Indecap AB

Diarienummer:
DI-2021-3422

Datum:
2023-11-07

Beslut efter tillsyn enligt dataskyddsförordningen – Indecap AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Indecap AB (556622–4480) har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1] genom att, i samband med ett utskick per e-post den 20 januari 2021, inte ha säkerställt en lämplig säkerhetsnivå i förhållande till riskerna med behandlingen.

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Indecap AB ska betala en administrativ sanktionsavgift på 500 000 kronor för överträdelsen av artikel 32.1 i dataskyddsförordningen.

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY) har mottagit klagomål som gör gällande att Indecap AB (Indecap) den 20 januari 2021 felaktigt skickat ett e-postmeddelande innehållande en fil med personuppgifter om bland annat kunders ekonomi till andra kunder. IMY har inlett tillsyn mot Indecap i syfte att utreda det som framgår av klagomålen.

Indecap har uppgett att det anser sig personuppgiftsansvarigt för den aktuella personuppgiftsbehandlingen. Bolaget har därutöver sammanfattningsvis uppgett följande.

All information i Indecaps system var skyddad och krävde inloggning av användarna för att få åtkomst till informationen som inkluderades i det felaktiga utskicket. Det som inträffade i det aktuella fallet var att en medarbetare hämtade ut information ur systemet innehållande personuppgifter för att bearbeta informationen till en rapport i Excel. Under bearbetningen sparades Excel-filen ned och döptes olyckligt till ett liknande namn som den generella PDF-rapport över fondernas utveckling som skulle skickas ut till kunder. När medarbetaren senare skulle bifoga PDF-rapporten i utskicket råkade medarbetaren bifoga den Excel-fil som var under bearbetning och som innehöll personuppgifter, istället för den korrekta PDF-rapporten. På grund av det mänskliga

[1] Europaparlamentet 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).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

misstaget skickades den felaktiga filen därmed ut till ett antal kunder innan felet uppmärksammades och utskicket stoppades.

Den felaktigt bifogade filen som skickades med e-post till bolagets kunder innehöll uppgifter om kunders namn, personnummer, bank, namn på bankrådgivare, mailadress, vald risknivå, fördelning på fonder (begränsat till enskilt fondval) samt det senast inlästa värdet av kundernas innehav i dessa fonder. Filen innehöll inga uppgifter om kontonummer, inloggningsuppgifter, andelsinnehav i specifika fonder, eller information om fondportföljer gällande kapitalförsäkringar, tjänste- eller privatpensioner. De felaktiga utskicken omfattade 52 364 registrerades personuppgifter, och mottogs av maximalt 2 813 personer. Det exakta mottagarantalet kan inte fastställas då Indecaps egna undersökningar visar att mailet har fastnat i mailfiltret hos många av kunderna.

Indecap har en informationssäkerhetspolicy och tillämpar dokumenterade processer och rutiner kopplade till personuppgifts- och informationssäkerhetshantering. Innan incidenten inträffade hade Indecap behörighetsbegränsat de aktuella system som berör kunduppgifter, så att endast fyra medarbetare hade tillgång till dessa. Indecap hade vidare utbildat samtlig personal i personuppgifts- och informationssäkerhetsahantering.

Den internutredning som Indecap genomfört efter den aktuella incidenten har visat på svårigheter att efterleva Indecaps dualitetsrutin som tillämpas vid större hantering av personuppgifter. Rutinen innebär att två individer ska godkänna/verifiera en viss handling innan den kan genomföras. Orsaken till svårigheterna att efterleva denna rutin förklaras av det ökade distansarbete som krävts med anledning av Covid-19-pandemin. Det moment som vid incidenten inte genomfördes var att rent visuellt, med en s.k. four-eyes principle, säkerställa att rätt data matats in i systemet och bifogats korrekt innan uppgifterna skickades ut via e-post. Detta gick inte att göra på distans och gjorde det möjligt att bifoga den felaktiga filen. Den fil som felaktigt inkluderades i mailet var av denna anledning inte krypterad eller innehöll några läsbegränsningar. Åtkomst till ursprungsdatorn var dock både begränsad utifrån behörighet samt lösenordskyddad.

