Göteborgs Stad

Tjänsteutlåtande
Utfärdat: 2024-08-13
Diarienummer 0013/24

Handläggare:
Petra Willquist
Telefon: 031-368 55 14
E-post: petra.willquist@gotalejon.goteborg.se

Rapport regelefterlevnadsfunktion kvartal 2 2024

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar rapport från regelefterlevnadsfunktionen kvartal 2 2024.

Sammanfattning

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan. Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för bolagets tillståndspliktiga verksamhet.

Bedömning ur ekonomisk dimension

Kontrollfunktionens granskar bolagets följsamhet mot krav som gäller för bolagets tillståndspliktiga verksamhet. Ur ekonomiskt perspektiv är det viktigt då det är en del av att säkerställa bolagets långsiktiga ekonomiska hållbarhet.

Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Brister i följsamhet mot bestämmelser, regelverk och riskaptit kan leda till ökad risk för minskat förtroende för bolagets verksamhet.

Samverkan

Ingen samverkan har genomförts.

Bilagor

1. Rapport regelefterlevnadsfunktionen kvartal 2 2024

Ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 2 2024.

För att ta del av rapporten hänvisas till bilaga 1.

Beskrivning av ärendet

Enligt Försäkringsrörelselagen 10 kap, 4 § ska försäkringsföretag ha fyra centrala funktioner. Dessa utgörs av regelefterlevnadsfunktionen, riskhanteringsfunktionen, aktuariefunktionen och internrevisionsfunktionen. Dessa kontrollfunktioner ska utvärdera systemet för internrevision, regelefterlevnad och riskhantering. Funktionerna ska även utvärdera andra delar av företagsstyrningssystemet och rapportera resultatet och lämna rekommendationer efter utvärdering till företagets styrelse.

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan. Under andra kvartalet har kontroller utförts avseende outsourcing, anpassning till nya eller förändrade regelverk samt övrig regelefterlevnad.

Under kvartal 2 2024 har regelefterlevnadsfunktionen utförda kontroller inte föranlett någon anmärkning för bolaget. Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för bolagets tillståndspliktiga verksamhet.

Göta Lejon arbetar löpande med att åtgärda utfärdade rekommendationer. Rekommendationerna uppdateras i bolagets styrnings- och ledningssystem Stratsys minst två gånger per år.

Bolagets bedömning

Det är bolagets bedömning att rapporten är relevant för bolagets arbete. Göta Lejon arbetar löpande med uppföljning av rekommendationer.

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 april - 30 juni 2024 avseende regelefterlevnad

1 Inledning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av Försäkrings AB Göta Lejons, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen för regelefterlevnad har vidtagit under det andra kvartalet 2024.

För en överblick över utfallet av kvartalets utförda kontroller, se bilaga 1.

2 Händelser av relevans under perioden

2.1 Regelbevakning

Följande nyhetsbrev har tillställts Bolaget under årets andra kvartal. Dessa finns återgivna i sin helhet i bilaga 2.

- Uppdatering kring DORA (endast skickat som e-postmeddelande).
- Finansinspektionens Konsumentskyddsrapport för år 2024.
- Anmärkning och sanktionsavgift mot Nasdaq Stockholm Aktiebolag.
- Sanktionsbeslut mot Avanza Bank AB.

2.2 Kontroll av Bolagets regelefterlevnad

Avgränsning och metod

Andra kvartalets kontroll har till övervägande del bestått i att följa upp Bolagets anpassning till

den kommande DORA-förordningen, vilket innefattar flera av kontrollområdena nedan, med undantag för anpassningen till nya hållbarhetsregler samt revideringar i Solvens II-direktivet. Bolaget har tillsammans med funktionen för regelefterlevnad planerat för implementeringsarbetet avseende DORA i enlighet med den GAP-analys som Bolaget mottagit från extern leverantör. Anpassningen till nya hållbarhetsregler samt revideringar i Solvens II-direktivet har endast diskuterats med Bolaget, inga särskilda stickprov har utförts.

