Till
Styrelsen i S:t Erik Försäkrings AB

Rapport för perioden 14 maj - 19 september 2024 avseende regelefterlevnad

1 Inledning

Genom denna rapport redovisar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av S:t Erik Försäkrings AB:s, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen har vidtagit under perioden.

2 Händelser av relevans under perioden

2.1 Regelbevakning och relevanta sanktionsbeslut

Under perioden har följande nyhetsbrev tillställts Bolaget. Dessa återfinns i sin helhet i bilaga 1.

- Anmärkning och sanktionsavgift mot Nasdaq Stockholm Aktiebolag.
- Sanktionsbeslut mot Avanza Bank AB.
- Granskning av dataskyddsombudens roll och ställning.
- IKT-säkerhet och IKT-risker.
- Kontraktsmässiga arrangemang.
- Teknisk standard om incidenthantering.
- Finansinspektionen återkallar Finans 24/7 Sverige AB:s tillstånd.
- De europeiska tillsynsmyndigheterna har offentliggjort den andra omgången policyprodukter inom ramen för DORA.
- Slutgiltig rapport om förslag till teknisk tillsynsstandard och tekniska genomförandestandarder för incidentrapportering.

Notera att nyhetsbreven avseende ”Finansinspektionen återkallar Finans 24/7 Sverige AB:s tillstånd” och ”De europeiska tillsynsmyndigheterna har offentliggjort den andra omgången policyprodukter inom ramen för DORA” endast har översänts via e-post och därför inte återfinns i bilaga 1.

2.2 Kontroll av Bolagets regelefterlevnad

Kontroll av Bolagets regelefterlevnad har ägt rum genom ett möte med representanter från Bolaget samt genom granskning av handlingar.

Kontrollen utgår från den årsplan som funktionen för regelefterlevnad har upprättat inför verksamhetsåret och redogörs för närmare nedan.

Område	*Kontroll*	*Compliancerisk (Grön/Gul/Röd)*
Övrig regelefterlevnad	Intressekonflikter.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Kompetens och kunskapsnivå hos personalen (kunskapskraven i IDD).	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Kompetens och kunskapsnivå hos styrelsen (fit & proper) inkl. samlad kompetens.	Kontrollen har inte föranlett några synpunkter.

Andra kvartalets kontroll har till övervägande del bestått i att följa upp Bolagets hantering av kunskap och kompetens hos såväl anställda som styrelsen. Kontrollen har utgått ifrån de krav som uppställs i försäkringsrörelselagen (FRL) samt i lagen om försäkringsdistribution (LFD). Därtill har funktionen för regelefterlevnad granskat Bolagets hantering av intressekonflikter samt Bolagets riktlinjer för ändamålet.

Intressekonflikter

Uppföljning av identifiering och hantering av intressekonflikter. Kontrollen har syftat till att följa upp om Bolaget identifierat några nya intressekonflikter som behövt hanteras.

Bolaget har redogjort för Bolagets interna rutiner för att identifiera och hantera intressekonflikter. Funktionen för regelefterlevnad har vidare tagit del av Bolagets interna riktlinjer för hantering av intressekonflikter som omfattar samtliga anställda och Bolagets ledning. Utöver att det finns en anmälningsskyldighet avseende intressekonflikter i verksamheten så är det även en stående punkt vid varje styrelsesammanträde i Bolaget.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

Kunskap och kompetens hos anställda

Granskning av Bolagets interna rutiner och riktlinjer för kunskap och kompetens. Kontrollen har syftat till att säkerställa att Bolaget vidtar rimliga åtgärder för att efterleva kunskaps- och fortbildningskravet i försäkringsdistributionsregelverket (IDD).

Bolaget har redogjort för Bolagets interna rutiner för fortbildning och kunskapstest som omfattar de anställda som direkt deltar i Bolagets försäkringsdistribution. Bolaget bedöms ha goda rutiner för löpande fortbildning. Bolagets anställda har därtill den 26 augusti 2024 avlagt godkänt kunskapstest avseende år 2024.

Funktionen för regelefterlevnad bedömer sammantaget att Bolaget har goda rutiner och riktlinjer för att säkerställa efterlevnad av kraven på kunskap och kompetens enligt IDD.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

Fit & proper

Uppföljning av styrelsens samlade kompetens. Kontrollen har syftat till att säkerställa att Bolagets styrelse efterlever kraven som ställs i Solvens II-regelverket på styrelsens samlade kompetens samt följa upp om det finns behov av kompetensutveckling.

Bolagets styrelse har under år 2023 genomfört den årliga ”fit & proper” övningen där samtliga styrelseledamöter skattat dels sin egen enskilda kunskap och kompetens, dels styrelsens samlade kompetens. I denna övning identifieras eventuella behov av kompetensutveckling och Bolaget följer upp och justerar styrelsens utbildningsplan för kommande år. Årets fit & proper kommer att genomföras den 27 september 2024.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

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.

2.4 Styrelsesammanträde

Funktionen för regelefterlevnad har den 24 maj 2024 deltagit vid styrelsemöte i Bolaget och därvid redogjort för bl.a. föregående kvartals regelefterlevnadsrapport.

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 20 september 2024

Johan Grenefalk

WESSLAU SÖDERQVIST

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.

Nyhetsbrev

Ang. Granskning av dataskyddsombudens roll och ställning

---

9 juli 2024

1 Bakgrund

Den Europeiska dataskyddstyrelsen tillsammans med de nationella dataskyddsmyndigheterna, däribland Integritetsskyddsmyndigheten, inledde år 2023 en samordnad åtgärd med syftet att undersöka dataskyddsombudets roll och ställning. Integritetsskyddsmyndigheten har som del i arbetet inlett tillsyn mot ett 50-tal organisationer som samtliga har dataskyddsombud, och en fördjupad granskning avseende sex av verksamheterna.

Enligt dataskyddsförordningen, nedan GDPR, är vissa verksamheter skyldiga att utse dataskyddsombud vars uppgift är att bidra till att den egna verksamheten följer dataskyddslagstiftningen. Ett ombud får därutöver utföra andra uppgifter och uppdrag, förutsatt att det inte leder till intressekonflikter. I enlighet med GDPR måste ombudens oberoende och förmåga att effektivt utföra sina dataskyddsuppgifter säkerställas.

