Delphi

Klara Thyrén

IMY beslutar om 6 miljoner i sanktionsavgift efter omfattande dataintrång

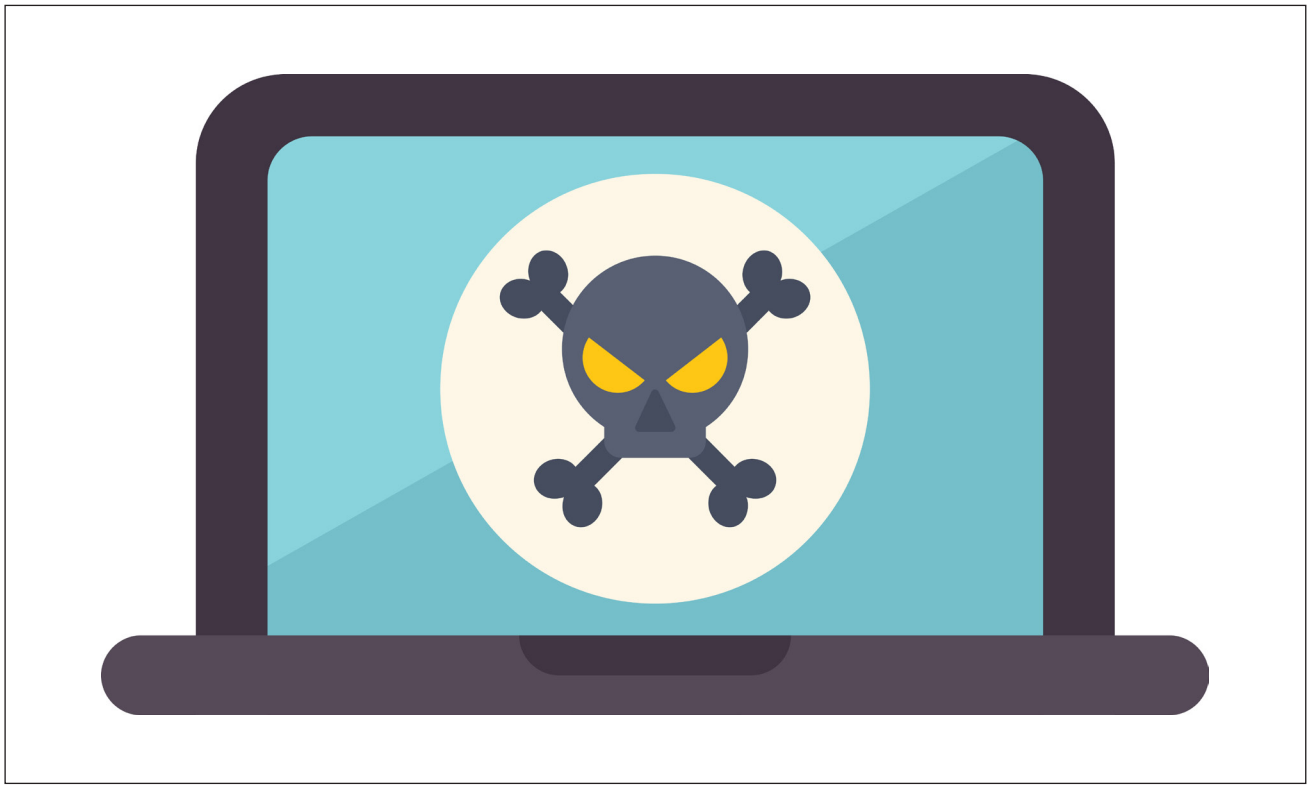
Integritetsskyddsmyndigheten (”**IMY**”) beslutade den 26 januari 2026 att ålägga Sportadmin i Skandinavien AB (”**Sportadmin**”), som är ett bolag som tillhandahåller digitala kommunikationstjänster för idrottsföreningar, en sanktionsavgift om 6 miljoner kronor. Beslutet följer den tillsyn som inleddes mot Sportadmin under 2025 med anledning av det dataintrång som upptäcktes den 16 januari 2025. Sportadmin agerade huvudsakligen som personuppgiftsbiträde, men var i viss utsträckning även personuppgiftsansvarig, och tillsynen avsåg frågan om Sportadmin hade vidtagit lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32.1 GDPR.

Enligt Sportadmin hade avvikande utgående trafik från produktionsmiljön identifierats genom loggar, vilket indikerade en eventuell dataöverföring. Sportadmin hade trots det inte kunnat fastställa att en dataöverföring faktiskt skett, men den 14 mars 2025 publicerades data som hotaktören kommit åt på Darknet. Sportadmin vidtog ett flertal åtgärder efter incidenten. Redan en timme efter att incidenten upptäcktes stängdes samtliga tjänster ner. Bolaget genomförde vidare tekniska åtgärder för att förhindra fortsatt åtkomst för hotaktören, bland annat genom att aktivera en ny produktionsmiljö och att gå igenom befintlig funktionalitet. Sportadmin informerade samtliga berörda föreningar och uppmanade dessa att anmäla incidenten till IMY samt bistod med att underlätta för korrekta och fullständiga anmälningar.