Outsourcing

Granskning av Bolagets uppdragsavtal samt Bolagets uppföljning av uppdragstagare i syfte att säkerställa att Bolaget uppfyller kraven på innehåll i sådana avtal enligt dels försäkringsrörelselagen (2010:2043) (FRL), dels Finansinspektionens föreskrifter och allmänna råd om försäkringsrörelse (FFFS 2015:8), dels Kommissionens delegerade förordning 2015/35 om upptagande och utövande av försäkringsverksamhet, dels EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer. Kontrollen har vidare syftat till att säkerställa att Bolaget har en fullgod uppföljning av Bolagets uppdragstagare.

Utöver ovan har även kontrollen syftat till att följa upp vilka förändringar som eventuellt behöver göras i Bolagets riktlinjer och uppdragsavtal med anledning av DORA-förordningen.

Funktionen för regelefterlevnad har inte haft några synpunkter på nuvarande utformning av avtal eller uppföljningsprocess av uppdragstagare. Funktionen har emellertid sett att vissa justeringsbehov finns för att dessa dokument och processer ska överensstämma med DORA-förordningen och kommer att hanteras mot bakgrund av den GAP-analys Bolaget mottagit under hösten.

Anpassning till nya eller förändrade regelverk

Uppföljning och kontroll av Bolagets anpassning till dels DORA-förordningen, dels nya regler om hållbarhetsredovisning, dels omarbetningen av Solvens II. Kontrollen har syftat till att säkerställa att Bolaget har anpassat rutiner och processer efter de nya regelverken.

Beträffande anpassningen till DORA-förordningen så pågår detta arbete i enlighet med ovan. Beträffande anpassningen till de nya reglerna om hållbarhetsredovisning samt omarbetningen av Solvens II-direktivet så består dessa förändringar i nuläget i förändrade regler kring hållbarhet. Bolaget träffas inte direkt av de nämnda hållbarhetsreglerna men kommer att

behöva leverera information och data till Staden som omfattas av reglerna om hållbarhetsredovisning.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen, men kommer fortsatt att följa och bistå i implementeringsarbetet av DORA-förordningen.

Övrig regelefterlevnad

Uppföljning och kontroll av Bolaget riktlinjer för avbrottsfri verksamhet. Kontrollen har syftat till att säkerställa att riktlinjerna följer relevanta regler.

Funktionen har tagit del av och granskat Bolagets riktlinjer för avbrottsfri verksamhet. Funktionen för regelefterlevnad har inte haft några synpunkter på nuvarande utformning av riktlinjerna, men har emellertid sett att vissa justeringsbehov finns för att detta dokument ska överensstämma med DORA-förordningen.

2.3 Råd och stöd

Funktionen för regelefterlevnad har under perioden funnits tillgänglig för att svara på frågor och lämna råd och stöd till Bolagets anställda.

3 Funktionen för regelefterlevnads bedömning

Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att Bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för Bolagets tillståndspliktiga verksamhet.

Stockholm den 5 juli 2024

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 1, 2024

	Område	*Kontroll*	*Anmärkning*
	Outsourcing	Uppdragsavtal	Ingen anmärkning.
		Uppdragstagare.	Ingen anmärkning.
	Anpassning till nya eller förändrade regelverk	Europaparlamentets och Rådets förordning om digital operativ motståndskraft för finanssektorn (DORA).	Ingen anmärkning.
		SOU 2023:35 - Nya regler om hållbarhetsredovisning	Ingen anmärkning.
		Omarbetning av Solvens II-direktivet.	Ingen anmärkning.
	Övrig regelefterlevnad	Avbrottsfri verksamhet.	Ingen anmärkning.

*Denna matris syftar till att ge Bolaget en överblick över resultatet av utförd kontroll av Bolagets regelefterlevnad samt återge vilka åtgärder som Bolaget rekommenderas att vidta eller som är under arbete. Denna färgskala är inte kopplad till den riskmatris som har tillsänts Bolaget som bilaga till årsplanen.