Förra veckan publicerades Integritetskyddsmyndighetens fördjupade granskning som avslutar arbetet med Dataskyddsstyrelsens samordnade åtgärd. Integritetskyddsmyndighetens arbete att vägleda dataskyddsombud fortsätter emellertid i andra former, bland annat har två referensgrupper upprättats för att föra en kontinuerlig dialog och fånga upp behov av ny vägledning för dataskyddsombuden. Nedan följer en kort översikt avseende de iakttagelser som Dataskyddsstyrelsen och Integritetsskyddsmyndigheten har identifierat.

2 Närmare om den Euroepiska dataskyddsstyrelens granskning

2.1 Undersökningen

I januari år 2024 publicerade Dataskyddsstyrelsen en rapport som sammanställde nationella iakttagelser av om dataskyddsombuden har den roll och ställning som krävs enligt artiklarna 37 – 39 i GDPR, samt om de har de resurser som de behöver för att utföra sina uppgifter. Olika organisationer och dataskyddsombud kontaktades utifrån ett brett spektrum av sektorer, både inom offentlig och privat sektor. Rapporten listar hinder som skyddsombuden står inför, tillsammans med rekommendationer för att ytterligare stärka skyddsombudens roll.

2.2 Undersökningens resultat

Trots vissa farhågor och utmaningar som dataskyddsombud står inför är resultaten av granskningen huvudsakligen uppmuntrande. Dataskyddsstyrelsen uppmärksammar att majoriteten av dataskyddsombuden har de färdigheter och kunskaper som krävs för att utföra arbetet och att de regelbundet får utbildning i dataskyddsfrågor. Därtill har de väl definierade uppgifter och utsätts sällan för påtryckningar om hur arbetet ska utföras.

De utmaningar som identifieras är att utse uppgiftsskyddsombud trots att det är obligatoriskt, otillräckliga resurser eller expertkunskaper samt att dataskyddsombuden inte fullt ut anförtros de uppgifter som föreskrivs i GDPR. Mot bakgrund av utmaningarna ger rapporten vissa rekommendationer till organisationer, dataskyddsombud och dataskyddsmyndigheter. Dataskyddsmyndigheter uppmuntras att genomföra medvetandehöjande åtgärder samt informations- och tillsynsåtgärder. Därtill betonas vikten vid att organisationer säkerställer att skyddsombud har tillräckliga möjligheter, tid och resurser för att kontinuerligt uppdatera sin kunskap och lära sig om den senaste utvecklingen på området.

3 Närmare om Integritetsskyddsmyndighetens granskning

3.1 Undersökningen

I Integritetskyddsmyndighetens tillsyn har organisationer besvarat frågor avseende dataskyddsombudens kvalifikationer, uppgifter och ställning med syftet att bedöma om deras roll och ställning svarar mot kraven i GDPR och om de har de resurser som behövs för att utföra sina uppgifter effektivt. En fördjupad granskning inleddes därefter med ett mindre urval verksamheter och kretsade kring några särskilt viktiga frågeställningar.

De verksamheter som ingått i den fördjupade tillsynen är Hemköpskedjan AB, PostNord Sverige AB, Regionstyrelsen i Region Västerbotten, Socialnämnden i Stockholms stad, Socialnämnden i Örebro kommun och Swedavia AB. Gemensamt för verksamheterna är att dataskyddsombuden har haft andra uppdrag utöver att bidra till att den egna verksamheten följer dataskyddslagstiftningen. Bland annat har dataskyddsombuden haft uppdrag som informationssäkerhetschefer, haft specifika ansvarsområden inom compliance, risk och säkerhet, och arbetat som förvaltningsjurister eller regionsjurister.

3.2 Undersökningens resultat

I besluten poängteras att funktioner som innebär ledande befattningar typiskt sett kan ge upphov till intressekonflikt med rollen som dataskyddsombud, i strid med GDPR. Detta eftersom det ofta innebär att ombudet är delaktigt i beslut rörande personuppgiftsbehandlingar på ett sådant sätt att skyddsombudets oberoende kan ifrågasättas. PostNords dataskyddsombud som innehar ledaransvar inom områdena compliance, risk och säkerhet, Hemköps dataskyddsombud som är Risk Manager, Socialnämnden i Stockholms dataskyddsombud som arbetar som förvaltningsjurist och Swedavias dataskyddsombud som arbetar som informationssäkerhetschef bedöms mot den bakgrunden inte medföras ansvar som leder till delaktighet i beslut som gäller ändamål och medel för personuppgiftsbehandlingar.

I sin tillsyn har Integritetsskyddsmyndigheten däremot identifierat brister i Region Västerbottens verksamhet, i vilken skyddsombudet också är regionsjurist vid ledningsstaben. Dataskyddsombudet ska oberoende och självständigt granska organisationens efterlevnad av dataskyddslagstiftningen, vilket omfattar granskning av dataskyddsarbetet i ledningsstaben. Eftersom regionsjuristen är delaktig i ledningsstaben genom rådgivning bedömer Integritetsskyddsmyndigheten att det funnits en intressekonflikt i strid med reglerna i GDPR.

Ytterligare en brist har identifierats hos Socialnämnden i Örebro eftersom varsamheten inte på ett korrekt sätt eller i god tid säkerställt att skyddsombudet deltagit i alla frågor som rör personuppgiftsskyddet. Integritetskyddsmyndigheten bedömer även att verksamheten inte stöttat ombudet tillräckligt genom att tillhandahålla de resurser som krävs och inte heller säkerställt att ombudet rapporterat direkt till socialnämndens högsta förvaltningsnivå. Med anledning av bristerna tilldelas Region Västerbotten och Socialnämnden i Örebro reprimander.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

För att säkerställa effektiv efterlevnad av GDPR och ett tillfredsställande säkerhetsarbete genom dataskyddsombud rekommenderas att verksamheter tar del av de fullständiga rapporter som den Europeiska dataskyddsstyrelsen och Integritetsskyddsmyndigheten publicerat.

