Integritetsskyddsmyndigheten

Sportadmin i Skandinavien AB

Diarienummer:
IMY-2025-7801

Datum:
2026-01-26

Beslut efter tillsyn enligt dataskyddsförordningen – Sportadmin i Skandinavien AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Sportadmin i Skandinavien AB, 556773-0832, har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1] genom att inte vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifterna i sina tjänster innan och vid tidpunkten för den personuppgiftsincident som konstaterades den 16 januari 2025.

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Sportadmin i Skandinavien AB ska betala en administrativ sanktionsavgift på 6 000 000 kronor för överträdelsen av artikel 32.1 i dataskyddsförordningen.

Redogörelse för tillsynsärendet

Bakgrund

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn mot Sportadmin i Skandinavien AB (Sportadmin) med anledning av en personuppgiftsincident som inträffade den 16 januari 2025 och anmäldes av Sportadmin till IMY den 17 januari 2025.

Sportadmin tillhandahåller digitala kommunikationstjänster (tjänsterna) i form av bland annat ett webbaserat administrationsverktyg för medlemshantering, fakturering och hemsidor för idrottsföreningar och andra organisationer (föreningarna) samt en mobilapplikation som används av föreningarnas ledare, medlemmar och medlemmars målsmän.

Av Sportadmins anmälan om personuppgiftsincident framgår bland annat att tjänsterna, i vilka personuppgifter som Sportadmin är såväl personuppgiftsansvarig som personuppgiftsbiträde för behandlas, har utsatts för ett dataintrång av en extern angripare (hotaktören). Vidare anges att det vid tidpunkten för anmälan fanns tecken

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).

på att data hade förts över till hotaktören och att det inte gick att utesluta att hotaktören därigenom fått tillgång till personuppgifter.

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

Vad Sportadmin har uppgett

Sportadmin anser att bolaget inte har brutit mot dataskyddsförordningen och att vidtagna säkerhetsåtgärder varit tillräckliga i förhållande till personuppgifterna som behandlats i tjänsterna och har därutöver i huvudsak framfört följande.

Sammanfattning av intrånget
Den 16 januari 2025 upptäckte Sportadmin att det skett ett intrång i tjänsterna och påbörjade en utredning med stöd av en extern säkerhetspartner. Av de systemloggar som granskades under utredningen framgår bland annat följande.

Intrånget den 16 januari skedde genom att en hotaktör utförde en så kallad SQL-injektion[2] via en specifik variabel[3], som införts på en av Sportadmins webbsidor, som saknade skydd mot den typen av attacker. Utredningen indikerar att det även förekommit upprepade försök till SQL-injektioner sedan morgonen den 14 januari 2025. På grund av för höga tillåtna rättigheter i de delar av tjänsten där intrånget skedde kunde hotaktören bereda sig tillgång till Sportadmins server. Loggarna visade på avvikande utgående trafik från produktionsmiljön under tidig morgon den 16 januari 2025, vilket Sportadmin vid tidpunkten för intrånget bedömde som ett troligt tecken på dataöverföring ur miljön. Inledningsvis kunde bolaget inte bekräfta att sådan överföring skett. Den 14 mars 2025 publicerades dock all uthämtad och stulen data, som innehöll personuppgifter, på Darknet.

Den sannolika orsaken till intrånget och dess omfattning
Av Sportadmins utredning framgår att intrånget sannolikt möjliggjordes genom att en hotaktör kunde ta sig in i systemen genom en SQL-injektion.

I samband med en förändring av inloggningsförfarandet för föreningshemsidor den 28 juni 2022 genomfördes en förändring av kod varvid en särskild variabel infördes på en av Sportadmins webbsidor. När variabeln lades till förbisåg Sportadmin att tillämpa sin befintliga säkerhetsmetod för skydd mot SQL-injektioner. Eftersom förändringen inte introducerade en ny variabel i systemen, utan avsåg återanvändning av en variabel som Sportadmin ansåg som säker och som i regel inte brukar kräva applicering av ytterligare säkerhetsmetoder, upptäcktes inte bristen. Den oskyddade variabeln användes därefter direkt vid kommunikation med databasen vilket medförde en förhöjd risk för dataintrång med hjälp av SQL-injektioner. Det var vid denna variabel som den aktuella SQL-injektionen utfördes och som sannolikt orsakade incidenten.

---

[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.
[3] IMY:s förklaring: Variabler används i program för att kortsiktigt lagra den data som behandlas. Dessa kan exempelvis innehålla uppgifter om användaren som namn och e-postadress, men även andra uppgifter som påverkar funktionaliteten i tjänsten.

Två faktorer som bidrog till incidentens omfattning rörde behörigheter och rättigheter för SQL-användaren[4] och Windows-användaren[5]. SQL-användaren hade högre rättigheter än nödvändigt på grund av vissa kompatibilitetskrav med Sportadmins äldre system. Vidare hade den Windows-användare som körde SQL-servertjänsten[6] vid tillfället högre rättigheter än vad som tidigare var känt. SQL-servern tillät även körning av externa programfiler, exempelvis Powershell-script.

Rutiner för kodgranskning och övervakningssystem
Den förändring av kod som genomfördes i juni 2022 klassificerades som en högriskändring och granskningar genomfördes därför av ytterligare personer. Avsaknaden av skydd mot SQL-injektioner fångades trots det inte upp på grund av att bolaget hade brister i sina granskningsrutiner för mer komplexa kodändringar. Bolaget har identifierat följande brister.

