Till
Styrelsen i S:t Erik Försäkrings AB

Rapport för perioden 10 februari - 12 maj 2023 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.

- ESRB:s rapport om verktyg för cyberresiliens.
- Finansinspektionens handlingsplan för stärkt kontroll av utlagd verksamhet.
- Sanktionsbeslut mot Swedbank AB.
- Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2).

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)*
Outsourcing	Uppdragsavtal.	Kontrollen har inte föranlett några synpunkter.
	Uppdragstagare.	Kontrollen har inte föranlett några synpunkter.
Anpassning till nya och förändrade regelverk	EIOPA:s riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik	Kontrollen har inte föranlett några synpunkter.
	EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer	Kontrollen har inte föranlett några synpunkter.
Försäkringsverksamhet	Aktuariefunktionen.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Efterlevnad av reglerna om förmånsregister, försäkringstekniska avsättningar och reservsättning.	Kontrollen har inte föranlett några synpunkter.
	Efterlevnad av försäkringstekniska riktlinjer.	Kontrollen har inte föranlett några synpunkter.
	Efterlevnad av reglerna om återförsäkringsrisker.	Kontrollen har inte föranlett några synpunkter.

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.

Bolaget har tidigare genomfört ett arbete tillsammans med funktionen för regelefterlevnad för att se över och revidera samtliga anmälningspliktiga uppdragsavtal i syfte att säkerställa regelefterlevnad enligt ovan angivna regelverk. Framförallt har ändringar varit påkallade enligt EIOPA:s riktlinjer för molntjänster och IKT-riktlinjer. Samtliga uppdragsavtal som bedömts kritiska och viktiga för Bolagets verksamhet har anmälts till Finansinspektionen.

Utöver ovan har funktionen för regelefterlevnad informerats om att Bolagets internrevisor har haft synpunkter på den utförda kontraktsuppföljningen. Funktionen för regelefterlevnad har bedömt att Bolaget nu har goda rutiner för att följa upp sina uppdragstagare samt att uppföljning görs löpande.

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

Nya regelverk

Uppföljning och kontroll av Bolagets anpassning till dels EIOPA:s riktlinjer om informationssäkerhet, dels EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer. Kontrollen har syftat till att säkerställa att Bolaget har anpassat rutiner och processer efter riktlinjerna.

Som nämnts ovan har funktionen för regelefterlevnad bistått Bolaget med att anpassa verksamheten efter EIOPA:s riktlinjer. Arbetet är i princip klart, men fortsätter löpande i vissa delar avseende frågor rörande informationssäkerhet. Beträffande det senare har även Bolagets internrevisor sedan tidigare avgivit vissa synpunkter, som Bolaget för närvarande arbetar med.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen, men kommer fortsatt att följa arbetet med utvecklingen av processer rörande informationssäkerheten.

Försäkringsverksamhet

Uppföljning och kontroll avseende Bolagets regler för aktuariefunktionen. Kontrollen har syftat till att säkerställa att Bolagets riktlinjer är upprättade i enlighet med gällande regler.

Funktionen för regelefterlevnad har mottagit och granskat riktlinjerna utan några synpunkter.

Övrig regelefterlevnad

a) Uppföljning av Bolagets efterlevnad av reglerna för försäkringstekniska avsättningar och reservsättning. Kontrollen har syftat till att säkerställa ändamålsenliga rutiner och riktlinjer i enlighet med för Bolaget gällande regler avseende dessa områden.

   Bolaget har redogjort för arbetet och dess tillvägagångsätt avseende försäkringstekniska avsättningar och reservsättning. Funktionen för regelefterlevnad har vidare granskat relevanta styrdokument.

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

b) Uppföljning av Bolagets försäkringstekniska riktlinjer. Kontrollen har syftat till att säkerställa att de försäkringstekniska riktlinjerna är ändamålsenliga och har det innehåll som krävs enligt 10 kap. 23 § FRL och 9 kap. 17, 25-26 §§ Finansinspektionens föreskrifter och allmänna råd (FFFS 2015:8) om försäkringsrörelse.

   Funktionen för regelefterlevnad har mottagit och granskat Bolagets försäkringstekniska riktlinjer. Funktionen för regelefterlevnad bedömer att riktlinjerna uppfyller ovan ställda krav.

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

c) Uppföljning och kontroll avseende Bolagets riktlinjer för återförsäkringsrisker. Kontrollen har syftat till att säkerställa att Bolagets riktlinjer är upprättade i enlighet med gällande regler.

   Funktionen för regelefterlevnad har mottagit och granskat riktlinjerna utan några synpunkter.

Uppföljning av tidigare kontroller

Bolaget har tidigare informerat funktionen för regelefterlevnad om att man ser över olika alternativ för att eventuellt byta ut Bolagets dataskyddsombud för att på ett enklare sätt kunna säkerställa dataskyddsombudets oberoende.

Funktionen för regelefterlevnad rekommenderar fortsatt Bolaget att se över situationen med dataskyddsombudets oberoende. Dataskyddsombudet är nu att betrakta som alltför inskränkt med anledning av övriga roller i Bolagets verksamhet.