Wesslau Söderqvist Advokatbyrå rekommenderar ett kontinuerligt arbete för att stärka dataskyddsombudens roll och ställning. Särskilt viktigt är det, för de verksamheter som enligt GDPR är skyldiga att utse dataskyddsombud, att skyddsombudets oberoende och självständighet garanteras, och att skyddsombud erhåller de möjligheter, den tid och de resurser som krävs för att kunna utföra ett effektivt arbete. Därutöver måste säkerställas att skyddsombuden har de färdigheter och kunskaper som krävs och att de regelbundet och

kontinuerligt får uppdatera sina kunskaper och lära sig om den senaste utvecklingen på området.

Har ni frågor avseende de krav som ställs enligt GDPR eller eventuella intressekonflikter kopplade till dataskyddsombuden får ni gärna kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. IKT-säkerhet och IKT-risker

---

11 juli 2024

1 Sammanfattning av delegerad förordning (EU) 2024/1774

1.1 IKT-säkerhet och riskhantering

Europeiska kommissionen har antagit en förordning som reglerar hantering av IKT-säkerhet och IKT-risker inom finansiella enheter och omfattar flera aspekter från övergripande riskprofiler till specifika procedurer för sårbarhetshantering. Förordningen kompletterar Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). Finansiella enheter ska vid utarbetande och genomförande av riktlinjer och verktyg för IKT-säkerhet beakta enhetens storlek, riskprofil och tjänsternas komplexitet. Detta inkluderar kryptering, nätverkssäkerhet, förändringsledning och påverkan på dataintegritet och tillgänglighet.

Denna förordning ska tillämpas från och med den 17 januari 2025.

1.2 IKT-säkerhetspolicyer och verktyg

Finansiella enheter ska utveckla strategier och protokoll som inkluderar nätverkssäkerhet, skydd mot dataintrång och bibehållande av dataintegritet och konfidentialitet. Dessa ska vara anpassade till enhetens informationssäkerhetsmål och strategier för digital operativ motståndskraft. Enheterna ska dokumentera och genomföra riktlinjer för att hantera IKT-risker inklusive identifiering av sårbarheter, riskbedömning och implementering av krishanteringsåtgärder. Årliga översyner av kvarstående risker är obligatoriska.

1.3 Förvaltning av IKT-tillgångar

Finansiella enheter ska ha en policy för livscykelhantering av IKT-tillgångar som inkluderar övervakning, dokumentation och klassificering. Kritiska tillgångar ska dokumenteras noggrant med information om ägare, placering och beroenden. Policyn ska inkludera kryptering av data i vila och under överföring, hantering av krypteringsnycklar samt krav på att uppdatera krypteringstekniker för att säkerställa motståndskraft mot cyberhot.

1.4 Säkerhet i IKT-verksamheten

Finansiella enheter ska utarbeta riktlinjer för säker installation, underhåll och återställning av IKT-system. Detta inkluderar säkerhetskopiering, övervakning och hantering av fel samt åtskillnad mellan produktions- och testmiljöer. Förfaranden ska säkerställa identifiering av kapacitetskrav och optimera resursanvändning för att upprätthålla och förbättra systemens tillgänglighet och effektivitet. Förfaranden ska identifiera och hantera sårbarheter genom regelbundna analyser och uppdateringar. Tredjepartsleverantörer ska övervakas för att säkerställa att de hanterar sårbarheter i tillhandahållna tjänster.

1.5 Data- och systemsäkerhet

Finansiella enheter ska skapa och implementera omfattande säkerhetsförfaranden för data och IKT-system. Det ska inkludera åtgärder som åtkomstbegränsningar, säker konfigurationsbaslinje och åtgärder mot skadlig kod och otillåten programvara. Säkerhetsåtgärder ska säkerställa att endast godkända datalagringsmedier och system används. Det inkluderar krav på hantering av portabla och privata slutpunktsenheter, säker radering av data och avveckling av datalagringsenheter som innehåller konfidentiell information.

1.6 Loggning och händelsespårning

Finansiella enheter ska utveckla loggnigsprocedurer för att identifiera och logga relevanta händelser, säkerställa att loggar skyddas mot manipulation och för att upptäcka systemfel. Loggarna ska kunna användas för att effektivt upptäcka onormal verksamhet.

1.7 Hantering av nätverkssäkerhet

Finansiella enheter ska genomföra åtgärder för att skydda sina nätverk mot intrång och dataförlust. Detta inkluderar segmentering av nätverk, dokumentation av nätverksanslutningar, användning av dedikerade nätverk för hantering av IKT-tillgångar och kryptering av nätverkskommunikation. Finansiella enheter ska säkerställa tillgänglighet, autenticitet, integritet och konfidentialitet under överföring. Åtgärder ska införas för att förebygga och upptäcka dataläckage och säkerställa säker överföring av information.

1.8 IKT-projekt och förändringsledning

En policy för IKT-projektledning ska säkerställa effektiv hantering av IKT-projekt, inklusive riskbedömningar och säkerhetstester. Vid förändringar av IKT-system ska kontroller införas för att säkerställa att säkerhetskraven uppfylls och att ändringar implementeras på ett kontrollerat sätt. Säkerhetsrutiner ska identifiera tekniska och säkerhetsmässiga specifikationer för IKT-system. Finansiella enheter ska genomföra testning av nya och uppdaterade system innan de tas i bruk för att säkerställa att de fungerar som avsett och uppfyller säkerhetskraven.

1.9 Åtkomstkontroll

Finansiella enheter måste utveckla och införa en åtkomstkontrollpolicy som omfattar:

1. Tilldelning av åtkomsträttigheter som är baserad på behovsenlig behörighet, användning och lägsta behörighet inklusive fjärr- och nödsituationer.

2. Åtskillnad av funktioner som avser att förhindra omotiverad tillgång till kritiska data och kombinationer av åtkomsträttigheter som kan kringgå kontroller.

3. Begränsa generiska och delade användarkonton. Säkerställ identifiering av användare för utförda åtgärder i IKT-system. Det är även av betydelse att använda kontroller och verktyg för att förhindra obehörigt tillträde till IKT-tillgångar.

4. Fastställ rutiner för att bevilja, ändra eller återkalla åtkomsträttigheter snabbt vid behov eller vid anställningens slut.