Vid intrånget berördes över två miljoner personer. De personuppgifter som omfattades innefattade bland annat personnummer, kön, relation mellan målsman och medlem, idrottstillhörighet samt nationalitet. Därutöver omfattades känsliga personuppgifter om hälsa, såsom uppgifter om allergier och funktionsnedsättningar. En betydande andel av de registrerade utgjordes av barn och ungdomar. Det framkom även att skyddade personuppgifter i viss utsträckning hade behandlats, trots att detta inte var avsett att göras i tjänsten.

IMY fann att de tekniska och organisatoriska åtgärderna inte var tillräckliga i förhållande till de risker som förelåg. Intrånget genomfördes genom en så kallad SQL-injektion, vilket är ett sätt för angripare att få åtkomst till databaser genom att utnyttja en säkerhetsbrist. Bristen upptäcktes varken vid den kodgranskning som genomförts, vid efterföljande genomlysningar eller då bolaget införde en uppdaterad säkerhetsmetod mot just denna typ av injektioner. Därutöver konstaterade IMY att de för höga rättigheterna i de bakomliggande systemen möjliggjorde tillgång till mer information än vad som annars hade varit möjligt. IMY noterade att bolagets system inte var utformat för att i realtid upptäcka intrångsförsök, utan endast övervakade prestanda och belastning. Varning utlöstes först två dagar efter att intrångsförsöken påbörjats. Sammantaget bedömde IMY att bolaget saknade tillräckliga åtgärder för att förhindra dataintrång, för att identifiera brister i befintligt skydd samt för att upptäcka pågående intrång i tillräckligt god tid.

IMY bedömde att överträdelsen var av hög allvarlighetsgrad med beaktande av bland annat svårighetsgrad, karaktär och varaktighet. Bristerna i skyddet ansågs vara av grundläggande karaktär, och intrånget omfattade ett mycket stort antal registrerade och en betydande mängd uppgifter om varje person, däribland känsliga personuppgifter och uppgifter om barn. Obehörig åtkomst till sådana uppgifter kan leda till allvarliga konsekvenser för de berörda, vilket enligt IMY ställde



Illustrasjon: Colourbox.com

krav på en hög säkerhetsnivå. Risker för denna typ av injektioner hade även förelegat under en längre period och Sportadmin hade därmed under en längre period undvikt att vidta nödvändiga säkerhetsåtgärder. Det bristfälliga skyddet som i sin tur resulterade i publiceringen av personuppgifter på Darknet innebar en betydande påverkan på de registrerades fri- och rättigheter. IMY hänvisade till EU-domstolens avgörande i mål C-340/21, där domstolen slagit fast att skada kan uppstå redan vid förlust av kontroll över personuppgifter.

IMY angav slutligen att den höga graden av oaktsamhet skulle beaktas som en försvårande omständighet. De åtgärder som vidtogs efter incidenten ansågs i huvudsak utgöra sådant som borde ha genomförts redan dessförinnan. Vad gäller förmildrande omständigheter beaktade IMY att Sportadmin hade tagit en aktiv roll i att bistå föreningarna med incidentanmälningar och information till de registrerade.

Vid fastställande av sanktionsavgiftens storlek prövade IMY huruvida Sportadmin och dess moderbolag, som vid tiden för beslutet ägde 85 % av aktierna, skulle anses utgöra en ekonomisk enhet. Begreppet företag enligt EU-domstolens praxis omfattar samtliga enheter som utövar ekonomisk verksamhet, även om dessa består av flera juridiska personer. Mellan koncernbolagen förelåg betydande organisatoriska, ekonomiska och rättsliga kopplingar. Mot denna bakgrund bedömde IMY att bolagen utgjorde en ekonomisk enhet, varför sanktionsavgiften skulle beräknas utifrån koncernens samlade årsomsättning.

Sanktionsavgiften fastställdes med beaktande av överträdelsens höga allvarlighetsgrad och koncernens omsättning. IMY bedömde att avgiften om 6 000 000 kronor var effektiv, proportionerlig och avskräckande.

Beslutet ger vägledning i vad IMY beaktar vid bedömningen av huruvida organisationer har vidtagit tillräckliga tekniska och organisatoriska säkerhetsåtgärder. Säkerhetsnivån ska anpassas utifrån de risker som föreligger i den specifika situationen, där vissa uppgifter kräver högre skyddsnivå. Det är vidare av vikt att exempelvis ha rutiner på plats som möjliggör upptäckt av eventuella intrång direkt. Organisationer bör säkerställa att deras säkerhetsåtgärder regelbundet ses över och anpassas i takt med förändrade risker och teknisk utveckling.

Klara Thyrén, arbetar som associate inom Tech & IP på Advokatfirman Delphi.