- Riskklassificeringen var för ensidig eftersom den huvudsakligen utgick från påverkan på inloggningsförfarandet och risk för otillbörlig åtkomst till användardata. Det innebar att andra typer av angrepp, såsom SQL-injektioner, inte beaktades i tillräcklig omfattning.
- Kombinationen av en tekniskt komplex miljö där äldre (legacy) kod blandades med nyare implementeringar, bidrog till att den aktuella sårbarheten inte identifierades under granskningen.
- Det saknades ytterligare granskningsrutiner vid förändring av kod som innebar en hög risk i kombination med särskilt beroende till äldre kod. De hade till exempel kunnat omfatta obligatorisk granskning av fler personer. Vidare hade automatiska säkerhetsgranskningar av koden kunnat identifiera sårbarheter.
- Kodgranskningen var subjektiv och otydlig. Eftersom kodgranskning vid tidpunkten inte var ett obligatoriskt steg vid förändring av kod och riskbedömningskriterierna var subjektiva, baserades beslutet om att genomföra granskning på en individuell bedömning i det enskilda fallet.

Sportadmins system för övervakning larmade inte om misstänkta aktiviteter i samband med intrånget den 14 januari 2025 och framåt. Det program som användes bevakar och analyserar ständigt hårdvara, programvara (mjukvara) och användande för att identifiera eventuell onormal aktivitet i form av prestanda eller belastning, men utgör inte ett verktyg för att i realtid bevaka och upptäcka intrångsförsök. Loggar från systemet granskades manuellt av bolaget på daglig basis. Genom analyser av loggar eller vid oväntade förändringar i systemets prestanda kunde misstänkt aktivitet identifieras.

Övervakningssystemet varnade dock för onormal aktivitet när en av Sportadmins servrar slutade svara den 16 januari 2025. Det ledde till en manuell granskning och detektion av det pågående intrånget. I den efterföljande utredningen möjliggjorde systemet vidare tillgång till loggar. Loggarna användes bland annat för att förstå vilka sannolika tillvägagångssätt hotaktören använde för att få tillgång till systemet och för att i efterhand konstatera att intrångsförsöken pågått sedan den 14 januari 2025.

---

[4] IMY:s förklaring: En SQL-användare är ett konto som kan användas för att ansluta till en SQL-server, som är en server som har den mjukvara som krävs för att hantera databasen.
[5] IMY:s förklaring: En Windows-användare är ett konto som kan användas i operativsystemet Microsoft Windows (exempelvis Windows Server 2025 eller Windows 11) för att logga in i datorn och/eller köra specifika program.
[6] IMY:s förklaring: Tjänster (mindre program) kan köras i bakgrunden på en server för att utföra specifika uppgifter. SQL-tjänst är ett exempel på en databasrelaterad tjänst som kommunicerar med databasen.

Riskbedömningar och vidtagna säkerhetsåtgärder
Sportadmin har ett strukturerat säkerhets- och dataskyddsarbete där riskbedömningar diskuteras och uppdateras löpande. Utöver det genomfördes större årliga genomlysningar under 2021 och 2022 samt vid årsskiftet 2023/2024. Vid genomlysningarna identifierade Sportadmin konsekvent förhöjda risker för dataintrång i form av bland annat SQL-injektioner på grund av att delar av systemet varit skriven i äldre kod. Sportadmin utförde därför ett kontinuerligt arbete för att minska riskerna genom att bland annat addera och uppdatera skyddet för SQL-injektioner samtidigt som bolaget successivt övergick till modern teknik.

De publikt exponerade delarna av Sportadmins system, såsom föreningshemsidor, bedömdes som områden med en förhöjd risknivå för potentiellt dataläckage eller förstörelse av data som konsekvens. Det genomfördes därför riktade insatser för att identifiera och åtgärda sårbarheter relaterade till SQL-injektioner i de delar av systemen som ännu inte migrerats till modern teknik. I början av 2023 infördes en förstärkt säkerhetsmetod mot SQL-injektioner. När den nya säkerhetsmetoden implementerades saknades dock kännedom om att en variabel stod utan skydd. Säkerhetsmetoden applicerades därför inte på denna variabel.

I maj och juni 2024 undersöktes möjligheten att införa ytterligare skydd för tjänsterna genom att implementera en så kallad Web Application Firewall (WAF)[7]. Vid testerna uppstod problem som gjorde att lösningen inte ansågs genomförbar vid tillfället på grund av att den krävde en hög grad av manuell hantering och skulle aktualisera höga genomförandekostnader. Testningen pausades därför temporärt med avsikten att framöver identifiera en mer hållbar lösning givet den dåvarande tekniska miljön. Vid tidpunkten för incidenten hade även ett arbete för att övergå till en SQL-användare med begränsade behörigheter påbörjats, men inte slutförts.

Personuppgifterna i tjänsterna
Personuppgiftsincidenten omfattade 2 126 075 fysiska personer, som var identifierbara via personnummer. Eftersom föreningarnas verksamheter primärt är inriktade på aktiviteter för barn och ungdomar är denna grupp mest förekommande i föreningarnas register. Tjänsterna innehåller flera kategorier av personuppgifter i form av bland annat fullständiga namn och kontaktuppgifter, kön, personnummer, relation mellan målsman och medlem, nationalitet samt den idrott och förening som en registrerad varit kopplad till. Bland de personuppgifter som behandlas i tjänsterna förekommer även känsliga personuppgifter om funktionsnedsättningar och allergier. Det har även framkommit att det i viss omfattning förekommit skyddade personuppgifter i tjänsterna, även om utgångspunkten var att sådana uppgifter inte skulle behandlas i tjänsterna.

Åtgärder som vidtagits med anledning av incidenten
Det skedde en fullständig nedstängning av samtliga tjänster cirka en timme efter att incidenten upptäcktes. Sportadmin hanterade händelsen som en allvarlig säkerhetsincident utifrån tre parallella fokusområden i form av minimering av skador för kunder och användare, återställning till normal drift och kommunikation gentemot föreningarna och användarna. Sportadmin genomförde även omfattande åtgärder i syfte att minimera risken för att en liknande incident ska inträffa. Bolaget vidtog bland annat flera tekniska åtgärder på kort tid i form av bland annat omfattande genomgångar av befintlig funktionalitet och aktivering av en ny produktionsmiljö i syfte att förhindra hotaktörens fortsatta, eller ytterligare, åtkomst till personuppgifterna. I den

[7] IMY:s förklaring: WAF är en typ av brandvägg som används för att skydda webbapplikationer mot attacker och intrång genom att stoppa skadliga förfrågningar innan dessa når servern.

nya produktionsmiljön som togs i drift den 18 januari 2024 infördes flera förstärkta skydd mot SQL-injektioner, exempelvis aktiverades WAF.

