

Avanza Bank AB Regeringsgatan 103 111 39 Stockholm

Diarienummer: DI-2021-5544

Datum: 2024-06-24

Beslut efter tillsyn enligt dataskyddsförordningen mot Avanza Bank AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Avanza Bank AB (organisationsnummer 556573-5668) har behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen¹ genom att under tiden från den 15 november 2019 till den 2 juni 2021 vid användning av analysverktyget Meta-pixeln inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter.

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Avanza Bank AB ska betala en administrativ sanktionsavgift på 15 000 000 (femton miljoner) kronor för överträdelserna av artiklarna 5.1 f och 32.1 i dataskyddsförordningen.

Redogörelse för tillsynsärendet

Utgångspunkt för tillsynen

Integritetsskyddsmyndigheten (IMY) mottog den 8 juni 2021 en anmälan om en personuppgiftsincident från Avanza Bank AB (banken). Av anmälan framgick att personuppgifter om 500 001 – 1 miljon under tiden från den 15 november 2019 till och med den 2 juni 2021 felaktigt överförts till bankens samarbetspartner Facebook (numera Meta). Bland uppgifterna som överförts fanns personnummer, lånebelopp och kontonummer.

Bakgrunden till det inträffade var att banken börjat använda Metas tjänst Facebookpixeln (numera Meta-pixeln) i syfte att optimera bankens marknadsföring. Under 2019 utvecklade Meta en ny delfunktion inom Meta-pixeln, kallad Automatic Advanced Matching (AAM). Den felaktiga överföringen av personuppgifter orsakades av att den nya AAM-funktionen aktiverades av banken av misstag. Banken fick kännedom om överföringen via extern information. Så snart banken fick kännedom om det inträffade avaktiverade banken Meta-pixeln i sin helhet.

Postadress:

Box 8114 104 20 Stockholm

Webbplats:

www.imy.se

E-post:

imy@imy.se

Telefon: 08-657 61 00

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).

Datum: 2024-06-24

Mot bakgrund av uppgifterna i anmälan om personuppgiftsincidenten inledde IMY tillsyn mot banken. Tillsynen har avgränsats till att avse i vad mån banken vidtagit lämpliga tekniska och organisatoriska åtgärder för att skydda webbplatsbesökares och appanvändares personuppgifter i enlighet med artiklarna 5.1 f och 32.1 i dataskyddsförordningen under perioden den 15 november 2019 till den 2 juni 2021.

Vad banken har uppgett

Banken har i huvudsak uppgett följande gällande de frågor som är föremål för IMY:s granskning.

Personuppgiftsansvar

Banken är personuppgiftsansvarig för införandet av Meta-pixeln och den efterföljande överföringen av personuppgifter till Meta.

Den ursprungliga implementeringen av Meta-pixeln

Banken har rutiner för att säkerställa korrekt behandling av personuppgifter inför, i samband med och efter införandet av nya funktioner på webbplatsen. Dessa rutiner är formaliserade och finns dokumenterade i bankens styrdokument. Enligt bankens rutiner för att säkerställa korrekt behandling av personuppgifter ska det inledningsvis inför varje ny eller förändrad personuppgiftsbehandling göras en genomgång och bedömning av den planerade behandlingen för att säkerställa att den uppfyller kraven i dataskyddsförordningen. Genomgången görs med hjälp av bland annat en dokumenterad mall för personuppgiftsbehandling vilken innehåller ett flertal steg som den medarbetare som är ansvarig för införandet av en ny eller förändrad personuppgiftsbehandling ska gå igenom. Stegen innebär bland annat att det ska göras en riskanalys av behandlingen, en laglig grund ska kunna fastställas och det ska säkerställas att de registrerade ges korrekt information om den nya personuppgiftsbehandlingen. Vidare ska behandlingen föras in i bankens registerförteckning.