Innan incidenten inträffade hade Indecap lanserat en systembaserad applikation med inloggning via BankID i syfte att minska riskerna som uppstår när uppgifter skickas via e-post. Indecap hade innan incidenten fattat ett beslut om att under 2021 fasa ut sin rutin för mailutskick. Sedan incidenten inträffade skickas inte längre kvartalsrapporter ut per mail. Numera hänvisas istället kunder till att logga in med BankID hos Indecap för att se sin portföljutveckling. Vidare är rapporter innehållande kunduppgifter numera krypterade och lösenordskyddade.

Utöver att omedelbart stoppa all planerad kundkommunikation genom brev/mailutskick vidtog Indecap ett antal åtgärder i samband med att incidenten inträffade. Bolaget initierade en större incidentutredning tillsammans med externa experter för att kartlägga och dokumentera händelsen, samt för att utföra en kontroll av Indecaps systematiska dataskyddsarbete. Internutredningen, som har färdigställts, innehåller en analys av personuppgiftsincidentens allvarhetsgrad enligt ENISA:s metod för bedömning av personuppgiftsincidenter och plan för åtgärder. Därutöver har Indecap bland annat uppdaterat rutiner kring hemarbete och dualitetsprocessen, skickat information till registrerade om det inträffade, vidtagit ytterligare tekniska säkerhetsåtgärder och hållit extra utbildningsinsatser för anställda.

Indecap har lämnat in en anmälan om personuppgiftsincident till IMY och gjort en incidentanmälan till Finansinspektionen med anledning av den händelse som utreds i ärendet. I anmälan till IMY angav Indecap bland annat att bolaget kontaktat de mottagare som fått e-postmeddelandet med personuppgifter och bett dessa att radera meddelandet samt bekräfta att meddelandet hade raderats.

Motivering av beslutet

Tillämpliga bestämmelser

Personuppgiftsansvarig är 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. Den personuppgiftsansvarige ansvarar för och ska kunna visa att de grundläggande principerna i artikel 5 i dataskyddsförordningen följs. Det framgår av artikel 5.2 i dataskyddsförordningen.

Enligt artikel 5.1 f i dataskyddsförordningen ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

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

Enligt artikel 32.1 omfattar lämpliga skyddsåtgärder, när det är lämpligt,
a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

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

Medlemsstaterna får, enligt artikel 87 dataskyddsförordningen, närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av

lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Enligt 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning får personnummer och samordningsnummer behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Integritetsskyddsmyndighetens bedömning

Genom utredningen i ärendet har det framkommit att Indecap av misstag har skickat en okrypterad fil innehållande personuppgifter om ca 52 000 kunder med e-post till ca 2 800 mottagare som inte varit behöriga att motta den aktuella informationen. Den aktuella filen innehöll bland annat uppgifter om kunders namn, mailadress, personnummer, bank, risknivå, enskilt fondval och det senast inlästa värdet av kundens innehav i dessa fonder.

Indecap är personuppgiftsansvarig
Indecap har uppgett att bolaget är personuppgiftsansvarig för den personuppgiftsbehandling som granskas i ärendet.

Av utredningen framgår att syftet med att skicka det aktuella meddelandet var att informera kunder om fonders generella utveckling. IMY konstaterar att Indecap har bestämt ändamål och medel med behandlingen av personuppgifterna, det vill säga hur och varför personuppgifterna ska behandlas. Det är således Indecap som enligt artikel 4.7 i dataskyddsförordningen varit personuppgiftsansvarig för den aktuella behandlingen av personuppgifter.