Sportadmin informerade och uppmanade samtliga föreningar att anmäla händelsen till IMY som egna personuppgiftsincidenter, med hänvisning till informationen i Sportadmins incidentanmälan. Sportadmin arbetade, i samråd med IMY, för att göra det så enkelt som möjligt för alla parter att lämna in korrekta och fullständiga anmälningar till IMY. Bolaget hade över 2000 uppsökande samtal med föreningarna, som utfördes av ett stort antal anställda under en mycket kort tid, för att informera om diskussionerna med IMY och för att stötta i arbetet med att anslutas till Sportadmins anmälan. Det resulterade i att de allra flesta föreningar, närmare 1700, inkom med anmälningar inom 72 timmar från incidenten. Sportadmin informerade föreningarna löpande om ärendets status och stöttade i deras kontakt med användarna.

Sportadmin inhämtade vidare samtycke från föreningarna att agera i deras ställe för att skicka ut information till samtliga registrerade kring incidenten. På grund av informationen kunde de registrerade tillvarata sina rättigheter enligt dataskyddsförordningen bättre, än om föreningarna tillhandahållit informationen, eftersom det gjorde det enkelt att överblicka vilka personuppgifter som behandlats och av vilka föreningar. Bolaget har uppgett att agerandet ledde till att de registrerade fick tillgång till information inom kort tid och innan hotaktören släppte uppgifterna. Det medförde bland annat att de registrerade omgående kunde vidta försiktighetsåtgärder avseende sina personuppgifter.

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.[8] Det ska dock noteras att en sådan tjänsteleverantör kan fungera som personuppgiftsansvarig för viss behandlingsaktivitet och personuppgiftsbiträde för annan aktivitet. För att avgöra hur personuppgiftsansvaret fördelar sig krävs att det för respektive aktivitet görs en analys

[8] Se Europeiska dataskyddsstyrelens (EDPB:s) riktlinjer Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 85.

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.[9]

Kravet på att vidta lämpliga skyddsåtgärder
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-ansvariga 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.[10]

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

---

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

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 som huvudregel 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. Sådant särskilt skydd bör i synnerhet gälla vid insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas.

IMY:s bedömning

Personuppgiftsansvar
Av utredningen i ärendet framgår att Sportadmin i huvudsak agerar som personuppgiftsbiträde för personuppgifterna som behandlas i tjänsterna, och i begränsad omfattning som personansvarig. 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
Sportadmin har enligt artikel 32 i dataskddsförordningen haft en skyldighet att vidta lämpliga säkerhetsåtgärder för att skydda personuppgifterna som behandlas i tjänsterna. Av utredningen framgår att det är bolaget 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 i det aktuella fallet beaktar IMY följande.

Behandlingen av personuppgifter i tjänsterna har varit omfattande. Enligt Sportadmin har 2 126 075 fysiska personer, som varit identifierbara via personnummer, omfattats av personuppgiftsincidenten. Tjänsterna, som använts av ett stort antal idrottsföreningar i hela Sverige, har vidare innehållit ett stort antal personuppgifter om varje registrerad såsom fullständiga namn och kontaktuppgifter, kön, personnummer, relation mellan medlem och målsman, nationalitet samt den idrott och klubb som en registrerad varit kopplad till. 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.

Vidare anser IMY att karaktären på de personuppgifter som behandlats i tjänsterna har varit sådan att behandlingen inneburit höga risker för de registrerades rättigheter och friheter. De aktuella personuppgifterna har huvudsakligen gällt barn som är särskilt skyddsvärda enligt dataskyddsförordningen. Vidare har tjänsterna innehållit känsliga

personuppgifter om hälsa i form av allergier och funktionsnedsättningar. Behandling av sådana uppgifter kan utgöra ett synnerligen allvarligt ingrepp i de grundläggande rättigheterna avseende respekt för privatlivet och skydd för personuppgifter.[11] Utredningen visar även att tjänsterna har innehållit skyddsvärda uppgifter i form av personnummer[12] samt skyddade personuppgifter.

Sammantaget har omfattningen av behandlingen sett till både antalet berörda registrerade, som huvudsakligen varit barn, och den omfattande mängden uppgifter om varje registrerad samt uppgifternas karaktär medfört en hög risk för fysiska personers rättigheter och friheter. Obehörigt röjande av 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 i de tekniska och organisatoriska åtgärder som vidtagits för att upprätthålla behandlingens säkerhet.

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

Bristande åtgärder i syfte att förhindra och begränsa omfattningen av intrånget

Av utredningen i ärendet framgår att Sportadmin i samband med en förändring av inloggningsförfarandet för föreningshemsidor den 28 juni 2022 på en viss webbsida infört en variabel som saknat det skydd som bolaget vid tidpunkten tillämpade mot SQL-attacker. IMY konstaterar att Sportadmins tjänster därigenom lämnats exponerade för förhöjda risker för intrång i form av SQL-injektioner. Även om Sportadmin i början av 2023 infört en förstärkt säkerhetsmetod mot SQL-injektioner förblev tjänsterna sårbara på grund av att Sportadmin inte uppmärksammat den aktuella bristen i form av den oskyddade variabeln vid implementeringen av metoden. Sportadmin har uppgett att intrånget sannolikt utförts genom denna variabel. IMY saknar anledning att ifrågasätta denna uppgift.