2 Översikt regelefterlevnad från föregående kontroller

	Kvartal	*Område*	*Kontroll*	*Anmärkning*

*Denna matris syftar till att ge Bolaget en överblick över föregående kontroller där funktionen för regelefterlevnad har haft anmärkningar eller synpunkter som inte är hanterade eller som är under arbete och som funktionen för regelefterlevnad avser att följa upp.

3 Färggradering

	Utförd kontroll har inte föranlett någon anmärkning.
	Utförd kontroll har föranlett mindre anmärkning eller synpunkt. Åtgärd rekommenderas eller är under arbete.
	Sannolikhet för att regelavvikelse inträffar. Åtgärd behöver vidtas inom kort.
	Regelavvikelse har uppmärksammats vid utförd kontroll. Åtgärd behöver vidtas snarast.

Bilaga 2

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Finansinspektionens Konsumentskyddsrapport för år 2024

---

23 maj 2024

1 Bakgrund

Finansinspektionen har nyligen publicerat sin årliga Konsumentskyddsrapport för år 2024. Årets rapport fokuserar särskilt på finansiellt utanförskap, olämpliga spar- och investeringsprodukter, osund kreditgivning samt de ökade antalet bedrägerier som drabbar konsumenter inom det finansiella området. Nedan följer en sammanfattning av relevanta delar ur rapporten.

2 Finansiell rådgivning

En av de mest framträdande frågorna i rapporten är de höga provisioner som rådgivare erhåller när de säljer dyra och ofta olämpliga finansiella produkter till konsumenter. Dessa provisioner skapar allvarliga intressekonflikter, där rådgivare kan prioritera sina egna ekonomiska intressen framför konsumentens bästa intressen. Finansinspektionen har identifierat flera exempel på hur rådgivare har sålt produkter som är direkt olämpliga för de flesta konsumenter på grund av deras komplexitet, höga kostnader och potentiella risker. Många finansiella produkter är så komplexa att konsumenter har svårt att förstå hur de fungerar, när de kan ge avkastning och vilka risker de innebär. Strukturerade produkter såsom aktieindexobligationer och indexbevis är exempel på sådana komplexa produkter. Produkter med höga avgifter kan leda till att hela eller en stor del av den förväntade avkastningen försvinner. Detta gäller särskilt för strukturerade produkter, onoterade företagsobligationer, vissa fonder och kapitalförsäkringar.

Finansinspektionen föreslår en statlig utredning för att ta fram åtgärder som kan motverka intressekonflikter på sparmarknaden. Detta inkluderar att granska ersättnings- och provisionsmodeller för försäkringsförmedlare som distribuerar sparförsäkringar samt att analysera de risker som finns när konsumenter sparar via digitala plattformar. Finansinspektionen betonar även behovet av oberoende rådgivning, som för närvarande är mycket begränsad på marknaden.

3 Ökade bedrägerier

En annan stor utmaning som framkommer i rapporten är den kraftiga ökningen av investeringsbedrägerier. Antalet polisanmälningar om investeringsbedrägerier ökade med cirka 54 procent mellan åren 2022-2023. Bedragare använder ofta social manipulation där bedragare kan utge sig för att representera banker eller myndigheter för att lura konsumenter att investera pengar i bedrägliga upplägg. Konsumenter luras även att investera i falska finansiella produkter. Finansinspektionen har en omfattande varningslista med företag som saknar nödvändiga tillstånd och publicerar kvartalsvisa sammanställningar om investeringsbedrägerier. Under år 2023 har Finansinspektionen publicerat närmare 3 300 varningar.

4 Behov av nya regler för stärkt konsumentskydd

En av Finansinspektionens rekommendationer är att flytta regler för kreditgivning från betaltjänstlagen till konsumentkreditlagen. Finansinspektionen föreslår att ett lagkrav införs som innebär att banker måste pröva om de kan hantera risker för penningtvätt och finansiering av terrorism genom andra åtgärder innan de nekar eller säger upp ett betalkonto. Detta krav skulle säkerställa att bankerna gör en individuell bedömning av varje kunds riskprofil istället för att fatta breda beslut som påverkar stora grupper av konsumenter. Många konsumenter som nekas ett betalkonto hamnar i ett finansiellt utanförskap och detta lagkrav skulle kunna minska den risken.