Meta-pixeln är ett analysverktyg som tillhandahålls av Meta och som hjälper till att mäta effektiviteten i bankens Facebook-annonsering. Meta-pixeln överförde och kopplade samman en webbplatsbesökares aktivitet och beteende på bankens webbplats med en unik registrerad användare av någon av Metas tjänster. Syftet med att införa och använda Meta-pixeln var att optimera bankens marknadsföring. Ändamålet med personuppgiftsbehandlingen var att använda riktad annonsering på Facebook och kunna marknadsföra banken till en relevant målgrupp. Meta-pixeln möjliggjorde att mer relevant marknadsföring kunde tas fram genom att marknadsföringen kunde baseras på information om vilka sidor på bankens webbplats som en person besökt.

Innan banken inledde samarbetet med Meta genomfördes en godkännandeprocess där funktioner hos banken inom risk, compliance, legal och informationssäkerhet involverades. Inom ramen för denna process behandlades frågor om banksekretess och personuppgiftsbehandling. Det var enbart uppgifter om en persons besökta webbsidor, IP-adress samt information om vissa unika händelser, t.ex. produktval och sökningar på webbplatsen, som var nödvändiga att behandla för ändamålet ifråga.

Aktivering av nya delfunktioner i Meta-pixeln

Under 2019 utvecklade Meta tjänsten Meta-pixeln genom att även tillhandahålla funktionen Automatic Advanced Matching ("AAM"). Detta är en delfunktion inom Meta-pixeln. Utöver AAM erbjuder Meta-pixeln även funktionen Automatiska Händelser ("AH") vilken kan aktiveras manuellt och som då på egen hand försöker att detektera och fånga upp händelser och interaktioner, såsom klick, sökningar och menyval, vid besök på bolagets webbplats eller i appen.

Under 2019 fick bankens legalavdelning en förfrågan från marknadsavdelningen om möjligheten att få använda en av Metas funktioner genom vilken kunddata skulle överföras till Meta. Bankens legalavdelning fann att den aktuella funktionen inte kunde implementeras. Det är vidare bankens uppfattning att om en implementering av en funktion så som AAM skulle ha blivit föremål för interna processer och rutiner hade det lett till bedömningen att banken inte hade kunnat acceptera villkoren och att det inte skulle vara möjligt att använda sig av funktionen. Detta eftersom funktionen riskerar innebära en överföring av data till Meta som banken inte lagligen kan utföra i sin bankverksamhet.

Det har aldrig varit bankens avsikt att använda sig av funktionerna AAM och AH. Banken har inte kunnat verifiera hur funktionerna aktiverats. Skulle funktionen ha aktiverats av någon anställd hos banken är bankens uppfattning att det skett av misstag. Banken har inte tagit något beslut om att aktivera funktionen AAM.

Bankens överföring av personuppgifter via funktionen AAM till Meta

Funktionen Automatic Advanced Matching (AAM)

Funktionen AAM överförde uppgifter i hashad form (med hashningsfunktionen SHA256) ² till Meta om användaren fyllde i något av de fem olika formulären på bankens webbplats eller i bankens mobilapp. Två formulär låg i nykundsflödet (öppet för besökare, där besökaren hade för avsikt att bli kund). Tre formulär avsåg bolån och låg bakom inloggning och kunde endast överföra uppgifter från befintliga kunder som ingått kundavtal med banken. För att uppgifterna skulle kunna överföras krävdes således att en person var inloggad på bankens webbplats och att personen tackat ja till marknadsföringscookies hos banken. Om dessa förutsättningar inte var uppfyllda aktiverades inte AAM och inga uppgifter överfördes. Om förutsättningarna var uppfyllda kunde följande hashade uppgifter överföras till Meta:

- Personnummer
- Kontaktuppgifter, såsom telefonnummer, e-postadress, postnummer samt postort
- Lånebelopp på befintligt lån
- Arbetsgivare
- Anställningsform
- Kontonummer

² IMY:s tillägg: Hashning är en kryptografisk envägsfunktion som kan användas för att åstadkomma pseudonymisering, som är en möjlig säkerhetsåtgärd enligt artikel 32 i dataskyddsförordningen, genom att personuppgifter ersätts med en så kallad hashsumma. Det innebär att de ersatta personuppgifterna inte är tillgängliga i klartext och att det behövs kompletterande uppgifter för att det ska gå att identifiera den registrerade.