Behandlingen har inneburit en hög risk
Indecap har enligt artikel 32 i dataskyddsförordningen en skyldighet att skydda de personuppgifter som bolaget behandlar genom att vidta lämpliga tekniska och organisatoriska åtgärder. Åtgärderna ska säkerställa en lämplig säkerhetsnivå. Vid bedömningen av vilken säkerhetsnivå som är lämplig ska den personuppgiftsansvarige beakta kostnaderna, behandlingens art, omfattning, sammanhang och ändamål och de risker för fysiska personers rättigheter och friheter som behandlingen medför.

Av 1 kap. 11 § första stycket lagen (2007:528) om värdepappersmarknaden följer att den som är eller har varit knuten till ett värdepappersbolag inte obehörigen får röja eller utnyttja vad han eller hon i anställningen eller under uppdraget har fått veta om någon annans affärsförhållanden eller personliga förhållanden. Eftersom Indecap är ett värdepappersbolag gäller dessa lagkrav om tystnadsplikt i bolagets verksamhet. Det ställer höga krav på skydd för de personuppgifter som behandlas i verksamheten.

I detta fall har de uppgifter som hanterats bland annat bestått av särskilt skyddsvärda personuppgifter, nämligen personnummer, som endast får behandlas under vissa förutsättningar. Det har även varit fråga om ekonomiska uppgifter, såsom det senaste innehavet i fonder samt det senast inlästa värdet av kundernas innehav i dessa fonder, för vilka de registrerade har berättigade förväntningar på en hög grad av konfidentialitet och ett robust skydd mot obehörig åtkomst. IMY konstaterar att sammanhanget för personuppgiftsbehandlingen medfört ett ännu högre krav på skyddsnivån. Personuppgiftsbehandlingen har skett inom ramen för Indecaps kärnverksamhet för vilken bolaget borde ha haft god förmåga att säkerställa en säkerhet som varit lämplig utifrån behandlingens omfattning och känslighet.

Att sammanställa en stor mängd personuppgifter av integritetskänslig karaktär medför dessutom särskilda risker då förlorad kontroll över en sådan sammanställning kan leda till skada för många registrerade. I det aktuella fallet har behandlingen rört uppgifter om ett stort antal registrerade (ca 52 000 personer).

Med hänsyn bland annat till att de uppgifter som Indecap behandlat har varit av skyddsvärd karaktär och berört ett mycket stort antal personer har Indecaps behandling av personuppgifterna sammantaget inneburit en hög risk för fysiska personers rättigheter och friheter. Behandlingens art, omfattning och sammanhang har därmed medfört ett krav på ett starkt skydd för uppgifterna. Åtgärderna skulle bland annat säkerställa att personuppgifterna skyddades mot obehörigt röjande och obehörig åtkomst.

Indecap har inte vidtagit tillräckliga åtgärder för att skydda uppgifterna
Av klagomålen och Indecaps redogörelse framgår att filen med personuppgifter har bifogats i ett e-postmeddelande som skickats ut till ett större antal personer. Indecaps utskick av den aktuella filen har inneburit att personer som inte har rätt att ta del av uppgifterna har fått åtkomst till dessa.

Indecap har uppgett att filen bifogades i e-postmeddelandet till följd av ett misstag från en enskild medarbetare. Indecap är, som personuppgiftsansvarig, ansvarig för all personuppgiftsbehandling som sker under bolagets ledning eller för bolagets räkning. I detta fall har det felaktiga bifogandet av filen skett inom ramen för den anställdes tjänst. Indecap är ansvarig för att behandlingen av personuppgifter som utförts av den anställde skett i enlighet med dataskyddsförordningens krav på en lämplig säkerhetsnivå.