Finansinspektionen stödjer också EU-kommissionens förslag till ett lagstiftningspaket för icke-professionella investeringar. Detta förslag syftar till att stärka konsumenternas ställning vid investeringar i spar- och försäkringsprodukter. Några punkter i förslaget inkluderar bl.a. regler för att minska intressekonflikter genom att begränsa provisionerna som rådgivare kan ta ut samt regler avseende tydligare och mer utförlig information om produkternas risker, kostnader och funktioner.

5 Wesslau Söderqvist Advokatbyrås rekommendationer

Rapporten understryker behovet av stärkt konsumentskydd och transparens inom den finansiella sektorn. Wesslau Söderqvist Advokatbyrå rekommenderar att finansiella rådgivare löpande utvärderar ersättningsmodeller för att säkerställa att intressekonflikter kan identifieras och hanteras på ett ändamålsenligt sätt. Även interna riktlinjer bör ses över och utbildningsinsatser genomföras för att säkerställa att rådgivning har kundens bästa i fokus.

Wesslau Söderqvist Advokatbyrå rekommenderar utöver det ovanstående att information om finansiella produkter löpande bör ses över och justeras vid behov. Det ska säkerställas transparens och finnas detaljerad information om risker och avgifter förenade med finansiella produkter och investeringar.

Wesslau Söderqvist Advokatbyrå bevakar all lagstiftning som tar sikte på konsumentskydd och avser att återkomma med information avseende initiativ om stärkt konsumentskydd från EU-kommissionen.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. Anmärkning och sanktionsavgift mot Nasdaq Stockholm Aktiebolag

---

19 juni 2024

1 Bakgrund

Finansinspektionen har i sin tillsyn av Nasdaq Stockholm Aktiebolag, nedan Nasdaq Stockholm alternativt börsen, identifierat betydande brister i börsens handelsövervakning och prospekthantering. Nasdaq Stockholm har enligt Finansinspektionen inte vidtagit de åtgärder som krävs för efterlevnad av lagen (2007:528) om värdepappersmarknaden (VpmL) samt EU:s marknadsmissbruksförordning (MAR). Med anledning av bristerna tilldelas Nasdaq Stockholm en anmärkning och åläggs att betala en sanktionsavgift om 100 miljoner kronor. Nedan följer en kort översikt om vilka iakttagelser och bedömningar som Finansinspektionen har identifierat.

2 Närmare om Finansinspektionens granskning

Finansinspektionen har undersökt om Nasdaq Stockholm har uppfyllt kraven på effektiv handelsövervakning i samband med fyra större bolagshändelser om offentliga uppköpserbjudanden och sammanslagningar under år 2021 och år 2022, samt om börsen har rapporterat om misstänkt insiderhandel. Därtill har undersökts om börsen vid två tillfällen under 2022 och 2023 inledde handel med finansiella instrument utan att Finansinspektionen godkänt och registrerat prospekt för instrumenten.

De bolag som berörs av granskningen genom att de vid tidpunkten för respektive bolagshändelse hade alla sina aktier upptagna till handel på Nasdaqs reglerade marknad är ICA Gruppen Aktiebolag, Lundin Energy AB, Swedish Match AB och Haldex Aktiebolag.

2.1 Transaktionerna utgör misstänkt insiderhandel

Nasdaq Stockholm har inför varje bolagshändelse fått förhandsinformation om att förhållanden som kan antas vara av extraordinär betydelse skulle offentliggöras. Under perioden mellan förhandsinformationen och offentliggörandet av informationen om händelsen, har aktörer med anknytning till Nasdaq Stockholms handelsövervakning och emittenten (gällande fallet ICA), köpt aktier av större volymer i de berörda bolagen. Under samma period har inte några sådana aktier sålts i bolagen och aktörernas handelsmönster konstateras ha avvikit från tidigare

handlingsmönster. Utifrån detta menar Finansinspektionen att transaktionerna har föranlett misstankar om insiderhandel.