Datum: 2024-06-24

Genom att funktionen AAM oavsiktligt aktiverats av banken kunde Meta-pixeln matcha de hashade uppgifterna med besökarnas beteende på webbplatsen för profilering. Detta gjorde det möjligt att få en mer detaljerad bild av besökarna. Profileringen gällde endast bankens marknadsföring och användes inte av Meta för egna, eller andra aktörers, affärsmässiga syften.

Exakt hur AAM har påverkat annonseringen är inte fastställt. Att detta resulterat i riktad reklam kan inte uteslutas.

Funktionen Automatiska Händelser (AH)

Funktionen AH överförde uppgifter i klartext till Meta när en användare navigerade på bankens webbplats eller i mobilappen. En förutsättning för överföring var att användaren tackat ja till marknadsföringscookies hos banken samt var inloggad som kund hos banken (med ett undantag, se nedan).

Den data som överfördes i klartext till Meta överfördes omedvetet då det inte fanns någon avsikt att visa informationen för någon annan än kunden. Det var från webbläsare eller app på kundens enhet som överföringen skedde och det på grund av tre huvudfaktorer:

- 1) Den funktion som oavsiktligt aktiverats av banken hos Meta följer även hur en användare rör sig på en sajt/i mobilen (konverterar). För att göra det skickas information om vilka "knappar" det vill säga element på sidan/skärmen användaren trycker på då denne navigerar på sajten/i appen. Meta samlar följaktligen in information som berättar om vilka knapptryck som sker för att förstå vilken kontext användaren konverterar i. Till exempel vill Meta förstå att kunden köper något vid tryck på en knapp med texten "Köp" även om annonsören inte har taggat upp köpknappen som en konvertering. Denna information skickades till Meta.
- 2) Banken använder element som Meta uppfattar som knappar, t.ex. knappmarkerade rutor och rullgardinsmenyer, i sin kod för att presentera viss information till bankens användare. Det gäller främst när det finns element på sajten/apparna som går att trycka på för att t.ex. visa mer information. Ofta visas dessa som ett mindre visuellt element som blir större när man trycker på dem, och då visar mer information. När användare har tryckt på dessa element för att se mer information har det registrerats som vanliga knapptryck av Metas script (Meta-pixeln IMY:s anmärkning). Scriptet har då sammanställt informationen och skickat den till Meta som ett registrerat knapptryck.
- 3) Information om knapptryck pseudonymiseras (hashas IMY:s anmärkning) inte av Meta på det sätt som annan information som de samlar in.

Dessa tre faktorer har tillsammans gjort att viss information skickades till Meta i klartext. Det var således en kombination av den (felaktigt) aktiverade funktionaliteten tillsammans med Metas hantering av knapptryck och en specifik teknisk lösning från banken som orsakade överföringen till Meta.

Sammanfattningsvis analyserade AH vilka knappar på webbplatsen och mobilappen som användaren tryckte på för att sedan ge förslag om marknadsföring på Facebook. Bankens överföring av uppgifter via AH uppstod eftersom banken kategoriserade visuella fält som knappar på webbplatsen och i mobilappens kod. Via AH kunde följande kategorier av uppgifter överföras till Meta i klartext:

- Värdepappersinnehav och värde, såsom tillgängligt belopp för köp, uttag och värdeutveckling
- Information om lånebelopp
- Kontonummer och kreditlimit
- Avgifter, skatter och aktuella räntor
- Pågående ordrar och dagens avslut
- Firmatecknare och bank som pension flyttas från
- E-postadress och personnummer

Majoriteten av de uppgifter som överfördes via AH kom från knappar bakom inloggat läge hos banken, det vill säga knappar som endast visades för kunder som ingått kundavtal med banken. På ett ställe på bankens webbplats fanns dock expanderbara paneler i flödet för teckning av tjänstepension, både för enskild firma och för aktiebolag, som låg öppet för alla besökare, det vill säga även uppgifter från ett begränsat antal besökare utan kundavtal med banken och som därmed inte var inloggade.

Åtgärder som vidtagits efter personuppgiftsincidenten

Meta har bekräftat till banken att de personuppgifter som behandlats har raderats hos Meta på ett sätt som inte gör det möjligt för Meta att återskapa dem.