IMY bedömer, även med beaktande av att det inte med full säkerhet kan konstateras vad som orsakat intrånget, att Sportadmin inte har haft ett tillräckligt skydd för att förhindra den typ av dataintrång som bolaget utsatts för. Sportadmin har sedan år 2021 återkommande identifierat att det funnits förhöjda risker för intrång i tjänsterna genom SQL-injektioner. I ärendet har det framkommit att en variabel trots det haft ett bristfälligt skydd mot sådana angrepp. Av utredningen framgår även att Sportadmin har avstått från att införa ytterligare skyddslager, exempelvis i form av WAF, som hade kunnat möjliggöra upptäckt och förhindrande av intrånget trots det bristfälliga skyddet för variabeln. Det har inte heller framkommit att bolaget i stället implementerat några andra tekniska åtgärder som skulle kunnat förhindra eller försvåra möjligheten att utföra SQL-injektioner. Sådana åtgärder har i stället genomförts först efter att personuppgiftsincidenten inträffat. Mot bakgrund av de höga risker för SQL-injektioner som identifierats och de allvarliga konsekvenser som ett sådant intrång riskerat

[11] Se EU-domstolens dom den 1 augusti 2022, C-184/20, Vyriausioji tarnybinės etikos komisija, EU:C:2019:773, p. 126.
[12] Se artikel 87 i dataskyddsförordningen och 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning som ger ett särskilt skydd för sådana personuppgifter.

medföra för de registrerade bedömer IMY att ytterligare åtgärder för att skydda tjänsterna mot sådana intrång lämpligen borde ha genomförts i ett tidigare skede.

Förutom avsaknaden av skydd mot SQL-injektioner framgår det av utredningen att Sportadmin, trots bolagets vetskap om de förhöjda riskerna i samband med SQL-injektioner via de publikt exponerade delarna av tjänsterna, har haft för höga rättigheter i tjänsternas bakomliggande system. Detta har möjliggjort för hotaktören att komma åt mer information vid intrånget än om så inte varit fallet. IMY konstaterar att en restriktiv uppsättning av behörigheter och uppföljning av dessa är en grundläggande säkerhetsåtgärd som begränsar möjligheten för obehöriga att bereda sig tillgång till personuppgifter och att sådana åtgärder hade kunnat begränsa omfattningen av det aktuella intrånget.

Mot denna bakgrund bedömer IMY sammantaget att Sportadmin inte i tillräcklig utsträckning har vidtagit lämpliga tekniska och organisatoriska åtgärder i förhållande till de risker som förelegat för dataintrång. Personuppgifterna har därmed inte getts ett tillräckligt skydd mot risken för obehörigt röjande och obehörig åtkomst.

Bristande åtgärder för att upptäcka de bristfälliga säkerhetsåtgärderna

IMY konstaterar att Sportadmin inte har upptäckt de konstaterade bristerna i skyddet mot SQL-injektioner i samband med kodgranskning som gjordes vid förändringen i juni 2022, och inte heller vid någon av de genomlysningar som skett därefter. Avsaknaden av ett sådant skydd har inte heller upptäckts i samband med att Sportadmin infört en uppdaterad säkerhetsmetod mot SQL-injektioner år 2023.

IMY anser att det har ankommit på Sportadmin att vidta lämpliga åtgärder för att löpande följa upp och säkerställa att vidtagna säkerhetsåtgärder varit tillräckligt effektiva. Den identifierade bristen i skyddet mot SQL-injektioner har varit av sådan grundläggande karaktär att Sportadmin borde ha upptäckt och åtgärdat den. Sportadmin har dock inte haft tillräckliga rutiner för kodgranskning för att upptäcka bristen vilket har lett till att den aktuella variabeln implementerats utan tillräckliga säkerhetsåtgärder. Bolaget har inte heller haft förmågan att under den långa period från det att variabeln infördes till att den aktuella personuppgiftsincidenten inträffade identifiera och åtgärda den aktuella bristen i efterhand. Mot bakgrund av de höga riskerna för SQL-injektioner som Sportadmin identifierat och att bolaget trots det inte upptäckt att det under en längre tid funnits grundläggande brister i skyddet mot sådana angrepp, bedömer IMY att bolagets rutiner för kodgranskning inte har varit tillräckliga för att följa upp effektiviteten av de tekniska och organisatoriska åtgärderna i syfte att säkerställa behandlingens säkerhet.

Bristande åtgärder för att upptäcka intrång eller intrångsförsök

Av Sportadmins redogörelse framgår att det övervakningssystem som bolaget använt har varnat för onormal aktivitet först när bolagets servrar slutat svara den 16 januari 2025, det vill säga två dagar efter att intrångsförsöken påbörjats den 14 januari 2025. Enligt Sportadmin har bolagets övervakningssystem inte utgjort ett verktyg för att i realtid bevaka och upptäcka intrångsförsök. Övervakningssystemet som använts har i stället bevakat och analyserat hårdvara, mjukvara och användande. Sportadmin har uppgett att bolaget har kunnat identifiera misstänkt aktivitet genom manuell analys av loggar från systemet på daglig basis och vid oväntade förändringar i systemets prestanda.

IMY konstaterar att de tekniska och organisatoriska säkerhetsåtgärderna som Sportadmin vidtagit för att övervaka säkerhetsrelaterade händelser inte har varit tillräckliga för att upptäcka eller varna för de initiala intrångsförsöken, körningen av skadlig kod från hotaktören eller överföringen av personuppgifter. Mot bakgrund av de höga risker som personuppgiftsbehandlingen inneburit och med hänsyn till att Sportadmin under flera år identifierat förhöjda risker för SQL-injektioner, bedömer IMY att Sportadmin borde ha vidtagit lämpliga åtgärder för att automatiskt i realtid identifiera förestående hot i form av exempelvis intrång eller intrångsförsök som kan leda till obehörig åtkomst. Om sådana åtgärder vidtagits hade Sportadmin haft bättre förutsättningar att förhindra eller i vart fall begränsa skadan för de registrerade.

