringgå virusdetektion, säkerhetsbevakning och multifaktorsautentisering samt tilldela sig höga rättigheter på den server som stödkomponenten var installerad på. Hotaktören kunde vidare röra sig lateralt mellan servrar i Miljödatas tekniska miljö under flera dagar utan att bli upptäckt. IMY bedömer att hotaktören har kommit åt mer information vid intrånget genom att det övervakningssystem som Miljödata har använt inte larmat om intrånget i tid.

Mot bakgrund av de höga risker som personuppgiftsbehandlingen har inneburit bedömer IMY att det var en grundläggande säkerhetsåtgärd för Miljödata att ha automatisk realtidsövervakning för att identifiera hot i form av exempelvis misstänkt aktivitet och intrång eller intrångsförsök som kan leda till obehörig åtkomst. Om sådana åtgärder hade vidtagits hade Miljödata haft bättre förutsättningar att i ett

tidigare skede upptäcka intrånget och följaktligen begränsa dess omfattning. Genom att underlåta att vidta sådana åtgärder bedömer IMY att Miljödata inte har vidtagit tillräckliga åtgärder för att säkerställa en lämplig säkerhetsnivå.

Sammanfattande bedömning

Sammantaget konstaterar IMY att personuppgiftsbehandlingen har krävt en hög skyddsnivå. IMY bedömer att Miljödata genom att inte kontrollera att den aktuella stödkomponenten var rätt version innan installation inte har vidtagit tillräckliga åtgärder för att säkerställa att personuppgifterna som behandlats i bolagets tjänster skyddats mot risken för obehörigt röjande eller obehörig åtkomst till följd av dataintrång. Vidare har bolaget inte vidtagit tillräckliga säkerhetsåtgärder genom att inte ha automatisk realtidsövervakning för att identifiera hot i form av exempelvis misstänkt aktivitet och intrång eller intrångsförsök som kan leda till obehörig åtkomst. Om sådana åtgärder hade vidtagits skulle bolaget ha haft bättre förutsättningar att i ett tidigare skede upptäcka intrånget och följaktligen begränsa dess omfattning.

Mot denna bakgrund bedömer IMY att Miljödata har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen genom att inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter i tjänsterna innan och vid tidpunkten för den personuppgiftsincident som konstaterades den 23 augusti 2025.

Val av ingripande

Vad Miljödata har uppgett

Miljödata har i huvudsak uppgett följande gällande valet av korrigerande åtgärd.

Om IMY anser att bolaget har handlat i strid med artikel 32 i dataskyddsförordningen, föreligger flera omständigheter som innebär att bolaget inte ska påföras en påföljd. Skulle IMY komma fram till att en påföljd är aktuell är dessa omständigheter av sådant slag att den enda effektiva, proportionella och avskräckande påföljden är en reprimand.

Det brottsliga intrång som bolaget har drabbats av kan inte anses vara av hög allvarlighetsgrad. Incidenten har inte sin grund i något uppsåtligt eller oaktsamt agerande från bolagets sida. Tvärtom har bolaget vidtagit mer omfattande säkerhetsåtgärder än vad som krävs enligt dataskyddsförordningen.

Även om ett stort antal registrerade har berörts av incidenten har dessa inte lidit någon konkret skada av betydelse. Personuppgifter av mer integritetskänslig karaktär har förekommit endast i begränsad omfattning. Att varken någon personuppgiftsansvarig eller registrerad framställt något konkret och specificerat anspråk mot bolaget med anledning av incidenten bekräftar att någon faktisk skada i praktiken inte uppstått. Bolaget har begränsat incidentens varaktighet genom vidtagna åtgärder i form av teknisk övervakning som utlöste larm och omedelbar isolering av samtliga servrar. Att bolaget hade krypterat bland annat bilagor och fritextfält begränsade omfattningen av incidenten och därmed den skada som de registrerade kan ha lidit. De skyndsamma och samordnade åtgärder som bolaget vidtagit har medfört att incidentens varaktighet och omfattning begränsats.

Bolaget har genomgående samarbetat med IMY under hela handläggningen av ärendet och själva anmält incidenten till IMY inom den lagstadgade tiden. Bolaget har därutöver löpande informerat berörda personuppgiftsansvariga och relevanta myndigheter vilket gjort det möjligt för de personuppgiftsansvariga att vidta ytterligare skyddsåtgärder och att anmäla incidenten till IMY. Bolaget har utöver detta haft individuella möten med flera hundra kunder och utgjort en samordnande funktion gentemot Sveriges Kommuner och Regioner, som flertalet kunder är anknutna till.

Efter incidenten har bolaget återigen sett över sina säkerhetsåtgärder vilket lett till förändringar av och ytterligare investeringar i tekniska och organisatoriska säkerhetsåtgärder för att förhindra framtida intrång. Incidenten har orsakat bolaget betydande kostnader och omfattande arbete. Bolaget har vidare inte varit föremål för utredning enligt dataskyddsförordningen tidigare.