Bankens uppfattning är att överföringen av uppgifterna inte inneburit någon skada eller risk för de registrerade eftersom Meta inte använt uppgifterna för eget ändamål eller överfört dem vidare samt att uppgifterna är raderade. All information har överförts av Meta-pixeln till Meta och bankens eget annonskonto hos Meta.

I syfte att upptäcka utgående trafik har banken numera upprättat en process för hur banken inför och hanterar tredjepartsscript. I den beskrivs hur dessa script ska utvärderas ur ett säkerhets- och integritetsperspektiv samt hur de underhålls långsiktigt.

Banken har vidare flyttat scripten från tredjepartsleverantörerna till bankens egna system för att undvika att förändringar i scripten införs utan att banken uppmärksammar det.

Banken har även kompletterat interna riktlinjer för att tydligare beskriva felscenariot, hur det undviks och vilka förväntningar som åligger bankens utvecklingsteam när de hanterar den här typen av produkter.

Utöver detta har banken implementerat ytterligare styrdokument och rutiner som syftar till att säkerställa en korrekt behandling av personuppgifter. Dessa styrdokument innehåller bland annat krav och riktlinjer i relation till behandling av personuppgifter inför, i samband med och efter införandet av nya funktioner på bankens webbplats.

Motivering av beslutet

Tillämpliga bestämmelser m.m.

Av artikel 95 i dataskyddsförordningen följer att dataskyddsförordningen inte ska innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter, för sådana områden som redan omfattas av skyldigheter

enligt det så kallade eDataskyddsdirektivet³. eDataskyddsdirektivet har genomförts i svensk rätt genom lagen (2003:389) om elektronisk kommunikation (LEK), där bland annat insamling av uppgifter genom webbkakor regleras.

Enligt 9 kap. 28 § LEK, som genomför artikel 5.3 i eDataskyddsdirektivet, får uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Vidare framgår att detta inte hindrar sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt. LEK trädde i kraft den 22 augusti 2022. Under den i ärendet aktuella tiden gällde dock samma krav enligt 6 kap. 18 § lagen om (2003:389) om elektronisk kommunikation. Det är Post- och telestyrelsen som är tillsynsmyndighet enligt LEK (1 kap 5 § förordningen (2022:511) om elektronisk kommunikation).

Europeiska dataskyddsstyrelsen (EDPB) har yttrat sig över samspelet mellan eDataskyddsdirektivet och dataskyddsförordningen. Av yttrandet följer bl.a. att den nationella tillsynsmyndighet som utsetts enligt eDataskyddsdirektivet är ensamt behörig att övervaka efterlevnaden av direktivet. Däremot är tillsynsmyndigheten enligt dataskyddsförordningen behörig tillsynsmyndighet för den behandling som inte regleras särskilt i eDataskyddsdirektivet.⁴

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 (principen om ansvarsskyldighet).

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.

³ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

⁴ Yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter, antaget den 12 mars 2019, punkt 68 och 69.

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.

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.

Av 1 kap. 10 § första stycket lagen (2004:297) om bank- och finansieringsrörelse (banklagen) framgår att enskildas förhållanden till kreditinstitut inte obehörigen får röjas.

Integritetsskyddsmyndighetens bedömning

Av utredningen i ärendet framgår att två funktioner i analysverktyget Meta-pixeln oavsiktligt aktiverats av banken. Som en följd av att funktionerna aktiverats har personuppgifter om ett stort antal personer som varit inloggade på bankens webbplats eller i bankens app obehörigen överförts till Meta. I några fall har även personuppgifter avseende personer som besökt webbplatsen eller appen och använt en specifik tjänst utan att ha varit inloggade överförts. Det är i huvudsak bankens egna kunder som har berörts av överföringen. De personuppgifter som överförts har bland annat innefattat personnummer och omfattande ekonomisk information. Informationen, däribland detaljerade uppgifter om kunders ekonomi, har i flera fall överförts i klartext.

Enligt banken har det inte varit möjligt att i efterhand verifiera hur funktionerna aktiverats eller av vem.

IMY tar inledningsvis ställning till om dataskyddsförordningen är tillämplig och om IMY är behörig tillsynsmyndighet.