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 Styrelsemöten

Funktionen för regelefterlevnad har den 7 mars 2023 närvarat vid styrelsemöte hos Bolaget och därvid redogjort för bl.a. föregående års rapport.

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 12 maj 2023

Johan Grenefalk

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. ESRB:s rapport om verktyg för cyberresiliens

24 februari 2023

1 Bakgrund

The European Systemic Risk Board (ESRB) arbetar bl.a. med att förebygga och mildra risker för finansiell ostabilitet i händelse av en cyberincident. ESRB har i sitt arbete bl.a. rekommenderat inrättandet av ett paneuropeiskt ramverk för systematisk samordning av cyberincidenter i syfte att underlätta ett effektivt arbete vid en större cyberincident som drabbar flera finansiella institut och sträcker sig över landsgränser. ESRB fokuserar på det finansiella systemet som helhet och ESRB:s arbete kompletterar arbetet inom den EU-gemensamma kommittén för de europeiska tillsynsmyndigheterna som utförs inom ramen för DORA[1].

Wesslau Söderqvist Advokatbyrå har tidigare informerat om DORA, som bl.a. innehåller regler kring hotstyrda penetrationstester. Enligt ESRB innebär de tester som genomförs enligt DORA ett test av det ”första lagret” av finansiella aktörers försvar. ESRB menar dock att det behövs ytterligare försvarsläge för att öka motståndskraften mot cyberincidenter.

2 Rapportens innehåll

Rapporten som ESRB publicerat belyser behovet av att öka cyberresiliens. I rapporten uppmuntras myndigheter inom hela EU att göra olika framsteg enligt i) – iii) nedan.

i) *Cyber Resilience Scenario Testing* är ett analytiskt verktyg utformat för att hjälpa myndigheter att (i) testa respons- och återhämtningskapaciteten hos det finansiella systemet i allvarliga men troliga scenarier som involverar en cyberincident, (ii) utvärdera effekten av dessa scenarier på finansiell och operativ stabilitet, och (iii) identifiera områden där ytterligare arbete krävs för att minska cyberrisken. ESRB uppmuntrar myndigheterna att testa systemomfattande cyberresiliensscenariotester så snart som möjligt. Sådana pilottester kan komplettera andra analysverktyg som myndigheterna kan tänkas använda och fördjupa myndigheternas förståelse för riskerna för systemövergripande cyberresiliens.

[1] *Förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn.*

ii) *Systemic Impact Tolerance Objectives* är ett ytterligare analytiskt verktyg utvecklat för att identifiera och mäta effekterna av cyberincidenter på det finansiella systemet, och för att utvärdera när de sannolikt kommer att överträda toleransnivåerna och orsaka betydande störningar. Att definiera sådana mål kan hjälpa myndigheter att bedöma sin egen samordnings- och handlingsförmåga.

iii) *Financial Crisis management*, som rapporten tar hänsyn till i termer av hur väl myndigheterna hanterar systemomfattande cyberincidenter. ESRB konstaterar att effektiviteten hos befintliga verktyg för finansiell krishantering när det gäller att reagera på en cyberincident beror på hur allvarlig påverkan det är på det finansiella systemet och på hur snabbt den sprider sig.

ESRB lyfter i sin rapport att konsekvenser av en cyberincident kan materialiseras så snabbt att återhämtningsplaner riskerar att inte bli genomförbara i tid. Operativa kontinuitetsplaner kommer att aktiveras tidigare och kommer därför att vara mer relevanta i förebyggande syfte. Återhämtningsplaner och riktlinjer för affärskontinuitet bör vara väl integrerade i krishanteringsstyrningen.

ESRB lyfter också att DORA kommer att lägga grunden för ökad koordination, kommunikation och ökat samarbete för krishanteringsövningar som involverar behöriga myndigheter, resolutionsmyndigheter, ECB, Single Resolution Board, ESRB och ENISA[2]. Detta kommer vara ett viktigt led i att öka motståndskraften för cyberincidenter.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

ESRB kommer att fortsätta att arbeta med en EU-omfattande strategi för att hjälpa till att minska systemiska cyberrisker. ESRB kommer att fungera som ett nav för att dela framstegsrapporter och god praxis, och uppdatera det konceptuella tillvägagångssättet för scenarietester för cyberresilience för att dela erfarenheter och insikter från olika pilotprojekt. ESRB:s framtida arbete kommer också att innefatta att analysera operativa verktyg för finansiell krishantering för systemiska cyberkriser.

DORA är antagen och ska börja tillämpas av finansiella aktörer och IKT-leverantörer[3] i januari 2025. Wesslau Söderqvist Advokatbyrå ser dock ingen anledning till att avvakta med implementeringen av DORA och arbetet med att analysera vilka åtgärder som måste vidtas bör

[2] *European Union Agency For Cybersecurity.*
[3] *Leverantörer av kommunikations- och informationsteknik.*

påbörjas omgående. Finansiella aktörer kommer dels att omfattas av ett testramverk, dels ökade krav på övervakning av tredjepartsrisker. Enligt DORA kan myndigheter utveckla krishantering och beredskapsövningar och förhoppningsvis kan ESRB vara behjälpliga i denna typ av arbete. Wesslau Söderqvist Advokatbyrå ser väldigt positivt på den ambition som finns mellan organisationer och myndigheter att vilja utbyta information för att öka motståndskraften. Detta kommer även vara gynnande för de aktörer som omfattas av DORA och ska leva upp till kraven på bl.a. krishantering och beredskap.