Sammanfattande bedömning

Sammantaget bedömer IMY att Sportadmin inte har vidtagit tillräckliga åtgärder för att säkerställa att personuppgifterna som behandlats i bolagets tjänster skyddats mot risken för bland annat obehörigt röjande eller obehörig åtkomst till följd av dataintrång. Vidare har bolaget, trots vetskapen om de förhöjda riskerna för SQL-injektioner, saknat förmågan att identifiera att de åtgärder som vidtagits i syfte att skydda tjänsterna mot sådana intrång varit bristfälliga. Bolaget har inte heller haft förutsättningar för att upptäcka intrånget i tillräckligt god tid för att förhindra eller i vart fall begränsa konsekvenserna av det. Mot denna bakgrund bedömer IMY att Sportadmin 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 16 januari 2025.

Val av ingripande

Vad Sportadmin har uppgett

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

Om IMY bedömer att Sportadmin har behandlat personuppgifter i strid med artikel 32 ska i första hand ingen sanktionsavgift utgå och i andra hand sanktionsavgiften bestämmas till ett lågt belopp.

Incidenten har skett på grund av att en extern aktör utnyttjat en tillfällig svaghet i Sportadmins IT-säkerhetssystem och har inte berott på att bolaget haft ett generellt otillräckligt eller undermåligt säkerhetssystem. Sportadmin har vidtagit omfattande tekniska och organisatoriska säkerhetsåtgärder för personuppgifterna i tjänsterna. Om dessa inte bedöms tillräckliga har bolaget varken agerat uppsåtligen eller oaktsamt genom att inte vidta skyddsåtgärder utöver vad som tillämpades vid tidpunkten för incidenten. Omständigheten att en eventuell brist inte har varit uppsåtlig talar för att överträdelsen är av lägre allvarlighetsgrad. Vidare har endast 115 föreningar och 25 medlemmar hört av sig till Sportadmin med ersättningskrav på grund av bristande funktionalitet i tjänsterna samt för att incidenten medfört en oro och osäkerhet för medlemmarna. Att tycka att en situation är obehaglig är dock inte samma sak som att drabbas av en reell skada. Utifrån det totala antalet individer som berörts av incidenten är det fråga om ett mycket lågt antal personer som har, eller anser sig ha, lidit skada.

Det föreligger flera förmildrande omständigheter bland annat i form av att bolaget på eget initiativ har anmält händelsen till IMY och har samarbetat med myndigheten och vidtagit åtgärder för att mildra skadan för de registrerade. Bolaget har bland annat

vidtagit mer omfattande åtgärder än som krävts för att skydda personuppgifterna i tjänsterna efter incidenten vilket medfört ökade driftkostnader och minskad användarvänlighet vilket har haft en negativ påverkan på bolagets kundnöjdhet. Sportadmin har tagit ett långtgående ansvar för att möjliggöra för föreningarna att göra incidentanmälningar samt uppfylla sin informationsskyldighet gentemot de registrerade. Arbetet har medfört stora kostnader för Sportadmin och haft stor inverkan på arbetsmiljön för de anställda. Incidenten har även i övrigt medfört ekonomiska förluster för bolaget på grund av att annat arbete än det som rört incidenten behövt nedprioriteras. Vidare har incidenten fått stor medial spridning på ett sätt som påverkat bolaget negativt. Sportadmin har inte tidigare gjort sig skyldig till någon överträdelse av dataskyddsförordningen och har vidtagit omfattande åtgärder för att minimera risken för liknande händelser.

Med beaktande av det säkerhetsarbete Sportadmin genomfört före och efter incidenten i syfte att begränsa skadan för de registrerade, Sportadmins uppvisade samarbete med IMY, föreningarna och även polisen samt den skada incidenten medfört för bolaget är en sanktionsavgift inte en effektiv eller proportionerlig åtgärd. IMY kan uppnå samma effekt med en mindre ingripande åtgärd i form av en reprimand.

Det är Sportadmins omsättning som ska ligga till grund för en beräkning av en eventuell sanktionsavgift. Sportadmins moderbolag äger endast 85 procent av aktierna i Sportadmin och förfogar inte på något sätt över övriga röster i Sportadmin. Det föreligger därmed ingen presumtion för att Sportadmin och moderbolaget utgör en ekonomisk enhet. Moderbolaget utövar inte, och har inte heller möjlighet att utöva, ett avgörande inflytande över Sportadmins beteende. Sportadmin har fortsatt att bedrivas som en fristående affärsenhet efter förvärvet. Sportadmin utgör en egen ekonomisk enhet, har en egen ledningsgrupp och styrelse samt ett separat kontor i förhållande till sitt moderbolag. Sportadmin har även en egen driftsmiljö och utvecklingsorganisation och vid tidpunkten för incidenten hade bolaget ingen assistans avseende drift från moderbolaget. Vidare arbetade ingen från moderbolaget för Sportadmin på regelbunden basis. Vid tidpunkten för överträdelsen hade Sportadmin endast funnits i koncernen under en kort tid. Moderbolaget har inte haft någon operativ kontroll och ansvar för den dagliga styrningen av Sportadmins produktutveckling, tekniska miljö eller drift och inte heller för övriga avdelningar. Sportadmin agerar således självständigt i såväl strategiska som operativa frågor kopplade till tjänsternas utformning och hantering av personuppgifter.