IMY är behörig tillsynsmyndighet

IMY:s granskning tar sikte på en situation då uppgifter om personer, i huvudsak kunder som varit inloggade hos banken, oavsiktligt överförts av Meta-pixeln till Meta i samband med att de besökt olika delar av bankens webbplats. Denna informationshantering innebär inte att uppgifter lagrats i eller hämtats från en abonnents eller användares terminalutrustning och omfattas därmed inte av 9 kap. 28 § i LEK eller tidigare gällande motsvarande bestämmelse i lagen (2003:389) om elektronisk kommunikation. IMY konstaterar därmed att dataskyddsförordningen är

Datum: 2024-06-24

tillämplig på den aktuella personuppgiftsbehandlingen och att IMY är behörig tillsynsmyndighet. Det kan vidare konstateras att IMY:s granskning avser om banken vidtagit tillräckliga säkerhetsåtgärder, vilket inte är något som regleras särskilt i LEK. Även det förhållandet medför således att IMY är behörig tillsynsmyndighet.

IMY bedömer härefter frågan om personuppgiftsansvar och om banken har vidtagit lämpliga säkerhetsåtgärder enligt artiklarna 5.1 f och 32 i dataskyddsförordningen för att skydda berörda webbplatsbesökares och appanvändares personuppgifter.

Banken är personuppgiftsansvarig

Banken har uppgett att banken är personuppgiftsansvarig för den personuppgiftsbehandling som granskats i ärendet. Av utredningen framgår att syftet med att implementera och använda Meta-pixeln varit att optimera bankens marknadsföring. Genom att behandla uppgifter om t.ex. en persons besökta webbsidor, sökningar och produktval har bankens marknadsföring på Metas tjänst Facebook således kunnat optimeras.

IMY konstaterar att banken har bestämt ändamål och medel för behandlingen av personuppgifterna, det vill säga hur och varför personuppgifterna ska behandlas. IMY bedömer att det är banken som enligt artikel 4.7 i dataskyddsförordningen är personuppgiftsansvarig för den personuppgiftsbehandling som tillsynen omfattar.

Behandlingen har inneburit en hög risk och krävt en hög skyddsnivå

Banken har enligt artikel 32 i dataskyddsförordningen en skyldighet att skydda de personuppgifter som banken 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. 10 § första stycket banklagen följer att den som är eller har varit knuten till en bank inte obehörigen får röja uppgifter som rör en bankkunds mellanhavanden med banken. Även uppgiften att en viss person är kund i banken eller inte, omfattas av tystnadsplikten. Dessa lagkrav om tystnadsplikt gäller således i bankens verksamhet. Det ställer höga krav på skydd för de personuppgifter som behandlas i bankens verksamhet.

IMY konstaterar att 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 uppgift om kontonummer, värdepappersinnehav, lånebelopp, och kreditlimit, för vilka de registrerade har berättigade förväntningar på en hög grad av konfidentialitet och ett robust skydd mot obehörig åtkomst. De uppgifter som överförts har omfattats av lagstadgad tystnadsplikt. Personuppgiftsbehandlingen har skett inom ramen för bankens kärnverksamhet, något som medför ännu högre krav på skyddsnivån. Banken borde ha haft god förmåga att säkerställa en säkerhet som varit lämplig utifrån behandlingens omfattning och känslighet.

Med hänsyn bland annat till att de uppgifter som banken behandlat har varit av skyddsvärd karaktär och berört ett mycket stort antal personer har bankens behandling av personuppgifterna sammantaget inneburit en hög risk för fysiska personers

Datum: 2024-06-24

rättigheter och friheter. Behandlingens art, omfattning och sammanhang har därmed medfört ett krav på en hög skyddsnivå för uppgifterna. Åtgärderna skulle bland annat säkerställa att personuppgifterna skyddades mot obehörigt röjande och obehörig åtkomst.

Banken har inte vidtagit tillräckliga åtgärder för att skydda uppgifterna

IMY konstaterar inledningsvis att det förhållandet att banken överfört de aktuella uppgifterna till Meta innebär att uppgifterna rent faktiskt inte har skyddats mot obehörigt röjande.

Av bankens uppgifter framgår att den har formaliserade rutiner för att säkerställa en korrekt behandling av personuppgifter inför, i samband med och efter införandet av nya funktioner på webbplatsen och att dessa rutiner finns dokumenterade i bankens styrdokument.