5. Använda autentisering som står i proportion till IKT-tillgångars riskprofil och stark autentisering för fjärråtkomst och kritiska funktioner.

6. Loggning och övervakning av fysisk åtkomst till kritiska områden. Säkerställ att endast behöriga personer har tillgång.

1.10 IKT-relaterade incidenter

För att hantera IKT-relaterade incidenter ska finansiella enheter dokumentera incidenthanteringsprocessen, upprätta kontaktlistor med interna och externa intressenter involverade i IKT-säkerhet. De ska även använda sig av tekniska

mekanismer för att snabbt upptäcka onormal verksamhet och beteenden, bevara bevis för IKT-incidenter så länge som nödvändigt och proportionellt till incidentens allvar. Finansiella enheter ska även analysera betydande eller återkommande incidenter och identifiera mönster.

1.11 Upptäckt och hantering av incidenter

Finansiella enheter måste fastställa roller och ansvar för en effektiv upptäckt och hantering av incidenter. De ska även samla in och analysera data från interna och externa faktorer, cyberhot och incidentrapportering från tredjepartsleverantörer. Finansiella enheter bär ansvar för att effektivt hantera och upptäcka incidenter både under och utanför arbetstid. De ska även säkerställa identifiering av datum och tid för avvikande aktiviteter och skydda inspelningar mot obehörig åtkomst.

1.12 Kontinuitetshantering inom IKT

Finansiella enheter ska ha IKT-kontinuitetsplaner som inkluderar beskrivning av IKT-kontinuitetens mål, arrangemang och tidsramar. De ska inneha tydliga roller och resurser för genomförandet av kontinuitetsplanen, regelbunden testning av kontinuitetsplanen och anpassning baserat på testresultat och scenarier. Kontinuitetsplanen ska vara godkänd av ledning samt dokumenterad och tillgänglig vid nödsituationer. Kontinuitetsplanen ska även testas minst en gång om året eller vid större förändringar.

1.13 Fysisk och miljösäkerhet

Finansiella enheter ska implementera fysiska säkerhetsåtgärder baserat på hotbild och riskprofil och skydda lokaler och datacentraler från obehörigt tillträde, angrepp och miljöhot. De ska även införliva skydd mot miljöfaror genom skyddsåtgärder efter lokalernas betydelse och verksamhetens kritikalitet.

1.14 Åtkomstkontroll

Finansiella enheter ska utveckla, dokumentera och genomföra åtkomstkontroll för fysisk åtkomst. De ska även hantera användaransvar, kontohantering och autentiseringsmetoder enligt praxis. Finansiella enheter ska regelbundet granska och uppdatera åtkomsträttigheter.

1.15 Säkerhet inom IKT-verksamheten

Finansiella enheter ska övervaka IKT-tillgångars livscykel, genomföra automatiserade sårbarhetsskanningar och hantera risker med äldre eller ostödda IKT-tillgångar. De ska även logga händelser relaterade till åtkomstkontroll och IKT-drift samt genomföra åtgärder för att identifiera och analysera hot mot kritisk IKT-verksamhet. Finansiella enheter ska skydda data under användning, överföring och lagring samt förebygga obehöriga anslutningar och säkra nätverkstrafik. Det är även av betydelse att implementera procedurer för säker radering och avveckling av datalagringsenheter. De ska även utföra säkerhetstestning genom upprättande och genomförande av plan för att testa IKT-säkerhetsåtgärder regelbundet samt övervaka och utvärdera testresultaten för att uppdatera säkerhetsåtgärder.

1.16 Rapportering och översyn

Översynsrapporter ska skickas in årligen till den berörda myndigheten. Det ska skickas in en sökbar elektronisk rapport om översyn av IKT-riskhanteringsramen. Rapporten ska innehålla sammanfattningar, analys av brister och åtgärdsplaner.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

För att effektivt hantera IKT-säkerhet och risker inom finansiella enheter rekommenderar Wesslau Söderqvist Advokatbyrå att finansiella enheter:

- Anpassar strategier och protokoll för nätverkssäkerhet, dataintegritet och konfidentialitet.
- Dokumenterar och implementerar riktlinjer för sårbarhetshantering, riskbedömning och krishantering. Årliga översyner av kvarstående risker är obligatoriska.
- Upprätthåller en livscykelhanteringspolicy för IKT-tillgångar inklusive kryptering och dokumentation av kritiska tillgångar.
- Säkerställer uppdatering av krypteringstekniker för att motstå cyberhot.
- Implementerar säkerhetsrutiner för installation, underhåll och återställning av IKT-system.

- Säkerställer regelbundna analyser och uppdateringar för att identifiera och hantera sårbarheter.
- Genomför åtgärder som åtkomstbegränsningar, säker konfigurationsbaslinje och skydd mot skadlig kod.
- Hanterar portabla och privata slutpunktsenheter samt säker radering av data.
- Utvecklar loggningsprocedurer för att identifiera och logga relevanta händelser och upptäcka systemfel.
- Skyddar loggar mot manipulation.
- Skyddar nätverk genom segmentering, dokumentation av nätverksanslutningar och kryptering av nätverkskommunikation.
- Förebygger och upptäcker dataläckage samt säkerställer säker överföring av information.
- Säkerställer effektiv hantering av IKT-projekt med riskbedömningar och säkerhetstester.
- Kontrollerar att säkerhetskraven uppfylls vid systemförändringar.
- Implementerar en policy för tilldelning av åtkomsträttigheter baserat på behov. Säkerställer stark autentisering för fjärråtkomst.
- Begränsar generiska och delade användarkonton samt loggar och övervakar fysisk åtkomst.
- Fastställer roller och ansvar för incidenthantering samt samlar in och analyserar data från olika källor.
- Utvecklar och testar regelbundet IKT-kontinuitetsplaner som inkluderar tydliga mål, roller och resurser.
- Implementerar fysiska säkerhetsåtgärder och skydd mot miljöfaror baserat på hotbild och riskprofil.

Rekommendationerna syftar till att stärka IKT-säkerheten, minimera risker och säkerställa kontinuitet i verksamheten för finansiella enheter.