IMY bedömer dessutom att det aktuella misstaget hade kunnat hindras eller i vart fall försvåras. Indecap behandlar i sin verksamhet såväl publik som skyddsvärd information. Beroende på bland annat informationens känslighet ställs olika krav på lämplig skyddsnivå och därmed innehållet i rutinerna för hantering av dessa uppgifter. Vid hanteringen av publik information saknas det till exempel anledning att beakta risken för obehörig åtkomst vid val av lämpliga kommunikationskanaler. För att inte äventyra skyddet för uppgifter av skyddsvärd karaktär borde Indecap ha haft tydliga rutiner för att säkerställa att hanteringen av skyddsvärd information inte skulle sammanblandas med hanteringen av publik information. Av Indecaps egna uppgifter framgår att en anledning till att en felaktig fil bifogats var att den hade döpts till ett liknande namn som en annan fil som innehöll generella information om fonders utveckling. Det talar för att Indecap inte har haft tillräckligt tydliga instruktioner för att motverka att dokument innehållande kunduppgifter sammanblandas med andra publika dokument.

Det har inte heller framkommit att Indecap implementerat några tekniska eller organisatoriska hinder eller kontrollfunktioner som har försvårat den felaktiga hanteringen av filen, t.ex. tekniska hinder eller varningar i samband med att filen bifogas i e-post. Indecap har visserligen haft en rutin som innebär att varje utskick ska kontrolleras av medpersonal i syfte att förhindra den aktuella typen av misstag. Det har dock framkommit att den aktuella rutinen inte användes till följd av svårigheter att upprätthålla rutinen vid hemarbete under den då rådande Covid-19 pandemin. IMY anser dock att Indecap i det uppkomna läget, särskilt med hänsyn till känsligheten i de uppgifter bolaget behandlar i sin kärnverksamhet, borde ha vidtagit andra åtgärder för att säkerställa en tillräcklig skyddsnivå för de aktuella uppgifterna när den aktuella skyddsåtgärden inte kunnat vidtas till följd av pandemin. Pandemin har således inte

utgjort en skälig ursäkt för att göra avsteg från befintliga säkerhetsrutiner utan att ersätta dessa med något annat likvärdigt skydd.

IMY konstaterar att avsaknaden av åtgärder för att förhindra att de integritetskänsliga uppgifterna om kunderna skickades ut har medfört att risken för att medarbetare skulle göra felaktiga utskick varit hög.

IMY konstaterar vidare att den aktuella filen saknat skydd i form av till exempel läsbegränsningar eller kryptering. Efter att filen felaktigt bifogats i e-postmeddelandet har därför obehöriga obehindrat kunnat ta del av integritetskänslig information om över 50 000 identifierbara individer i klartext. Det har också funnits en risk för att uppgifterna skulle spridas vidare, till exempel genom att någon av de obehöriga mottagarna vidarebefordrade e-postmeddelandet.

Enligt IMY har det förelegat brister avseende skyddet av personuppgifter dels genom att Indecap inte vidtagit tillräckliga tekniska eller organisatoriska åtgärder för att hindra medarbetare från att felaktigt skicka ut kunduppgifter per e-post till obehöriga mottagare, dels genom att uppgifterna inte varit skyddade mot obehörig åtkomst, t.ex. genom kryptering.

Indecaps skyddsåtgärder skulle säkerställa att personuppgifter om bolagets kunder skyddades mot obehörigt röjande och obehörig åtkomst. Indecap har dock genom e-postmeddelandet den 20 januari 2021 som skickades till en stor mängd obehöriga mottagare röjt okrypterade personuppgifter om sina kunder, bland annat uppgifter om kundernas ekonomi.

IMY konstaterar sammanfattningsvis att Indecap inte har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som varit lämplig i förhållande till risken. Indecap har således behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Val av ingripande

Rättslig reglering
IMY har vid överträdelser av dataskyddsförordningen ett antal korrigerande befogenheter, bland annat reprimand, föreläggande och sanktionsavgifter. Det följer av artikel 58.2 a–j i dataskyddsförordningen. IMY ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 i dataskyddsförordningen. I artikel 83.2 anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras och, i så fall, med vilket belopp.