IMY konstaterar att banken således haft organisatoriska åtgärder på plats i form av rutiner som dokumenterats i bankens styrdokument. Banken har dock i det aktuella fallet inte följt sina rutiner. Banken har haft Meta-pixeln införd på delar av bankens webbplats och app som varit avsedda endast för inloggade kunder och potentiella kunder. De två funktionerna AAM och AH i Meta-pixeln har därefter aktiverats utan att banken varit medveten om det. Som en konsekvens av att banken vid införandet av dessa funktioner inte följt sina rutiner och dokumenterat vad som skett har det inte varit möjligt för banken att i efterhand verifiera hur eller av vem dessa funktioner aktiverades.

Som en följd av att de två funktionerna AAM och AH aktiverats utan bankens vetskap har ett obehörigt röjande av uppgifter som omfattas av tystnadsplikt och en obehörig överföring av personuppgifter skett till Meta. Detta pågick i drygt ett och ett halvt år. Att röjandet och den obehöriga överföringen upphörde berodde inte på att banken själv uppmärksammande vad som pågick, utan på att banken via en extern källa fick kännedom om det.

Banken har således saknat förmåga att upptäcka röjandet av och den pågående överföringen av personuppgifter till Meta. IMY anser att banken borde ha haft ett sådant systematiskt säkerhetsarbete att detta skulle ha upptäckts av banken. Ett sådant säkerhetsarbete innefattar att kontroller görs med viss regelbundenhet. Eftersom banken endast har haft rutiner för att följa upp dokumenterade förändringar som utförts enligt uppsatta rutiner, har banken saknat förmåga att upptäcka och åtgärda förändringar som, liksom i det aktuella fallet, genomförts utan att rutinerna följts. Mot denna bakgrund konstaterar IMY att banken har saknat tekniska och organisatoriska säkerhetsrutiner för att systematiskt följa upp och upptäcka oavsiktliga förändringar i sina system.

Som en följd av att banken dels inte tillämpat sina organisatoriska säkerhetsrutiner när banken införde funktionerna AAM och AH, dels saknat organisatoriska och tekniska säkerhetsrutiner för att upptäcka överföringar har personuppgifter om ett stort antal personer obehörigen förts över till Meta. Utredningen visar att det har varit fråga om personuppgifter om cirka $500\ 000\ - 1\ 000\ 000$ personer.

IMY konstaterar sammanfattningsvis att banken vid användningen av Meta-pixeln inte har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som varit lämplig i förhållande till risken. Detta innebär att banken under

Datum: 2024-06-24

tiden från den 15 november 2019 till den 2 juni 2021 har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Enligt den grundläggande säkerhetsprincipen i 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. Genom det inträffade har uppgifter om bankens kunder, till exempel uppgifter om personnummer, kontonummer, värdepappersinnehav, lånebelopp och kreditlimit, förts över till Meta i klartext. Därutöver har vissa uppgifter förts över i hashad form vilket möjliggjort matchning med personuppgifter hos Meta. Det har varit fråga om uppgifter som omfattas av lagstadgad tystnadsplikt. Förlust av kontroll av bankinformation kan innebära en hög risk för de registrerades fri- och rättigheter. Att ärendet gäller bankinformation och att personuppgifterna dessutom till övervägande del har röjts och överförts i klartext från ett för kunderna inloggat läge medför enligt IMY att det inträffade är särskilt allvarligt. Bankens underlåtenhet att följa sina formaliserade rutiner och avsaknad av förmåga att upptäcka den obehöriga överföringen av personuppgifter bedöms därför vara av så allvarligt slag att bristen även innebär en överträdelse av artikel 5.1 f 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 vad som kan påverka sanktionsavgiftens storlek. Av betydelse för bedömningen av överträdelsen allvar är bland annat dess karaktär, svårighetsgrad och varaktighet.

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 två procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Enligt artikel 83.5 ska det vid överträdelser av bland annat artikel 5 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till fyra procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Datum: 2024-06-24

EDPB har antagit riktlinjer om beräkning av administrativa sanktionsavgifter enligt dataskyddsförordningen som syftar till att skapa en harmoniserad metod och principer för beräkning av sanktionsavgifter.⁵

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 banken har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen samt att överträdelsen är av sådant allvarligt slag att det också är fråga om en överträdelse av principerna om integritet och konfidentialitet i artikel 5.1 f.