Har ni frågor med anledning av det ovanstående eller vill ha hjälp med att implementera en riskhanteringsram i enlighet med DORA är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. kontraktsmässiga arrangemang

---

11 juli 2024

1 Sammanfattning av delegerad förordning (EU) 2024/1773

1.1 Bakgrund och syfte

Europeiska kommissionen har nyligen antagit en förordning som kompletterar Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). Den kompletterande förordningen rör kontraktsrättsliga arrangemang och hanteringen av IKT-tredjepartsrisker. Förordningen påverkar inte skyldigheter enligt GDPR och inte heller kravet på att ha skriftliga personuppgiftsbiträdesavtal. Förordningen syftar till att säkerställa transparent och ansvarsfull hantering av leverantörsrelationer för att upprätthålla integritet och effektivitet i den finansiella verksamheten.

Denna förordning ska tillämpas från och med den 17 januari 2025.

1.2 Hantering av IKT-tredjepartsrisker

Finansiella enheter ska etablera och regelbundet revidera strategier för hantering av risker kopplade till tredjepartsleverantörer av IKT-tjänster. Strategin ska omfatta policyer för kritiska eller viktiga funktioner som stöds av dessa leverantörer och tillämpas både på individuell och gruppnivå. Förordningen tar hänsyn till variationen i storlek, struktur och komplexitet bland finansiella enheter. Kraven ska tillämpas på ett sätt som är proportionellt med ovanstående skillnader. Ledningen bär det yttersta ansvaret för att hantera IKT-risker, inklusive risker som uppstår vid användning av tredjepartsleverantörer. De måste säkerställa att policyn antas och revideras minst en gång per år. Policyn ska innehålla detaljer om planering, genomförande, övervakning och förvaltning av kontraktsmässiga arrangemang med tredjepartsleverantörer, inklusive exitstrategier och avslutningsförfaranden.

1.3 Grupp-program och styrformer

Vid tillämpning av denna förordning på undergrupps- eller gruppnivå åligger det moderföretaget som har ansvaret för att tillhandahålla koncernredovisningen eller

undergruppsredovisningen att säkerställa en enhetlig tillämpning av policyn i samtliga finansiella enheter som ingår i koncernen. Ledningsorganet bär ansvar att se över policyn minst en gång om året och uppdatera den vid eventuella behov. Ändringar i policyn ska utgöras i god tid och så snart det är möjligt inom ramen för de relevanta avtalsarrangemangen. Den finansiella enheten ska dokumentera den planerade tidsplanen för genomförandet. Policyn syftar till att etablera tydliga riktlinjer för hantering av IKT-tjänster som understödjer kritiska eller viktiga funktioner inom finansiella enheter. För det första fastställs eller refereras en metod för att identifiera sådana tjänster samt hur och när bedömningen av dem ska utföras och granskas. Ansvarsfördelningen internt identifieras tydligt för godkännande, ledning, kontroll och dokumentation av relevanta kontraktsmässiga arrangemang. Det försäkras att nödvändiga färdigheter och kunskaper upprätthålls för effektiv övervakning av dessa arrangemang, inklusive de IKT-tjänster som omfattas.

1.4 Policy

Intern policy kräver även att tredjepartsleverantörer av IKT-tjänster ska bedömas för att säkerställa att de har tillräckliga resurser för att möta alla juridiska och regulatoriska krav som den finansiella enheten är skyldig att uppfylla. Policyn ska säkerställa att finansiella enheter har rätt att få tillgång till information, genomföra inspektioner, revisioner och IKT-tester enligt fastställda metoder, inklusive intern revision eller tredjepartsrevisioner. En specifik roll inom den verkställande ledningen tillskrivs ansvaret för övervakningen av dessa kontraktsarrangemang, med tydliga riktlinjer för samarbete med kontrollfunktioner och rapporteringsvägar till ledningsorganet. Kontraktsmässiga arrangemang ska vara förenliga med en rad specifika ramar och planer för IKT-riskhantering, informationssäkerhet, IKT-kontinuitet och incidentrapportering enligt relevanta EU-förordningar. Policyn inkluderar krav på oberoende granskning av IKT-tjänster som stödjer kritiska funktioner och deras inkludering i revisionsplaner.

Policyn ska specificera övervakning av kontraktsmässiga arrangemang, inklusive åtgärder vid avtalsbrott och en dokumenterad plan för avtalsuppsägning. Kontraktsmässiga arrangemang befriar inte den finansiella enheten från lagstadgade skyldigheter gentemot kunder. Den finansiella enheten får inte förhindra effektiv tillsyn eller överträda tillsynsrestriktioner. Den finansiella enheten ska säkerställa samarbete med behöriga myndigheter, tillhandahålla tillgång till relevant data och lokaler för revison och tillsyn av IKT-tjänster som stödjer kritiska eller andra viktiga funktioner.

1.5 Riskbedömning

Policyn föreskriver också att en omfattande riskbedömning ska genomföras på flera nivåer för finansiella enheter samt på gruppnivå och undergruppsnivå vid behov innan avtal ingås. Riskbedömningen måste ta hänsyn till alla relevanta krav och tillämplig sektorsspecifik unionslagstiftning. Särskilt viktigt är att bedöma hur tredjepartsleverantörer av IKT-tjänster levererar stödjande tjänster för kritiska eller viktiga funktioner inom den finansiella enheten samt identifiera risker i samband med dessa tjänster.

Det innefattar operativa, rättsliga, IKT-relaterade, renommé-, och konfidentialitets- och personlighetsuppgiftskydds-, datatillgångs-, datahanteringsplats-, leverantörsplats- samt IKT-koncentrationsrisker på entitetsnivå. Åtgärderna syftar till att säkerställa att den finansiella enheten, innan avtal ingås, innehar en grundläggande kunskap för sina affärsbehov, bedömer och hanterar de mångfacetterade riskerna som är förknippade med tredjepartsleverantörers IKT-tjänster som stödjer dess kritiska funktioner.