Tillämpliga bestämmelser

Val av korrigerande åtgärder och beräkning av sanktionsavgiftens storlek
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 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.[13]

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).[14] 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 årsomsättningen under föregående räkenskapsår.[15] 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.[16]

Av EU-domstolens praxis framgår att begreppet företag omfattar varje enhet som utövar ekonomisk verksamhet, oavsett enhetens rättsliga form och sättet för dess finansiering samt även om enheten i juridisk mening består av flera fysiska eller juridiska personer. Olika företag inom samma koncern kan således bilda en ekonomisk enhet och därmed utgöra ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget.[17] En sådan ekonomisk enhet består av en enhetlig organisation med personal samt materiella och immateriella tillgångar, vilken på ett varaktigt sätt strävar efter att uppnå ett bestämt ekonomiskt mål, och som kan medverka till en överträdelse enligt artikel 101.1 EUF-fördraget.[18]

Frågan om moderbolag och dotterbolag ska betraktas som en del av samma ekonomiska enhet beror till stor del på om dotterbolaget, trots att det är en självständig juridisk person, inte självständigt bestämmer sitt beteende på marknaden utan huvudsakligen tillämpar instruktioner som det får från moderbolaget som kan anses utöva ett avgörande inflytande över dotterbolaget. Kriterierna för att fastställa detta bygger på de ekonomiska, rättsliga och organisatoriska kopplingarna mellan moderbolaget och dess dotterbolag, exempelvis storleken på deltagandet, personalen eller organisatoriska kopplingar, instruktioner och förekomsten av företagskontrakt.[19]

---

[13] Se EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR.
[14] Se skäl 150 till dataskyddsförordningen.
[15] Se EU-domstolens dom den 5 december 2023, Deutsche Wohnen, C-807/21, EU:C:2023:950, p. 57.
[16] Se EU-domstolens dom den 13 februari 2025, ILVA, C-383/23, EU:C:2025:84, p. 36.
[17] Se EU-domstolens dom den 27 april 2017, Akzo Nobel, C-516/15 P, EU:C:2017:314, p. 48.
[18] Se EU-domstolens dom den 6 oktober 2021, Sumal SL mot Mercedes Benz Trucks España SL, C-882/19, EU:C:2021:800, p. 41.
[19] Se bland annat EU-domstolens domar den 20 januari 2011, General Química m.fl. mot kommissionen, C-90/09 P, EU:C:2011:21, p. 37 och den 6 oktober 2021, Sumal SL mot Mercedes Benz Trucks España SL, C-882/19, EU:C:2021:800, p. 43 samt EDPB:s riktlinjer 04/2022, p. 122.

För att avgöra huruvida det har förelegat en ekonomisk enhet kan även beaktas om samma personer innehar nyckelposter i ledningen för bolagen i en koncern.[20]

EU-domstolen har uttalat att omständigheten att ett dotterbolag i huvudsak tillämpar instruktioner från moderbolaget och inte självständigt kan anses bestämma sitt agerande på marknaden endast utgör ett tecken på att en ekonomisk enhet föreligger, men utgör inte den enda omständigheten som gör moderbolaget ansvarigt. Domstolen har även uttalat att det inte är avgörande huruvida moderbolaget har blandat sig i dotterbolagets löpande verksamhet. Ett moderbolag kan ha ett avgörande inflytande på dotterbolaget även om det inte har någon konkret medbestämmanderätt eller tillhandahåller några konkreta instruktioner eller riktlinjer avseende enskilda delar av affärspolitiken. Följaktligen kan en gemensam affärspolitik inom en koncern även framgå indirekt av det sammanlagda ekonomiska och rättsliga sambandet mellan moderbolaget och dess dotterbolag. Till exempel kan moderbolagets inflytande på dess dotterbolag avseende företagets strategi, verksamhetspolitik och -planer, investeringar, kapacitet, finansiering, personalfrågor och rättsliga frågor indirekt påverka dotterbolagets och hela koncernens agerande på marknaden.[21]

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.[22]

IMY:s bedömning

Sanktionsavgift ska påföras
IMY har bedömt att Sportadmin 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. Av Sportadmins uppgifter i ärendet framgår att den oskyddade variabeln, som sannolikt möjliggjorde SQL-intrånget i januari 2025, infördes redan i juni 2022. De konstaterade bristerna har lett till obehörig åtkomst till en stor mängd personuppgifter som huvudsakligen gällt barn och 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.[23]

Sportadmin har i egenskap av personuppgiftsbiträde, och i begränsad omfattning även som personuppgiftsansvarig, haft ett ansvar för att uppfylla dataskyddsförordningens

---

[20] Se EU-domstolens dom den 1 juli 2010, Knauf Gips KG mot kommissionen, C-407/08 P, EU:C:2010:389, p. 66, 72 och 85–86.
[21] Se EU-domstolens dom den 10 september 2009, Akzo Nobel m.fl. mot kommissionen, C-97/08 P, EU:C:2009:536, p. 72 och 73 som hänvisar till p. 87–94 i generaladvokatens förslag till avgörande den 23 april 2009 i samma mål.
[22] Se EU-domstolens domar den 10 september 2009, Akzo Nobel m.fl. mot kommissionen, C-97/08 P, EU:C:2009:536, p. 59–61 och den 14 juli 1972, ICI mot Commission, C-48/69, EU:C:1972:70, p. 136.
[23] Se EU-domstolens domar 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.

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 IMY kommit fram till att Sportadmin behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen. IMY bedömer att Sportadmin inte kan anses ha varit okunnigt om att agerandet inneburit en överträdelse av förordningen. IMY anser mot denna bakgrund att Sportadmin har varit oaktsamt i förhållande till den överträdelse av dataskyddsförordningen som konstaterats. Samtliga förutsättningar för att påföra Sportadmin en sanktionsavgift är därmed uppfyllda.

Lime-koncernens årsomsättning ska ligga till grund för beräkningen av sanktionsavgiften

Av Sportadmins årsredovisning för år 2024 framgår följande. Den 9 januari 2024 tecknade Lime Technologies Sweden AB (Lime Sweden) avtal om att förvärva aktierna i Sportadmin. Den första delen av förvärvet avsåg 85 procent av aktierna och rösterna, och genomfördes den 9 januari 2024. Resterande 15 procent av aktierna ska förvärvas det tredje kvartalet 2027. Sportadmin och Lime Sweden ingår i koncernen Lime Technologies Group (Lime-koncernen) vars moderbolag är Lime Technologies AB (publ) (Lime).