2.2 Transaktionerna borde ha upptäckts

Finansinspektionen betonar att Nasdaq Stockholm blivit försedd med förhandsinformation om bolagshändelserna. Att börsen hade kännedom om insiderinformation som sannolikt hade stor kurspåverkan menar inspektionen borde motiverat en ingående granskning. Därutöver uppmärksammas att förhandsinformationen i sig gav anledning att granska handeln innan offentliggörandet. Detta eftersom den indikerade på en förhöjd risk för insiderhandel.

Finansinspektionen uppmärksammar vidare att det, med tanke på Nasdaqs omfattande handel på de handelsplatser som börsen bedriver och med utgångspunkt i artikel 2.3 och 2.4 i MAR, krävs att börsen analyserar enskilda aktörers handel, utöver handelsmönster för specifika aktier. Åtminstone måste de största nettoköparna som är fysiska personer och aktörer som gjort förhållandevis stora köp innan offentliggörandet utan att sälja några aktier i bolagen omfattas av den analysen. En sådan fördjupad analys motiveras också utifrån de berörda individernas historiska handelsmönster.

I undersökningen framhålls att Finansinspektionen med lätthet kunde hitta de personkopplingar som fanns mellan de handlande aktörerna och ICA respektive Nasdaq Stockholms handelsövervakning. Börsen borde därför ha upptäckt de misstänkta transaktionerna.

2.3 Övervakningen har inte varit effektiv

Nasdaq Stockholm är enligt 16.1 Mar och 13 kap. 7 § första stycket första meningen VpmL förpliktigad att ha effektiva arrangemang, system och förfaranden för att förhindra- och upptäcka insiderhandel och försök därtill. Särskilt bedöms Nasdaq Stockholm ha brustit i säkerställandet av en lämplig skyddsnivå gällande analyserna som utförts av människor inom övervakning, upptäckt och identifiering av transaktioner och handelsorder som potentiellt kunnat utgöra insiderhandel. Detta har resultat i att börsen anses åsidosatt sina skyldigheter avseende effektiv övervakning.

2.4 Underlåtenhet att rapportera misstänkt insiderhandel

Genom att underlåta att underrätta Finansinspektionen om de misstänkta transaktionerna har Nasdaq Stockholm åsidosatt bestämmelsen i 16.1 andra stycket MAR och därigenom inte heller uppfyllt det krav som framkommer av 13 kap. 7 § andra stycket VpmL.

2.5 Bristande prospekthantering

Slutligen har Finansinspektionen undersökt om Nasdaq Stockholm vid två tillfällen under år 2022 och år 2023 inledde handel med finansiella instrument på den reglerade marknaden i strid med 13 kap. 3 § VpmL eftersom inspektionen varken godkänt eller registrerat prospekt för instrumenten. Eftersom det ställs krav på att i varje fall som ett finansiellt instrument tas upp till handel på en reglerad marknad kontrollera om det finns prospektskyldighet, inte enbart på en systematisk nivå, konstateras Nasdaq Stockholm också brustit i detta ansvar.

3 Sanktioner mot Nasdaq Stockholm

De brister som identifierats i Nasdaq Stockholms övervakning och rapportering av misstänkt insiderhandel visar att bestämmelser i både MAR och VpmL har överträtts, vilket påkallar ett ingripande från Finansinspektionen. Bristerna anses dock inte så allvarliga att det blivit aktuellt att återkalla börsens tillstånd eller ge börsen en varning. I stället ges Nasdaq Stockholm en anmärkning förenat med en sanktionsavgift om 100 miljoner kronor. Finansinspektionen anför att det finns skäl att se allvarligt på bristerna eftersom det ytterst handlar om förtroendet för finansmarknaden.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Till följd av Finansinspektionens ingripande mot Nasdaq Sverige, kan börsen förväntas se över sina interna rutiner, vilket kan föranleda en ökad intensitet beträffande övervakning av emittenter.

Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer som står under Nasdaq Sveriges övervakning bör om aktuellt se över dess egna rutiner avseende insyn och insiderhandel, men även mer generella processer och rutiner avseende intern styrning och kontroll för att förhindra att likartade problem uppstår. Vidare bör aktörer som omfattas se till att dess oberoende kontrollfunktioner, t.ex. risk eller compliance, löpande följer upp och kontrollerar att rutiner och processer är fullgoda och lämpliga för att identifiera liknande problematik.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. Sanktionsbeslut mot Avanza Bank AB

---

27 juni 2024

1 Bakgrund

Integritetsskyddsmyndigheten (IMY) har i sin tillsyn av Avanza Bank AB, nedan Avanza alternativt banken, identifierat brister i Avanzas behandling av personuppgifter och utfärdat en sanktionsavgift om 15 miljoner kronor. Avanza har enligt beslutet använt en så kallad Meta-pixel på sin webbplats och app vilket medfört att en stor mängd uppgifter om exempelvis kunders värdepappersinnehav, personnummer och kontonummer obehörigen överförts till Meta. Avanza konstateras härigenom ha behandlat personuppgifter med en otillräcklig säkerhetsnivå, i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen (GDPR).

Bakgrunden till det inträffade är att Avanza, i syfte att optimera sin marknadsföring, började använda Metas tjänst Facebook-pixeln (numera Meta-pixeln). Därefter utvecklades under 2019 två nya delfunktioner inom Meta-pixeln kallade Automatic Advanced Matching (AAM), och Automatiska Händelser (AH), som av misstag aktiverades av banken. IMY mottog sommaren 2021 en anmälan om personuppgiftsincidenten och inledde tillsyn. 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 GDPR. Nedan följer en sammanfattning av vilka iakttagelser och bedömningar som IMY har gjort.

2 Integritetsskyddsmyndighetens bedömning

2.1 Personuppgiftbehandlingen har inneburit en hög risk och krävt en hög skyddsnivå

Syftet med implementerandet av Meta-pixeln var att optimera bankens marknadsföring. Avanza har en skyldighet att, oavsett ändamål med behandlingen, skydda personuppgifter genom att vidta lämpliga tekniska och organisatoriska åtgärder med syftet att säkerställa en lämplig säkerhetsnivå.

IMY konstaterar att de uppgifter som hanterats av Avanza bestått av särskilt skyddsvärda personuppgifter i form av personnummer, vilka endast får behandlas under vissa förutsättningar. Därutöver har ekonomiska uppgifter behandlats, såsom uppgifter om kontonummer, värdepappersinnehav, kredlimit och lånebelopp, för vilka de registrerade har berättigade förväntningar på en hög grad av konfidentialitet. Personuppgiftsbehandlingen har

skett inom ramen för Avanzas kärnverksamhet i vilken uppgifterna omfattas av lagstadgad tystnadsplikt. Sammantaget medför detta att banken borde haft god förmåga att säkerställa en lämplig säkerhetsnivå.

Därtill noteras att Avanzas behandling av personuppgifterna har inneburit en hög risk för fysiska personers rättigheter och friheter med hänsyn till att uppgifterna som behandlats har varit av skyddsvärd karaktär och berört cirka 500 000 –1 000 000 personer vars uppgifter obehörigen överförts till Meta. Mot bakgrund av detta konstateras att behandlingens art, omfattning och sammanhang har medfört krav på en hög skyddsnivå.