1.6 Tillbörlig aktsamhet

Den föreslagna policyn syftar till att etablera tydliga och proportionella riktlinjer för att välja och bedöma leverantörer av IKT-tjänster för finansiella enheter. Syftet är att säkerställa att leverantören uppfyller standarderna angående kapacitet, kompetens, resurser och säkerhetsåtgärder som är nödvändiga för att stödja kritiska eller viktiga funktioner. Policyn ställer krav på att finansiella enheter genomför en noggrann bedömning av potentiella leverantörer innan avtal ingås. Bedömningen baseras på leverantörens affärsrykte, kapacitet, tekniska kunskaper, resurser såsom ekonomiska och personella resurser, samt deras förmåga att upprätthålla höga standarder inom informationssäkerhet, riskhantering och interna kontroller. Leverantören ansvarar också för att följa och tillämpa ledande praxis inom IKT-säkerhet och att inneha förmåga att hantera och överväga teknisk utveckling.

Leverantören ska godkänna kontraktsmässiga revisioner för att möjliggöra granskningar från den finansiella enheten eller auktoriserade myndigheter. Policyn specificerar även säkerhetsnivån som krävs för IKT-tjänsternas riskhanteringsram, inklusive krav på riskreducerande och kontinuitetsåtgärder. Metoder för att bedöma leverantörens prestation inkluderar revisioner, oberoende bedömningar,

revisionsrapporter och certifieringar från tredje part samt annan relevant tillgänglig information.

1.7 Rapportering och övervakning

Policyn ska fastställa interna ansvarsområden för godkännande och övervakning av avtal med tredjepartsleverantörer. Den ska även säkerställa att lämplig rapportering till ledningsorganet sker regelbundet. Policyn kräver att finansiella enheter identifierar, förebygger och hanterar intressekonflikter som kan uppstå med tredjepartsleverantörer av IKT-tjänster innan avtal ingås. Det krävs även kontinuerlig övervakning av sådana konflikter. Om koncerninterna IKT-tjänster används för kritiska funktioner måste policyn säkerställa objektiva beslut om avtalsvillkor, inklusive ekonomiska aspekter.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att det antas och införlivas en policy som anpassas efter den specifika enhetens storlek, övergripande riskprofil samt arten och omfattningen av de tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster i enlighet med vad som framgår av den kompletterande förordningen.

En central del av policyn bör vara en noggrann riskbedömning på både enskild enhetsnivå och eventuellt på gruppnivå. Det är viktigt att identifiera och bedöma alla operativa, rättsliga och IKT-relaterade risker som är förknippade med användningen av tredjepartsleverantörer av IKT-tjänster. Denna bedömning bör även omfatta faktorer som leverantörens rykte, tekniska kapacitet, säkerhetsstandarder och förmåga att hantera krav på konfidentialitet och dataskydd.

Policyn bör tydligt fastställa ansvarsområden och metoder för godkännande, ledning och övervakning av de kontraktsmässiga arrangemangen. Det är viktigt att en dedikerad funktion eller medlem av den verkställande ledningen utses för att säkerställa att övervakningen av tredjepartsleverantörernas prestationer sker regelbundet och effektivt. Rapporteringsvägarna till ledningsorganet bör också specificeras för att säkerställa en snabb hantering av eventuella incidenter eller problem.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå. Vi har god erfarenhet av att se över och anpassa IKT-avtal i enlighet med DORA och bistår er gärna.

Nyhetsbrev

Ang. teknisk standard om incidenthantering

---

11 juli 2024

1 Sammanfattning av delegerad förordning (EU) 2024/1772

1.1 Syfte och mål

Europeiska kommissionen har antagit en förordning som syftar till att specificera klassificeringskriterier och väsentlighetströsklar för att fastställa och rapportera allvarliga incidenter och betydande cyberhot inom finanssektorn. Förordningen kompletterar Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). Förordningen har som mål att harmonisera rapporteringskraven för IKT-relaterade incidenter, informations- och kommunikationsteknologi och andra operativa eller säkerhetsrelaterade incidenter som påverkar kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar. Med beaktande av proportionalitetsprincipen bör klassificeringskriterierna och väsentlighetströsklarna återspegla storleken och den övergripande riskprofilen samt karaktären, omfattningen och komplexiteten hos alla finansiella enheters tjänster. Målet är att skapa en konsekvent och proportionell metod för incidentrapportering som inte belastar mindre finansiella enheter på ett oproportionerligt sätt.

Denna förordning ska tillämpas från och med den 17 januari 2025.

1.2 Klassificeringskriterier

Förordningen anger kriterier för att klassificera incidenter som allvarliga. Dessa inkluderar följande:

1. Antal kunder och finansiella motparter som påverkas av incidenten. Antalet berörda kunder och finansiella motparter samt incidentens inverkan på affärsmål och marknadseffektivitet. Den finansiella enheten ska beakta hur påverkan på en kund eller en finansiell motpart kan inverka på uppfyllandet av enhetens verksamhetsmål samt incidentens möjliga inverkan på marknadseffektiviteten.

2. Påverkan på finansiella enheters anseende, det räcker med att ett av följande kriterier är uppfyllt. Incidentens synlighet i media, kundklagomål, förutsättningen att uppfylla lagstadgade krav till följd av incidenten och potentiell kundförlust. När finansiella enheter bedömer incidentens påverkan på anseendet ska de beakta hur mycket uppmärksamhet incidenten har fått eller sannolikt kommer att få i förhållande till varje angivet kriterium.

3. Varaktighet och tjänstavbrott. Hur länge incidenten pågår samt hur tjänstens tillgänglighet påverkas. Finansiella enheter ska mäta incidentens varaktighet från den tidpunkt den inträffar fram tills att den är löst. Om detta inte är möjligt, ska de mäta varaktigheten från när den upptäcktes, alternativt utföra skattningar.

4. Geografisk spridning. Incidentens påverkan på flera medlemsstater och betydelsen av effekterna i andra jurisdiktioner. Effekten ska baseras på kunder och finansiella motparter i andra medlemsstater, filialer eller andra finansiella enheter inom koncernen som verkar i andra medlemsstater, alternativt finansmarknadsinfrastrukturer eller tredjepartsleverantörer som kan påverka finansiella enheter i andra medlemsstater till vilka de tillhandahåller tjänster i den mån sådan information är tillgänglig.

5. Dataförluster. Finansiella enheter ska ta hänsyn till huruvida uppgifters tillgänglighet, äkthet, integritet och konfidentialitet påverkas.