Enligt artikel 83.4 ska det vid överträdelser av bland annat artikel 32 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

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.[2]

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

IMY:s bedömning

Sanktionsavgift ska påföras

IMY har gjort bedömningen att Indecap har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Överträdelsen har skett genom att Indecap behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har medfört att bland annat ekonomiska uppgifter om över 50 000 registrerade skickats via mail till omkring 2 800 obehöriga mottagare. Indecap har varit medveten om riskerna med mailutskick och hade därför infört särskilda kontrollrutiner, men på grund av pandemin, gjort avsteg från kontrollrutinen utan att vidta kompenserande skyddsåtgärder. Det felaktiga utskicket har medfört en hög risk för de registrerades fri- och rättigheter, bland annat avseende förlust av konfidentialitet för skyddsvärda uppgifter.

IMY bedömer mot denna bakgrund att det inte varit fråga om en mindre överträdelse. Indecap ska därför påföras en administrativ sanktionsavgift för överträdelsen. Vid bestämmande av sanktionsavgiftens storlek ska IMY beakta de omständigheter som anges i artikel 83.2 samt säkerställa att den administrativa sanktionsavgiften är effektiv, proportionell och avskräckande.

Moderbolagets årsomsättning ska läggas till grund för beräkningen

Vid bestämmande av maxbeloppet för sanktionsavgiften ska den definition av begreppet företag användas som följer av EU-domstolens praxis enligt artiklarna 101 och 102 i EUF-fördraget (se skäl 150 i dataskyddsförordningen). Av 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.

Vad som utgör ett företag ska således utgå från konkurrensrättens definitioner. Reglerna för koncernansvar i EU:s konkurrenslagstiftning kretsar kring begreppet ekonomisk enhet. Ett moderbolag och ett dotterbolag betraktas som en del av samma ekonomiska enhet när moderbolaget utövar ett avgörande inflytande över dotterbolaget. Det avgörande inflytandet (dvs. kontrollen) kan antingen uppnås genom ägande eller genom avtal. Av EU-domstolens praxis framgår att ett hundraprocentigt eller nästan hundraprocentigt ägande innebär en presumtion för att kontroll ska anses föreligga. Presumtionen kan dock motbevisas om företaget lämnar tillräcklig bevisning för att styrka att dotterbolaget agerar självständigt på marknaden.[3] För att motbevisa presumtionen måste företaget alltså tillhandahålla bevis som rör de organisatoriska, ekonomiska och rättsliga kopplingarna mellan dotterbolaget och dess moderbolag som visar att de inte utgör en ekonomisk enhet trots att moderbolaget innehar 100 procent eller nästan 100 procent av aktierna.[4]

---

[2] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, antagna den 24 maj 2023.
[3] Mål C-97/08, punkt. 59-61
[4] Jfr EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 125 och där redovisade avgöranden.

Den koncern i vilken Indecap ingår består av tre företag, moderbolaget Indecap Holding AB och de två systerföretagen Indecap och Indecap Fonder AB. Indecap Holding AB:s provisionsintäkter består av Indecaps och Indecap Fonder AB:s provisionsintäkter.

Indecap har anfört att den omsättning som är hänförlig till Indecap Fonder AB bör exkluderas vid beräkningen av en sanktionsavgift. Till stöd för detta har Indecap anfört att den nu aktuella överträdelsen endast skett i ett av koncernbolagen, nämligen Indecap. Indecap är ett värdepappersbolag som tillhandahåller individuellt pensionssparande och rådgivning på fondmarknaden. Indecap Fonder AB är i sin tur ett fondbolag som förvaltar nio fonder inom olika aktie- och räntestrategier. Indecap Fonder AB har få direktkunder utan distribuerar fonderna via olika plattformar och banker. Indecap Fonder AB:s fonder är visserligen valbara hos Indecap, men Indecaps fondportföljer består även av många andra fonder som inte har någon koppling till vare sig Indecap Fonder AB eller Indecap Holding AB. De kunduppgifter som ingick i utskicket tillhörde endast kunder i Indecap.