Överträdelsen har skett genom att banken behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har medfört att bland annat ekonomiska uppgifter om cirka 500 000 - 1 000 000 personer obehörigen överförts till Meta under drygt ett och ett halvt års tid. Banken har vidare saknat förmåga att under denna tid upptäcka överföringen av personuppgifter till Meta. IMY anser att banken borde ha haft ett sådant systematiskt säkerhetsarbete att överföringen av personuppgifter skulle ha upptäckts i samband med en regelbunden kontroll. Den obehöriga överföringen har medfört en hög risk för de registrerades fri- och rättigheter, bland annat avseende förlust av konfidentialitet för skyddsvärda uppgifter. Mot denna bakgrund bedömer IMY att det inte är fråga om sådana mindre överträdelser som avses i skäl 148 i dataskyddsförordningen.

EU-domstolen har klargjort att det krävs att den personuppgiftsansvarige har begått en överträdelse uppsåtligen eller av oaktsamhet för att administrativa sanktionsavgifter ska kunna påföras enligt dataskyddsförordningen. EU-domstolen har uttalat att personuppgiftsansvariga kan påföras sanktionsavgifter för ageranden om de inte kan anses ha varit okunniga om att agerandet utgjorde en överträdelse, oavsett om de varit medvetna om att de åsidosatte bestämmelserna i dataskyddsförordningen.⁶

Enligt principen om ansvarsskyldighet som bland annat kommer till uttryck i artikel 5.2 i dataskyddsförordningen ska den som ansvarar för behandlingen av personuppgifter säkerställa och kunna visa att behandlingen är förenlig med dataskyddsförordningen. IMY konstaterar således att banken ansvarar för att de personuppgifter som behandlas i verksamheten, behandlas på ett sätt som säkerställer en lämplig säkerhetsnivå. IMY har vid sin prövning konstaterat att banken inte levt upp till de krav som dataskyddsförordningen ställer i detta avseende. Banken kan inte anses ha varit okunnig om att dess agerande inneburit en överträdelse av förordningen. Det

⁵ EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, antagna den 24 maj 2023.

⁶ EU-domstolens dom i mål C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos mot Valstybinė duomenų apsaugos inspekcija av den 5 december 2023, punkt 81 och dom i mål C 807/21 Deutsche Wohnen av den 5 december 2023, punkt 76

Datum: 2024-06-24

föreligger därmed förutsättningar för att påföra banken en administrativ sanktionsavgift.⁷

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.

IMY konstaterar att överträdelser av artikel 5.1 f i dataskyddsförordningen omfattas av artikel 83.5 vilket innebär att en sanktionsavgift på upp till tjugo miljoner euro eller fyra procent av den globala årsomsättningen under föregående budgetår, beroende på vilket som är högst, kan påföras.

Avanza-koncernens årsomsättning enligt moderbolagets koncernredovisning ska läggas till grund för beräkningen

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 EUF-fördraget (se skäl 150 i dataskyddsförordningen). Av domstolens praxis framgår att detta 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.

Bedömningen av 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 (det vill säga kontrollen) kan antingen uppnås genom ägande eller genom avtal. Av rättspraxis 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.⁸ 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.⁹

Avanza Bank AB är ett helägt dotterbolag till moderbolaget Avanza Bank Holding AB (publ). Enligt den ovan beskrivna presumtionen är det därför omsättningen för Avanzakoncernen enligt Avanza Bank Holding AB:s (publ) koncernredovisning som ska läggas till grund för beräkning av det maximala sanktionsavgiftsbeloppet.

Av Avanza Bank Holding AB:s koncernredovisning för 2023 framgår att den totala globala årsomsättningen var ca 4 716 000 000 kr. Fyra procent av den årsomsättningen är ca 189 000 000 kr. Då detta belopp understiger det maxbelopp som framgår av artikel 83.5 är det högsta sanktionsbelopp som kan fastställas i ärendet 20 000 000 euro.