2.2 Avanza har inte vidtagit tillräckliga åtgärder för att skydda uppgifterna

IMY poängterar att enbart det förhållande att Avanza överfört uppgifter till Meta innebär att uppgifterna rent faktiskt inte har skyddats mot obehörigt röjande. Av bankens rapporterade information framgår att det finns formaliserade rutiner för att säkerställa en korrekt behandling av personuppgifter inför, i samband med och efter införandet av nya funktioner på webbplatsen, samt att dessa ingår i bankens styrdokument. IMY noterar därmed att bristen uppstått genom att banken inte följt rutinerna, trots att organisatoriska åtgärder fanns på plats. Att banken inte tillämpat sina säkerhetsrutiner vid införandet av de två funktionerna, AAM och AH i Meta-pixeln, konstateras bero på att de aktiverats utan bankens vetskap.

Röjandet av och den pågående överföringen av personuppgifter till Meta pågick i ett och ett halvt år innan banken via en extern källa fick kännedom om den obehöriga överföringen. IMY noterar att banken saknat förmåga att upptäcka incidenten och poängterar att banken borde ha haft ett sådant systematiskt säkerhetsarbete med kontroller av viss regelbundenhet att incidenten skulle ha upptäckts.

Sammanfattningsvis konstateras Avanza ha haft rutiner att följa upp dokumenterade förändringar men saknat förmåga att upptäcka och åtgärda förändringar som genomförts utan att rutinerna följts. Givet detta framhåller IMY att banken saknat tekniska och organisatoriska säkerhetsrutiner för att systematiskt följa upp och upptäckta oavsiktliga förändringar i sina system. Detta innebär att personuppgifter behandlats i strid med GDPR. Att ärendet gäller bankinformation och att personuppgifterna till övervägande del har röjts och överförts från ett för kunderna inloggat läge medför att IMY ser allvarligt på det inträffade. Bristen har därför också inneburit en överträdelse av de grundläggande säkerhetsprinciperna avseende integritet och konfidentialitet i GDPR.

2.3 Avanzas agerande efter personuppgiftsincidenten

När Avanza fick kännedom om det inträffade avaktiverade banken Meta-pixeln i sin helhet och uppger att Meta bekräftat att de personuppgifter som insamlats har raderats på ett sätt som omöjliggör för Meta att återskapa dem. Därutöver har Avanza meddelat att de sett över sina interna rutiner och implementerat ytterligare styrdokument som syftar till att säkerställa en korrekt och säker behandling av personuppgifter.

3 Val av ingripande

Att Avanza har behandlat personuppgifter i strid med artikel 32.1 i GDPR och att överträdelsen är av så allvarligt slag att det också är fråga om en överträdelse av den grundläggande säkerhetsprincipen i artikel 5.1 f i GDPR medför att en administrativ sanktionsavgift ska utfärdas mot Avanza. Vid beräknandet av sanktionsavgiftens storlek ska Avanza-koncernens årsomsättning enligt moderbolagets koncernredovisning läggas till grund för beräkningen, liksom överträdelsens allvar och att sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande. Mot bakgrund av överträdelsen som anses allvarlig och att överträdelsen pågått under en längre tid fastställer IMY att Avanza ska betala en sanktionsavgift om 15 miljoner kronor för de konstaterade överträdelserna.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

IMY signalerar tydligt att användande av analysverktyg i syfte att optimera marknadsföring kan påkalla ett säkerhetsarbete med regelbundna kontroller utöver det vanliga säkerhetsarbete som utförs. Personuppgifter måste behandlas på ett sätt som säkerställer lämplig säkerhet, inbegripet skydd mot obehörig eller otillåten behandling, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Wesslau Söderqvist Advokatbyrå rekommenderar mot bakgrund av IMY:s sanktionsbeslut att personuppgiftsansvariga utöver att ha rutiner för att följa upp dokumenterade förändringar som utförts, också säkerställer att förmåga finns att upptäcka och åtgärda förändringar som genomförs i de fall rutinerna inte följs. Detta innefattar ett systematiskt säkerhetsarbete med att bland annat genomföra kontroller och stresstester med viss regelbundenhet.

Har ni frågor med anledning av det ovanstående eller vill ha hjälp med att se över säkerhetsarbetet och de interna rutinerna avseende er personuppgiftsbehandling är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.