Indecap Holding AB äger 100 procent av aktierna i Indecap och det föreligger därför en presumtion för att Indecap och Indecap Holding AB är en ekonomisk enhet. Indecap har inte lyft fram något som visar att Indecap agerar självständigt i förhållande till moderbolaget som gör att presumtionen bryts. Att dotterbolag i koncernen har verksamheter med olika inriktningar, eller att en incident endast inträffat i ett dotterbolag, är inte sådana omständigheter som i sig får någon påverkan på presumtionen om moderbolagets inflytande.

IMY bedömer med hänsyn till det ovanstående att det företags omsättning som ska läggas till grund för beräkning av den administrativa sanktionsavgift som Indecap kan åläggas är Indecaps moderbolag Indecap Holding AB (556971-6987).

I EDPB:s riktlinjer[5] är utgångspunkten att årsomsättningen avser bolagets nettoomsättning, dvs. det belopp som erhållits genom försäljning av varor och tillhandahållande av tjänster efter avdrag av försäljningsrabatter och mervärdesskatt samt andra skatter som direkt relateras till omsättningen.[6] För att fastställa vilken omsättning Indecap Holding AB hade under föregående räkenskapsår har IMY inhämtat uppgifter ur koncernens årsredovisning för 2022. Av dessa uppgifter framgår att Indecap Holding AB har haft provisionsintäkter uppgående till 558 260 000 kr.

Indecap har anfört att Indecap Holding AB:s årsredovisning är upprättad enligt lagen (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag och att posten för provisionsintäkter inte på ett rättvisande sätt återger koncernens nettoomsättning. De aktuella provisionsintäkterna är därvid angivna innan Pensionsmyndighetens avtalade obligatoriska rabatt på förvaltningsavgifter har dragits av. Avtalet med Pensionsmyndigheten om rabatt är ett krav för att ett fondbolag ska kunna erbjuda fonder på premiepensionens fondtorg. Rabatter till Pensionsmyndigheten uppgick år 2022 till 394 326 770 kr. Indecap Holding AB:s nettoomsättning är således summan

[5] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 128-130.
[6] Definitionen motsvarar den som anges i artikel 5.2 i Europaparlamentets och rådets direktiv 2013/34/EU av den 26 juni 2013 om årsbokslut, koncernredovisning och rapporter i vissa typer av företag, om ändring av Europaparlamentets och rådets direktiv 2006/43/EG och om upphävande av rådets direktiv 78/660/EEG och 83/349/EEG Text av betydelse för EES och som implementerats i svensk rätt genom 1 kap 3 § tredje punkten årsredovisningslagen (1995:1554)

som kvarstår efter att denna rabatt dragits av. Indecap har gett in handlingar till styrkande av de rabatter som lämnats till Pensionsmyndigheten.

IMY gör följande bedömning. Indecap Holding AB:s årsredovisning innehåller ingen tydlig redovisningspost som kan likställas med bolagets nettoomsättning. För att en sanktionsavgift ska få motsvarande effekt oavsett vilka redovisningsregler som den ingripandet riktas mot tillämpar är det enligt IMY dock angeläget att omsättningen beräknas på ett sådant sätt att den motsvarar vad som hade utgjort nettoomsättning om årsredovisningslagens redovisningsregler hade tillämpats. Det saknas vägledande klargöranden från EU-domstolen eller EDPB som tydliggör hur årsomsättningen i kreditinstitut och värdepappersbolag ska beräknas. IMY bedömer därför, mot bakgrund av att nettoomsättning ska fastställas med avdrag av lämnade rabatter, att relevant årsomsättning för Indecap Holding AB ska bedömas med avdrag för rabatter på förvaltningsavgifter. Indecap har genom ingivna handlingar styrkt att rabatterna till Pensionsmyndigheten under år 2022 uppgick till det belopp de angivit.