6. Tjänsternas allvarlighetsgrad. Om incidenten påverkar kritiska eller viktiga funktioner eller finansiella tjänster.

7. Ekonomiska konsekvenser. Direkta eller indirekta kostnader och förluster som inträffar till följd av incidenten, inklusive stulna tillgångar, personalkostnader, avgifter på grund av att avtalsförpliktelser inte har fullgjorts, kostnader för gottgörelse och ersättning till kunder, förluster på grund av uteblivna intäkter, rådgivningskostnader, inklusive kostnader i samband med juridisk rådgivning, kriminaltekniska tjänster och saneringstjänster.

1.3 Allvarliga incidenter och väsentlighetströsklar

Förordningen specificerar väsentlighetströsklar som ska användas för att avgöra om en incident är allvarlig nog för att rapporteras:

- Trösklarna är avsedda att vara proportionella mot finansiella enheters storlek, riskprofil och komplexitet.

- Incidents ekonomiska konsekvenser och dess inverkan på verksamheten och kunder i andra medlemsstater är centrala i bedömningen.

- Återkommande incidenter med liknande grundorsaker kan betraktas som allvarliga om de tyder på brister i enhetens riskhanteringsförfaranden.

- Kriteriet för väsentlighet är uppfyllt för kunder, finansiella motparter och transaktioner om något av följande villkor är uppfyllda:

    1. Antalet påverkade kunder överstiger 10 % av alla kunder som använder den aktuella tjänsten,

    2. antalet påverkade kunder som använder den aktuella tjänsten överstiger 100 000,

    3. antalet påverkade finansiella motparter överstiger 30 % av alla finansiella motparter som är involverade i tillhandahållandet av den aktuella tjänsten,

    4. antalet påverkade transaktioner överstiger 10 % av det dagliga genomsnittet av transaktioner utförda av den finansiella entiteten i samband med den aktuella tjänsten och

    5. värdet av de påverkade transaktionerna överstiger 10 % av det dagliga genomsnittliga transaktionsvärdet som utförs av den finansiella entiteten i samband med den aktuella tjänsten, eller att kunder eller finansiella motparter har identifierats som relevanta.

- Om det faktiska antalet kunder eller finansiella motparter som påverkas eller det faktiska antalet eller den faktiska mängden transaktioner som påverkas inte kan fastställas, ska den finansiella entiteten uppskatta dessa på grundval av tillgängliga uppgifter från jämförbara referensperioder.

1.4 Användning och rapportering

För att säkerställa att incidentrapporter används effektivt för tillsyn och för att förhindra spridningseffekter inom finanssektorn, ska rapporterna omfatta detaljerade uppgifter om incidentens påverkan och de åtgärder som vidtagits. Incidenter som utgör personuppgiftsincidenter enligt GDPR ska rapporteras i enlighet med GDPR. Det innebär att finanssektorns aktörer måste följa GDPR-krav när personuppgifter är involverade i incidenten.

Sammanfattningsvis syftar förordningen till att förbättra den digitala operativa motståndskraften i EU-finanssektor genom att skapa en enhetlig och rättvis metod för rapportering av IKT-relaterade incidenter och cyberhot.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

2.1 Implementera ett incidenthanteringssystem

Det är av betydelse att införliva en incidentidentifiering och klassificering genom att säkerställa att det finnsmekanismer för att snabbt identifiera, klassificera och spåra IKT-relaterade incidenter. Wesslau Söderqvist Advokatbyrå rekommenderar en översyn av de rutiner och processer som krävs för att rapportera allvarliga incidenter till Finansinspektionen. Om en incident inträffar rekommenderas att dokumentera och övervaka antalet kunder och finansiella motparter som påverkas. Det är även av betydelse att bevaka incidentens påverkan på verksamhetens anseende, mäta och registrera varaktigheten samt driftstoppet för incidenten. Wesslau Söderqvist Advokatbyrå rekommenderar även att incidentens geografiska påverkan och dataförluster bedöms och dokumenteras vid en incident. Det är även av vikt att identifiera och kategorisera kritiska tjänster, bedöma incidentens påverkan på dessa och beräkna de ekonomiska konsekvenserna av incidenter.

2.2 Utveckla och implementera kontinuitets- och beredskapsplaner

Wesslau Söderqvist Advokatbyrå rekommenderar att befintliga beredskaps- och kontinuitetsplaner som hanterar potentiella IKT-relaterade incidenter och cyberhot ses över och kompletteras enligt DORA. Det är även av betydelse att säkerställa att tredjepartsleverantörer som påverkar verksamheten omfattas av kontinuitetsplaner och incidentrapportering. Detta kan kräva översyn av befintliga IKT-avtal.

2.3 Analysera och förbättra incidenthantering efter varje incident

Efter varje incident rekommenderar vi er att genomföra en detaljerad analys samt granska bolagets återkoppling och hantering. Det är även av relevans att identifiera och implementera förbättringar som är baserade på lärdomar från tidigare incidenter för att kunna stärka framtida hantering. Genom att följa dessa rekommendationer förstärks säkerställandet av efterlevnad av den delegerade förordningen och den operativa motståndskraften, samt minimeras riskerna för allvarliga incidenter.

Har ni frågor avseende de krav som ställs enligt ovan gällande incidenthantering eller om DORA generellt får ni gärna kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. slutgiltig rapport om förslag till tekniska tillsynsstandarder och tekniska genomförandestandarder för incidentrapportering

---

25 juli 2024

1 Inledning

Den europeiska tillsynsmyndigheten (ESA) har den 17 juli 2024 offentliggjort den slutgiltiga rapporten om förslag till tekniska tillsynsstandarder (RTS) och förslag till tekniska genomförandestandarder (ITS) i enlighet med förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA). I detta nyhetsbrev informerar vi om innehållet i RTS och ITS för hur incidenter ska rapporteras.

De slutgiltiga förslagen kommer att träda i kraft efter att de har antagits av Europeiska kommissionen och publicerats i Europeiska unionens officiella tidning.