 ⁷ Se för bedömningen av oaktsamhet även Kammarrätten i Stockholms dom den 11 mars 2024 i mål 2829-23 s.12.
⁸ EU-domstolens dom i mål C-97/08 P Akzo Nobel NV m.fl. mot EU-kommissionen den 10 september 2009, punkt 59-61 Anpassa/ensa fotnoter där vi hänvisar till EU-domstolens avgöranden.

⁹ Jfr. EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 125 och där redovisade avgöranden.

Datum: 2024-06-24

Överträdelsens allvar

Av EDPB:s riktlinjer framgår att tillsynsmyndigheten ska bedöma om överträdelsen är av låg, medelhög eller hög allvarlighetsgrad.¹⁰

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

IMY har konstaterat att banken inte följt sina rutiner i samband med att funktionerna AAM och AH i Meta-pixeln aktiverades och att banken har saknat det systematiska säkerhetsarbete som krävts för att upptäcka det obehöriga röjandet och överföringen av personuppgifter till Meta. De aktuella säkerhetsbristerna har lett till en incident som har berört ett stort antal registrerade och Meta har kunnat ta del av en stor mängd personuppgifter, i många fall i klartext, som inte skulle ha överförts till Meta. Uppgifterna har omfattat ekonomiska uppgifter och uppgifter om personnummer, dvs. uppgifter som kräver en hög skyddsnivå. Överträdelsen har pågått under en längre tid, från den 15 november 2019 till och med den 2 juni 2021 då banken blev uppmärksammad på den obehöriga överföringen av uppgifterna. Behandlingen av personuppgifterna på bankens webbplats är en del av bankens kärnverksamhet där uppgifterna omfattats av lagstadgad tystnadsplikt, vilket gör att överträdelsen ska betraktas som mer allvarlig än om så inte varit fallet.¹¹

IMY har konstaterat att överträdelsen är så allvarlig att den utöver en överträdelse av artikel 32.1 i dataskyddsförordningen även utgör en överträdelse av den grundläggande principen om integritet och konfidentialitet enligt artikel 5.1 f. IMY bedömer sammantaget, att den aktuella överträdelsen har en låg allvarlighetsgrad inom spannet för överträdelser av artikel 5.1 f.

IMY ska vid sin bedömning av sanktionsavgiftens storlek även ta hänsyn till sådana försvårande och förmildrande faktorer som förtecknas i artikel 83.2 i dataskyddsförordningen. IMY konstaterar att banken vidtagit vissa åtgärder för att lindra den skada som de registrerade lidit enligt artikel 83.2 c. Banken stängde omedelbart av pixelfunktionerna när banken medvetandegjordes om överföringen. Banken tog även kontakt med Meta för att försäkra sig om att Meta inte behandlat uppgifterna för egna syften och att uppgifterna raderats hos Meta. Utöver detta har banken implementerat ytterligare styrdokument och rutiner som syftar till att säkerställa en korrekt behandling av personuppgifter. IMY bedömer att banken genom dessa åtgärder gjort vad som kunde förväntas med tanke på behandlingens karaktär, ändamål och omfattning. De vidtagna åtgärderna utgör därför inte en förmildrande faktor. IMY konstaterar att det inte heller i övrigt framkommit några omständigheter som påverkar IMY:s bedömning av sanktionsavgiftens storlek varken i försvårande eller förmildrande riktning

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.

¹⁰ EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 60.

¹¹ EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 53.

Datum: 2024-06-24

Mot bakgrund av överträdelsens allvar bestämmer IMY att banken ska betala en administrativ sanktionsavgift på 15 000 000 kr för de konstaterade överträdelserna. IMY bedömer att detta belopp är effektivt, proportionerligt och avskräckande.

Detta beslut har fattats av vikarierande generaldirektören David Törngren efter föredragning av seniora juristen Hans Kärnlöf. Vid den slutliga handläggningen har även tillförordnade rättschefen Cecilia Agnehall och enhetschefen Catharina Fernquist samt it- och informationssäkerhetsspecialisten Petter Flink medverkat.

David Törngren, 2024-06-24 (Det här är en elektronisk signatur)

Kopia till

DSO

Datum: 2024-06-24

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 Integritetsskyddsmyndigheten senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.