Tillämpliga bestämmelser m.m.

Val av korrigerande åtgärder och beräkning av sanktionsavgiftens storlek
Vid överträdelse av dataskyddsförordningen har IMY ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen, bland annat reprimand, föreläggande och sanktionsavgift. 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. Enligt artikel 83.1 ska varje tillsynsmyndighet säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande.

I artikel 83.2 i dataskyddsförordningen anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras och vad som ska påverka sanktionsavgiftens storlek. Av betydelse för bedömningen av överträdelsens allvar är bland annat dess karaktär, svårighetsgrad och varaktighet. Europeiska dataskyddsstyrelsen (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.[10]

Enligt artikel 83.4 i dataskyddsförordningen ska det vid överträdelser av bland annat artikel 32 påföras administrativa sanktionsavgifter på upp till 10 000 000 euro eller, om det gäller ett företag, på upp till två procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Om det är fråga om en mindre överträdelse får IMY enligt skäl 148 till dataskydds-förordningen i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i förordningen.

Definitionen av begreppet företag
Vid bestämmande av maxbeloppet för en sanktionsavgift som ska påföras ett företag ska den definition av begreppet företag användas som EU-domstolen använder vid tillämpning av artiklarna 101 och 102 i Fördraget om Europeiska unionens funktionssätt (EUF-fördraget).[11] Beräkningen av maxbeloppet för en personuppgiftsansvarig som utgör ett sådant företag eller ingår i ett sådant företag ska ske på grundval av en procentandel av det berörda företagets totala globala

[10] Se EDPB:s riktlinjer 04/2022 om beräkning av administrativa sanktionsavgifter enligt den allmänna dataskyddsförordningen antagna den 24 maj 2023.
[11] Se skäl 150 till dataskyddsförordningen.

årsomsättningen under föregående räkenskapsår.[12] Begreppet företag ska även beaktas för att bedöma den faktiska eller materiella ekonomiska kapaciteten hos den personuppgiftsansvarige som påförs sanktionsavgiften och därigenom kontrollera om sanktionsavgiften är effektiv, proportionerlig och avskräckande.[13]

Ett moderbolag och ett dotterbolag betraktas som en del av samma ekonomiska enhet när moderbolaget utövar ett avgörande inflytande över dotterbolaget. Av EU-domstolens praxis följer att om ett moderbolag äger 100 procent eller nästan 100 procent av aktierna i ett dotterbolag föreligger en presumtion för att moderbolaget utövar ett avgörande inflytande över dotterbolagets beteende (den så kallade Akzo-principen). Presumtionen kan dock motbevisas om företaget lämnar tillräcklig bevisning för att styrka att dotterbolaget agerar självständigt på marknaden.[14]

IMY:s bedömning

Sanktionsavgift ska påföras
IMY har bedömt att Miljödata har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen genom att inte vidta tillräckliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna som behandlas i bolagets tjänster. Detta har lett till obehörig åtkomst till en stor mängd personuppgifter som omfattat känsliga liksom särskilt skyddsvärda personuppgifter. IMY bedömer att det inte är fråga om en sådan mindre allvarlig överträdelse som kan medföra att en reprimand utfärdas i stället för en sanktionsavgift.

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 härvid 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.[15]

Miljödata har i egenskap av personuppgiftsbiträde och i begränsad omfattning som personuppgiftsansvarig, haft ett ansvar för att uppfylla dataskyddsförordningens krav på att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig skyddsnivå för personuppgifterna som behandlats i tjänsterna. Genom att inte vidta sådana åtgärder har Miljödata behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen. IMY bedömer att Miljödata inte kan ha varit okunnigt om att agerandet inneburit en överträdelse av förordningen. IMY anser att Miljödata har varit oaktsamt i förhållande till den överträdelse av dataskyddsförordningen som konstaterats. Samtliga förutsättningar för att påföra Miljödata en sanktionsavgift är därmed uppfyllda.

Vilken årsomsättning som ska läggas till grund för beräkningen av sanktionsavgiften
Av Miljödatas årsredovisning för år 2025 framgår att bolaget är ett helägt dotterbolag till Persona Grata Informationssystem Aktiebolag. Tillsammans bildar bolagen en koncern. Eftersom Persona Grata Informationssystem Aktiebolag äger 100 procent av aktierna i Miljödata föreligger enligt den s.k. Akzo-principen en presumtion, som inte