Lime äger 100 procent av aktierna i Lime Sweden. Enligt Akzo-principen föreligger därmed en presumtion, som inte har motbevisats i ärendet, för att Lime utövar ett avgörande inflytande över Lime Swedens beteende. Den aktuella presumtionen är inte tillämplig avseende förhållandet mellan Lime Sweden och Sportadmin. IMY konstaterar dock att Lime Swedens betydande aktieinnehav om 85 procent i Sportadmin, tillsammans med avtalet om att ett heltäckande förvärv ska ske inom en överskådlig framtid, utgör omständigheter som bör tillmätas stor vikt vid bedömningen av om Lime Sweden vid tidpunkten för överträdelsen utövade ett avgörande inflytande över Sportadmin. Därutöver beaktas även följande omständigheter som enligt IMY:s mening talar för att Lime, Lime Sweden och Sportadmin ska betraktas som en ekonomisk enhet.

I Limes årsredovisning för 2024 benämns Sportadmin genomgående som ”Lime Sportadmin”. Vidare framhålls köpet av Sportadmin som ett sätt att stärka Limes produktportfölj samt möjliggöra en lokal tillväxtpotential och långsiktig internationalisering, där Lime Sportadmins produktutbud förväntas bidra till både tillväxt och lönsamhet för koncernens resultat. Av årsredovisningen framgår även att internationaliseringen av Sportadmin har påbörjats genom förvärv av ett nederländskt bolag, som Sportadmin äger 100 procent av aktierna i. Det anges också att koncernen fortsätter ha en aktiv Mergers and Acquisitions Agenda för Sportadmins vidare internationalisering. I årsredovisningen anges även att Lime, i samband med förvärvet av Sportadmin, adderade medlemsorganisationer som en femte fokusbransch, där Lime under en längre tid stärkt sin position på flera marknader bland idrottsföreningar och andra typer av medlemsbolag. Vidare anges att sedan Sportadmin blev en del av Lime-koncernen har koncernen fortsatt att utveckla Sportadmins plattform med fokus på användarvänlighet, integrationer och skalbarhet. IMY anser att dessa uttalanden ger stöd för att det föreligger sådana gemensamma planer och ekonomiska mål inom koncernen som bolagen tillsammans strävar mot, som utgör ytterligare faktorer som talar för att bolagen i fråga utgör en ekonomisk enhet.

Av Sportadmins respektive Lime Swedens årsredovisningar för år 2024 framgår att två av fem styrelseledamöter hade chefs- och styrelsepositioner inom både Sportadmin och Lime Sweden vid tidpunkten för överträdelsen. Vidare framgår av Limes

årsredovisning för år 2024 att fyra av styrelseledamöterna i Sportadmin även ingick i koncernledningen och den utökade ledningsgruppen för Lime, varav en i egenskap av VD och koncernchef för Lime-koncernen. Det kan därmed konstateras att samma personer innehaft nyckelposter i ledningen för flera av de aktuella bolagen samtidigt.

Vidare anges i Sportadmins personuppgiftspolicy att eftersom Sportadmin ingår i Lime-koncernen behandlar även Lime Sweden, som hanterar koncernens huvudsakliga administrativa funktioner, de registrerades personuppgifter som gemensamt personuppgiftsansvariga med Sportadmin. Av Sportadmins redogörelse för personuppgiftsincidenten framgår även att Lime Swedens chefsjurist har agerat som Sportadmins juridiska ombud i det juridiska team som sattes samman med anledning av incidenten. Vidare framgår att Lime-gruppens interna kompetens nyttjats i samband med vidtagandet av tekniska och organisatoriska åtgärder efter personuppgiftsincidenten. Sportadmin har även uppgett att bolaget sedan 2024 haft tillgång till dokumenterade rutiner för kodändringar som tagits fram av Lime-koncernen som stöd i sitt arbete med säkerhetsaspekten i utvecklingsprocessen. Enligt Sportadmin har bolaget sedan förvärvet arbetat med att implementera dessa dokument i sin verksamhet. IMY bedömer att dessa omständigheter ger stöd för att det finns tydliga organisatoriska kopplingar, bland annat vad gäller personal och tillämpning av instruktioner, mellan de berörda bolagen.

Vid en samlad bedömning av ovanstående ekonomiska, rättsliga och organisatoriska kopplingar mellan bolagen bedömer IMY att dessa ska betraktas som en sådan ekonomisk enhet som utgör ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Beräkningen av sanktionsavgiften ska därför göras utifrån Lime-koncernens årsomsättning för år 2024[24] vilken var cirka 685 700 000 kronor. Två procent av Lime-koncernens årsomsättning för år 2024 är därmed 13 714 000 kr. 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.[25]

Sportadmin har haft en långtgående skyldighet att skydda personuppgifterna som behandlas i bolagets tjänster som används av ett stort antal idrottsföreningar i hela Sverige. De konstaterade bristerna i skyddet för personuppgifter har varit av grundläggande karaktär och medfört möjlighet till obehörig åtkomst till över två miljoner personers uppgifter. Merparten av personuppgifterna har omfattat barn, som på grund av sin sårbarhet ska ges ett särskilt starkt skydd för sina personuppgifter. Överträdelsen har vidare omfattat en stor mängd uppgifter om varje person, vilket medför att integritetsriskerna ökat.[26] Uppgifterna i fråga har därtill omfattat känsliga personuppgifter om hälsa och andra uppgifter av integritetskänslig karaktär i form av personnummer och skyddade personuppgifter. Överträdelsen har dessutom gällt den centrala behandlingen av personuppgifter i Sportadmins kärnverksamhet, där bolaget får förutsättas ha goda förutsättningar att vidta lämpliga säkerhetsåtgärder i