IMY bedömer med hänsyn till det ovanstående att den relevanta årsomsättningen för Indecap Holding AB är ca 140 199 260 kr. Två procent av den årsomsättningen är ca 2 800 000 kr. Det högsta sanktionsbelopp som kan fastställas i ärendet är därför 10 000 000 EUR.

Överträdelsens allvar
IMY bedömer att följande faktorer har betydelse för bedömningen av överträdelsens allvarlighet.

IMY har konstaterat att Indecap inte vidtagit tillräckliga tekniska och organisatoriska åtgärder för att minska risken för att personuppgifter om bolagets kunder skulle spridas till obehöriga. De aktuella säkerhetsbristerna har lett till en incident som har berört ett stort antal registrerade och en stor mängd obehöriga mottagare har kunnat ta del av andras personuppgifter i klartext. Uppgifterna har omfattat ekonomiska uppgifter och uppgifter om personnummer, dvs. uppgifter som kräver ett starkt skydd. Hanteringen av personuppgifterna var också en del av Indecaps kärnverksamhet där uppgifterna omfattats av lagstadgad tystnadsplikt. Indecap har dessutom varit medveten om riskerna med mailutskick och hade därför infört särskilda kontrollrutiner, men på grund av pandemin, gjort avsteg från kontrollrutinen utan att vidta kompenserande skyddsåtgärder.

IMY beaktar vid bedömningen av överträdelsens allvar, i förmildrande riktning, att Indecap redan innan den aktuella incidenten påbörjat ett arbete med att byta ut mailutskick mot ett säkrare alternativ. Denna process påskyndades också efter den aktuella incidenten.

Av EDPB:s riktlinjer framgår att tillsynsmyndigheten ska bedöma om överträdelsen är av låg, medelhög eller hög allvarlighetsgrad.[7] IMY bedömer mot bakgrund av ovanstående omständigheter att det sammantaget rör sig om en överträdelse av artikel 32.1 i datasskyddsförordningen av medelhög allvarlighetsgrad.

Som förmildrande omständighet beaktas att Indecap, innan IMY inledde tillsyn, omgående och på ett tydligt sätt informerade de registrerade som berörts om vad som inträffat. IMY beaktar också att Indecap kontaktat mottagarna av det felskickade e-

[7] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 60.

postmeddelandet och bett dem att radera meddelandet, samt bekräfta att så skett, som en förmildrande omständighet.

Sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande
Den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande. Det innebär att beloppet ska bestämmas så att den administrativa sanktionsavgiften leder till rättelse, att den ger en preventiv effekt och att den dessutom är proportionerlig i förhållande till såväl aktuella överträdelser som till tillsynsobjektets betalningsförmåga.

IMY bedömer att en sanktionsavgift beräknad på moderbolagets totala nettoomsättning inte, i det nu aktuella fallet, skulle leda till att sanktionsavgiften sätts allt för högt i relation till den överträdelse som konstaterats i ärendet. Det finns därför inte skäl att sätta ner sanktionsavgiften på den grunden att överträdelsen endast avsett ett bolag i koncernen.

Mot bakgrund av överträdelsens allvar, försvårande och förmildrande omständigheter bestämmer IMY den administrativa sanktionsavgiften för Indecap till 500 000 kronor för den konstaterade överträdelsen. IMY bedömer att detta belopp är effektivt, proportionerligt och avskräckande.

Detta beslut har fattats av enhetschefen Catharina Fernquist efter föredragning av juristen Evelin Palmér. Vid den slutliga handläggningen har även rättschefen David Törngren, juristen Cecilia Agnehall och it- och informationssäkerhetsspecialisten Katarina Bengtsson medverkat.

Catharina Fernquist, 2023-11-07 (Det här är en elektronisk signatur)

Kopia till:
1. Klagandena

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till IMY senast tre veckor från den dag ni fick del av beslutet. 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.