[12] Se EU-domstolens dom den 5 december 2023, Deutsche Wohnen, C-807/21, EU:C:2023:950, p. 57.
[13] Se EU-domstolens dom den 13 februari 2025, ILVA, C-383/23, EU:C:2025:84, p. 36.
[14] Se EU-domstolens dom den 10 september 2009, Akzo Nobel m.fl. mot kommissionen, C-97/08 P, EU:C:2009:536, p. 59–61 och dom den 14 juli 1972, ICI mot Commission, C-48/69, EU:C:1972:70, p. 136.
[15] Se EU-domstolens dom den 4 maj 2023, Nacionalinis visuomenes sveikatos centras, C-683/21, EU:C:2023:949, p. 81 och den 5 december 2023, Deutsche Wohnen, C-807/21, EU:C:2023:950, p. 76.

har motbevisats i ärendet, för att Persona Grata Informationssystem Aktiebolag utövar ett avgörande inflytande över Miljödatas beteende. IMY bedömer att bolagen således ska betraktas som en sådan ekonomisk enhet som utgör ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget.

Eftersom det inte har upprättats någon koncernredovisning för koncernen ska beräkningen av sanktionsavgiften göras utifrån Persona Grata Informationssystem Aktiebolags och Miljödatas samlade årsomsättning för budgetåret 2025. För det budgetåret redovisade Persona Grata Informationssystem Aktiebolag 0 kr i årsomsättning medan Miljödatas årsomsättning uppgick till 58 476 045 kronor. Två procent av den totala årsomsättningen för företaget för budgetår 2025 är således 1 169 521 kronor. Eftersom detta belopp är lägre än det statiska maxbeloppet som anges i artikel 83.4 i dataskyddsförordningen är den högsta sanktionsavgiften som kan fastställas i ärendet 10 miljoner euro.

Överträdelsen är av hög allvarlighetsgrad
Vid bedömningen av överträdelsens allvar ska hänsyn tas till bland annat dess karaktär, svårighetsgrad och varaktighet. Av EDPB:s riktlinjer framgår att allvarlighetsgraden delas in i låg, medel eller hög allvarlighetsgrad.[16] Vid bedömningen av överträdelsens allvarlighetsgrad tar IMY hänsyn till följande omständigheter.

Bolagets tjänster har använts av ett stort antal kommuner, regioner och företag i hela Sverige. Personuppgiftsbehandlingen har varit omfattande och de konstaterade bristerna har möjliggjort obehörig åtkomst till över två miljoner personers uppgifter. Personuppgiftsbehandlingen har innefattat en stor mängd uppgifter om varje person, vilket medfört att integritetsriskerna ökat.[17] En stor del av bolagets tjänster har avsett hantering av personaladministrativa ärenden kopplade till bland annat sjukfrånvaro, rehabilitering och arbetsskador. Detta har inneburit en behandling av känsliga personuppgifter om hälsa och av andra integritetskänsliga uppgifter som förtjänar ett särskilt skydd. Tjänsterna har även innefattat personuppgifter om barn, som på grund av sin sårbarhet ska ges ett särskilt starkt skydd för sina personuppgifter. Att Miljödata hade krypterat personuppgifter i fritextfält och bilagor får dock i viss mån anses ha minskat risken för skada hos de berörda registrerade jämfört med om så inte hade varit fallet. IMY bedömer dock att krypteringen inte kan tas till intäkt för att uppgifterna har skyddats från obehörig åtkomst i samband med intrånget.

Överträdelsen har dessutom gällt den centrala behandlingen av personuppgifter för Miljödatas kärnverksamhet, där bolaget får förutsättas ha goda förutsättningar att vidta lämpliga säkerhetsåtgärder. Det gör att överträdelsen ska anses som allvarligare, än om så inte varit fallet.[18]

IMY konstaterar att redan en obehörig åtkomst till den typ av personuppgifter som behandlas i tjänsterna medför skada för de registrerade. EU-domstolen har uttalat att skada kan uppkomma för registrerade redan vid förlust av kontroll över egna personuppgifter, även om det inte förekommit något konkret missbruk av uppgifterna i fråga.[19] I detta fall har bristerna i skyddet för personuppgifterna lett till att hotaktören kunnat bereda sig tillgång till och därefter publicera personuppgifter från Miljödatas tjänster på Darknet. IMY anser således att Miljödatas bristfälliga agerande har haft stor

[16] Se EDPB:s riktlinjer 04/2022, p. 60.
[17] Se EDPB:s riktlinjer 04/2022, p. 58.
[18] Se EDPB:s riktlinjer 04/2022, p. 53.
[19] Se EU-domstolens dom den 14 december 2023, Natsionalna agentsia za prihodite, C-340/21, EU:C:2023:986, p.82 och dom den 4 oktober 2024, Agentsia po vpisvaniyata, C-200/23, EU:C:2024:827, p. 145.

påverkan på de registrerades fri- och rättigheter och att den skada som berörda registrerade har lidit innebär att överträdelsen ska betraktas som mer allvarlig.