För att förhindra potentiella spridningseffekter inom ramen för DORA, bör rapportering om större incidenter som lämnas in av finansiella enheter till behöriga myndigheter ge väsentlig och uttömmande information om incidenten på ett enhetligt och standardiserat sätt. Innehållet i den initiala anmälan bör begränsas till den mest väsentliga informationen för att undvika otillbörlig rapporteringsbörda för den finansiella enheten. De föreslagna ändringarna avser tidsgränser vid rapportering av den initiala anmälan, delrapporten och slutrapporten. ESA föreslår även en aggregerad rapportering på nationellt plan för finansiella enheter som endast övervakas av en behörig myndighet, förutsatt att vissa villkor är uppfyllda.

ESA har i samråd med Europeiska centralbanken och Europeiska unionens cybersäkerhetsbyrå:

- Utarbetat förslag till RTS som fastställer innehållet i rapporterna för IKT-relaterade incidenter och anmälan av betydande cyberhot samt tidsgränserna för finansiella enheter att rapportera dessa incidenter till behöriga myndigheter.

- Utarbetat förslag till ITS som fastställer standardformulär, mallar och tillvägagångssätt för finansiella enheter att rapportera en större IKT-relaterad incident eller anmäla ett betydande cyberhot.

Innehållet i RTS och ITS beskrivs ytterligare nedan.

2 Förslag till tekniska tillsynsstandarder (RTS)

Förslagen till RTS specificerar rapportering av större IKT-relaterade incidenter och anmälan om betydande cyberhot. Förslagen innehåller tidsgränser för när finansiella enheter har skyldighet att rapportera incidenterna till behöriga myndigheter. ESA:s förslag syftar till att harmonisera och effektivisera kraven på incidentrapportering och säkerställa att behöriga myndigheter får nödvändig information för att vidta tillsynsåtgärder samt förhindra spridningseffekter.

Rapporteringskrav

Finansiella enheter ska lämna tre typer av rapporter vid större incidenter, en initial anmälan, delrapport och slutrapport. Initialanmälan ska innehålla grundläggande information om incidenten och ska lämnas in snarast, senast fyra timmar efter klassificeringen av en större incident. Delrapporten ska innehålla utförligare information och lämnas in inom 72 timmar efter initialanmälan. Den slutgiltiga rapporten ska lämnas in inom en månad efter den senaste delrapporten och ska innehålla en fullständig beskrivning av incidenten samt redovisa de åtgärder som har vidtagits.

Rapporterna

Den initiala anmälan ska innehålla grundläggande information genom incidentreferenskod, upptäckts- och klassificeringstid, beskrivning av incidenten och klassificeringskriterier. Delrapporten ska bestå av datum- och tidsdetaljer för incidentens uppkomst, på vilket sätt incidenten har påverkat funktionellt område, hot och tekniker som har använts, samt information om tillfälliga åtgärder. Den slutgiltiga rapporten ska bestå av incidentens grundorsak, återställningstider, åtgärder för att förhindra framtida incidenter och ekonomisk påverkan. Rapporteringstidsgränserna syftar till att ge behöriga myndigheter effektiv information samtidigt som de finansiella enheterna får tillräckligt med tid för att hantera och rapportera incidenten på ett korrekt tillvägagångssätt. Tidsfristerna tar hänsyn till helger och bankhelgdagar och det finns undantag för mindre betydande finansiella enheter för att undvika onödig arbetsbörda.

Incidentrapportering om betydande cyberhot är frivilligt och den ska innehålla mindre omfattande information. Informationen ska inkludera hotets ursprung, potentiell påverkan och åtgärder som har vidtagits för att förhindra hotet. ESA:s förslag syftar till att skapa en enhetlig och effektiv rapporteringsstruktur för att stärka den digitala operativa motståndskraften för större IKT-relaterade incidenter och cyberhot inom EU:s finanssektor.

3 Förslag till tekniska genomförandestandarder (ITS)

ESA:s förslag fastställer tekniska standardformulär, mallar och förfaranden för hur finansiella enheter ska rapportera större IKT-relaterade incidenter och anmäla betydande cyberhot enligt DORA. Förslagen eftersträvar att harmonisera och förbättra kvaliteten på rapportering av IKT-relaterade incidenter och cyberhot inom den finansiella sektorn inom EU.

En standardiserad mall ska användas för att rapportera större IKT-incidenter i olika stadier. Finansiella enheter ska fylla i relevanta datafält i mallen för varje rapporteringsstadium och har möjlighet att fylla i informationen som krävs för senare stadier om den redan är tillgänglig. Informationen som återfinns i rapporterna måste vara korrekt. Om exakt data inte är tillgänglig vid tiden för rapportering, ska uppskattade värden baserade på tillgänglig information tillämpas. Finansiella enheter ska uppdatera tidigare lämnad information i del- och slutrapporter. Rapporterna ska lämnas genom säkra elektroniska kanaler som fastställs av den behöriga myndigheten. Om de etablerade kanalerna inte kan användas, ska finansiella enheter informera den behöriga myndigheten och använda andra säkra medel efter samråd med eller enligt tidigare överenskommelse med myndigheten. Om återkommande incidenter kumulativt uppfyller kriterierna för en större IKT-relaterad incident, ska finansiella enheter lämna aggregerad information om dessa incidenter.

Finansiella enheter som avser att låta någon annan sköta rapporteringsskyldigheten måste informera sin behöriga myndighet om det i förväg och lämna kontaktuppgifter till den tredje part som kommer att sköta rapporteringen. Tredje parts leverantörer kan skicka aggregerade rapporter om större incidenter som påverkar flera finansiella aktörer, förutsatt att vissa villkor är uppfyllda och att de behöriga myndigheterna har godkänt det.

För frivillig rapportering av betydande cyberhot ska en specifik mall användas och informationen ska vara fullständig och korrekt.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar finansiella aktörer att se över interna riktlinjer och processer för incidentrapportering. Allvarliga incidenter ska rapporteras inom fyra timmar och processen bör därför vara dokumenterad och innehålla en klar beskrivning över roller och ansvar vid en potentiell incident. Säkerställ också att IKT-avtal innehåller klausuler som ålägger IKT-leverantörer att bistå med bl.a. information vid en incident samt att IKT-leverantörer ska medverka till att begränsa potentiella skador. Wesslau Söderqvist Advokatbyrå bevakar

kontinuerligt utvecklingen för att genomföra DORA och avser att återkomma med mer information inom kort.

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