[24] Om företaget omfattas av en skyldighet att upprätta koncernredovisningar, vilket Lime gör, är det koncernredovisningen för koncernens moderbolag som är relevant för att återspegla företagets sammanlagda omsättning, se EDPB:s riktlinjer 04/2022, p. 130 och EU-domstolens dom den 30 maj 2013, Groupe Gascogne SA mot kommissionen, C-58/12P, EU:C:2013:770, p. 54–56.
[25] Se EDPB:s riktlinjer 04/2022, p. 60.
[26] Se EDPB:s riktlinjer 04/2022, p. 58.

förhållande till identifierade risker. Det gör att överträdelsen ska anses som allvarligare, än om så inte varit fallet.[27]

Bristerna i skyddet för personuppgifterna har lett till att hotaktören kunnat bereda sig tillgång till och därefter publicera personuppgifter från tjänsterna på Darknet. IMY konstaterar att en obehörig åtkomst till den typ av personuppgifter som behandlas i tjänsterna medför en hög risk för skada för de registrerade. Detta särskilt med beaktande av att EU-domstolen 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.[28] Sportadmins bristfälliga agerande har därmed, enligt IMY, haft stor påverkan på de registrerades fri- och rättigheter.

Bedömningen av överträdelsens allvar påverkas även av faktorer som varaktighet och, beroende på omständigheterna i det enskilda fallet, graden av oaktsamhet i förhållande till konstaterade brister.[29] Sportadmin har under flera års tid identifierat förhöjda risker för sådana SQL-injektioner som sannolikt orsakat den aktuella personuppgiftsincidenten. Det innebär att Sportadmin under en lång period underlåtit att vidta tillräckliga säkerhetsåtgärder för att förhindra och upptäcka den aktuella typen av dataintrång, trots att bolaget under hela denna period varit medvetet om de risker som ett sådant bristfälligt skydd innebar. IMY konstaterar att bolaget beslutat att avvakta med att vidta flera lämpliga åtgärder för att förstärka skyddet mot SQL-injektioner och andra dataintrång, trots att åtgärderna var nödvändiga för att säkerställa ett tillräckligt skydd. Av utredningen framgår att bolaget haft förmåga att utföra sådana åtgärder på kort tid efter personuppgiftsincidenten. Mot denna bakgrund, och med beaktande av behandlingens omfattning och karaktär, bedömer IMY att Sportadmin har uppvisat en sådan hög grad av oaktsamhet att det ska beaktas i skärpande riktning.

Med hänvisning till 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 Sportadmin vidtagit flera tekniska och organisatoriska åtgärder efter incidenten bland annat i syfte att skydda de registrerades personuppgifter, minska påverkan på de registrerade och stärka IT-säkerheten långsiktigt. IMY konstaterar att de genomförda åtgärderna i stor utsträckning omfattat sådant som borde ha vidtagits redan innan incidenten inträffade för att uppnå en lämplig säkerhetsnivå. De vidtagna åtgärderna kan inte heller anses gå utöver vad som kan förväntas av Sportadmin i det aktuella fallet. 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.[30]

---

[27] Se EDPB:s riktlinjer 04/2022, p. 53.
[28] Se EU-domstolens domar den 14 december 2023, Natsionalna agentsia za prihodite, C-340/21, EU:C:2023:986, p. 82 och den 4 oktober 2024, Agentsia po vpisvaniyata, C-200/23, EU:C:2024:827, p. 145.
[29] Se EDPB:s riktlinjer 04/2022, p. 56. Som framgår av den hänvisade punkten i riktlinjerna, och Kammarrätten i Stockholms dom den 16 december 2022 i mål 7837-21, saknas det däremot stöd för att bedöma allvarligheten i en överträdelse minskar till följd av att den inte skett uppsåtligen på det sätt som Sportadmin argumenterat för.
[30] Se EDPB:s riktlinjer 04/2022, p. 74.

Den omständigheten att Sportadmin 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.[31]

Däremot beaktar IMY som förmildrande vid bedömningen av sanktionsavgiftens storlek att Sportadmin har tagit en aktiv och samordnande roll för att möjliggöra för samtliga föreningar som omfattats av personuppgiftsincidenten att uppfylla sina skyldigheter att lämna in incidentanmälningar till IMY i rätt tid. Sportadmin har dessutom utgjort en central kontaktpunkt mellan IMY, bolaget och föreningarna samt bistått föreningarna i att lämna information om incidenten till berörda registrerade i syfte att bland annat underlätta för dessa personer att vidta försiktighetsåtgärder för att skydda sina personuppgifter.

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

Sanktionsavgiftens storlek
IMY bestämmer utifrån en samlad bedömning att Sportadmin ska betala en administrativ sanktionsavgift på 6 000 000 kronor. Vid bestämmandet av sanktionsavgiftens storlek har överträdelsens höga allvarlighetsgrad och Lime-koncernens omsättning beaktats.[32] IMY har som en förmildrande omständighet beaktat Sportadmins agerande i samband med incidenten men också tagit hänsyn till att överträdelsen skett inom ramen för Sportadmins verksamhet och inte i övriga delar av koncernen. Sammanfattningsvis bedömer IMY att sanktionsavgiften är effektiv, proportionerlig och avskräckande.

Detta beslut har fattats av generaldirektören Eric Leijonram efter föredragning av avdelningsjuristen Maja Welander. Vid den slutliga handläggningen har även rättschefen David Törngren, enhetschefen Christelle Bourquin, rådgivaren Sara Ahmed, juristen Viktor Johnsson samt it- och informationssäkerhetsspecialisten Johnny Gordon Tornesjö medverkat.

Eric Leijonram

Bilaga

Information om betalning av sanktionsavgift.

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

---

[31] Se EDPB:s riktlinjer 04/2022, p. 95–98.
[32] 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.

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.