Beroende på omständigheterna i det enskilda fallet påverkas bedömningen av överträdelsens allvar även av graden av oaktsamhet i förhållande till konstaterade brister.[20] I detta fall har IMY konstaterat att bristerna bestått i att bolaget inte kontrollerat att de fått rätt version av den aktuella stödkomponenten innan installation och att detta varit en grundläggande säkerhetsåtgärd sett till behandlingens art och omfattning. Information om att den aktuella stödkomponenten innehållit sårbarheter har dessutom varit känd och tillgänglig på leverantörens hemsida i mer än ett år före installation. Sett till behandlingens karaktär och omfattning, har det även varit grundläggande att ha en robust övervakning. I detta avseende visar utredningen att Miljödata haft förmåga att vidta säkerhetsåtgärder genom att bolaget en kort tid efter personuppgiftsincidenten infört automatisk realtidsövervakning. IMY bedömer mot den bakgrunden att Miljödata har uppvisat oaktsamhet av sådan grad att överträdelsen ska anses som allvarligare.

Med beaktande av det nu anförda bedömer IMY att den aktuella överträdelsen är av hög allvarlighetsgrad.

Förmildrande och försvårande faktorer
Vid bedömningen av sanktionsavgiftens storlek ska hänsyn även tas till de försvårande och förmildrande faktorer som anges i artikel 83.2 i dataskyddsförordningen.

Av utredningen framgår att Miljödata såväl före som efter incidenten har vidtagit förändringar och gjort investeringar i tekniska och organisatoriska säkerhetsåtgärder.

Beträffande åtgärder som vidtagits före incidenten har Miljödata bland annat anfört att det ska beaktas att bolaget hade krypterat uppgifter i bilagor och fritextfält vilket enligt bolaget utgjorde ett adekvat skydd som direkt begränsade incidentens omfattning och den skada registrerade kan ha lidit. IMY anser att de vidtagna åtgärderna, så som kryptering av bilagor och fritextfält, inte kan anses gå utöver vad som kan förväntas av Miljödata med tanke på behandlingens karaktär och omfattning.

IMY bedömer vidare att det inte har framkommit att åtgärderna som vidtagits efter intrånget har mildrat skadan för de registrerade i sådan utsträckning att dessa ska betraktas som förmildrande faktorer.[21]

Den omständigheten att Miljödata har anmält en egen personuppgiftsincident och samarbetat med IMY vid utredningen av händelsen i den utsträckning som det kan förväntas påverkar inte sanktionsavgiftens storlek i höjande eller sänkande riktning.[22] IMY bedömer inte heller att Miljödatas åtgärder för att möjliggöra för kunderna att uppfylla sina skyldigheter att lämna in incidentanmälningar till IMY i rätt tid varit av sådant slag att dessa ska betraktas som förmildrande.

IMY beaktar däremot, i viss förmildrande riktning, de informationsinsatser som Miljödata vidtog i nära anslutning till incidenten och innan tillsyn inletts. Dessa insatser har bland annat bestått av individuella möten med flera hundra berörda personuppgiftsansvariga vilket möjliggjort för dem att vidta ytterligare säkerhetsåtgärder. Därutöver har bolaget haft en samordnande funktion gentemot

[20] Se EDPB:s riktlinjer 04/2022, p. 56.
[21] Se EDPB:s riktlinjer 04/2022, p. 74.
[22] Se EDPB:s riktlinjer 04/2022, p. 95–98.

Sveriges Kommuner och Regioner, som flertalet kunder är anknutna till, och hållit flera informationsmöten med berörda kunder.

IMY bedömer att det därutöver saknas försvårande eller förmildrande faktorer som påverkar sanktionsavgiften.

Sanktionsavgiftens storlek
IMY bestämmer utifrån en samlad bedömning att Miljödata ska betala en administrativ sanktionsavgift på 1 800 000 kronor. Vid bestämmandet av sanktionsavgiftens storlek har överträdelsens höga allvarlighetsgrad och företagets storlek beaktats.[23] IMY har som en förmildrande omständighet beaktat Miljödatas agerande i samband med incidenten. IMY bedömer att beloppet är effektivt, proportionerligt och avskräckande.

Detta beslut har fattats av generaldirektören Eric Leijonram efter föredragning av avdelningsjuristen Måns Lysén. Vid den slutliga handläggningen har även rättschefen David Törngren, rådgivaren Sara Ahmed, enhetscheferna Jenny Bård och Christelle Bourquin, juristen Erika Palmheden samt it- och informationssäkerhetsspecialisten Andreas Majunie medverkat.

Eric Leijonram

Bilaga

Information om betalning av sanktionsavgift.

[23] Av EDPB:s riktlinjer 04/2022, p. 63–69, framgår hur ett företags årsomsättning kan påverka en beräkning av sanktionsavgiftens storlek som utgår från det statiska beloppet om 10 000 000 euro.

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.