Har ni frågor med anledning av det ovanstående eller behöver hjälp med att se över ert arbete för att implementera DORA är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Finansinspektionens handlingsplan för stärkt kontroll av utlagd verksamhet

---

2 mars 2023

1 Bakgrund

Allvarliga IT-incidenter hos finansiella aktörer, inklusive incidenter kopplade till utkontrakterad verksamhet, kan ha en negativ inverkan på den finansiella stabiliteten oavsett incidentens typ och dess eventuella syfte. Ett viktigt verktyg i Finansinspektionens tillsyn över de finansiella aktörerna och hur de hanterar IT-risker är därför tillsynen över utkontrakterade verksamheter hos tredjepartsleverantörer av IKT- och molntjänster.

Finansinspektionen har tidigare, i en rapport från våren 2022, konstaterat att det finns ett behov av en mer omfattande kontroll och bättre tillsyn över de finansiella företagens utlagda verksamheter. Sedan den rapporten har Europarlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn, nedan DORA, publicerats. Ett av DORA:s kärnområden är just utkontrakterad verksamhet och det kommer ställas högre krav på de finansiella aktörerna att identifiera och hantera tredjepartsrisker, inklusive risker i leverantörskedjor.

2 Behov av regeländringar och handlingsplan

Genom DORA ökar kraven avseende uppdragsavtal, utvärdering och uppföljning av tredjepartsleverantörer. De europiska tillsynsmyndigheterna har också fått i uppdrag att ta fram ett antal tekniska standarder för att ytterligare specificera detaljerna som relaterar till tredjepartsrisk, bl.a. detaljerade bestämmelser för den strategi för IKT-tredjepartsrisk som finansiella aktörer är skyldiga att anta. Förslagen till tekniska standarder ska överlämnas till Kommissionen senast den 17 januari 2024 och i vissa fall senast den 17 juni 2024. Finansinspektionen bedömer det som sannolikt att det kommer att finnas ett behov av nationella verkställighetsföreskrifter i vissa delar utan att nämna någon närmre redogörelse i detalj. Finansinspektionen kommer inte att lämna närmare förslag på förändringar i gällande svenska författningar förrän de tekniska standarderna publicerats.

Finansinspektionen meddelar avseende tillsyn att de fortsatt kommer att ha tredjepartsrisker som ett prioriterat tillsynsområde. Finansinspektionen kommer att utforma tillsynsmetoder för att på ett effektivt sätt granska företagens hantering av tredjepartsrisker. Exempelvis kommer

de register som ska föras enligt DORA ge Finansinspektionen en uppfattning om koncentrationsrisker inom företagen och en uppfattning om hur företagen följer upp utkontrakterad verksamhet. Detaljerade mallar avseende registerföring kommer att tas fram i en teknisk standard.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer som omfattas av DORA i god tid säkerställer att DORA efterlevs per den 17 januari 2025 då regelverket ska börja tillämpas. En del i detta arbete är att bl.a. se över och omförhandla avtal med IKT- och molntjänstleverantörer, vilket kan ta lång tid i vissa fall. Förhoppningsvis kommer DORA att leda till att det blir enklare för finansiella aktörer att ställa krav på tredjepartsleverantörer eftersom deras verksamheter kan påverkas även om de formellt inte omfattas av DORA.

Förutom att IKT-tredjepartsrisker ska hanteras innehåller DORA krav inom ett flertal områden. Dessa avser bl.a. följande:

- IKT-riskhantering och IKT-strategier.
- Processer för att upptäcka, hantera och rapportera IKT-relaterade incidenter.
- Informationsdelning och behörighetstilldelning.
- Program för testning av digital operativ motståndskraft. Det kan röra sig om sårbarhetsanalyser och skanningar, analyser av öppen källkod, nätverkssäkerhetsbedömningar, GAP-analyser, scenariobaserade tester, prestandatester och penetrationstester.
- Kunskap och kompetens.

Har ni frågor med anledning av det ovanstående eller behöver hjälp med att implementera DORA är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Sanktionsbeslut mot Swedbank AB

---

16 mars 2023

1 Inledning

Under april 2022 drabbades Swedbank AB, nedan Swedbank, av en IT-incident. Denna incident föranledde Finansinspektionen att undersöka hur Swedbank följt relevanta lagar, föreskrifter, interna rutiner och processer. Undersökningen visade att Swedbank inte hade haft en tillfredsställande intern kontroll vid ändringen i Swedbanks IT-system. Finansinspektionen har därför beslutat om att ge Swedbank en anmärkning förenad med en sanktionsavgift om 850 000 000 kronor. Nedan redogörs sammanfattningsvis för den incident som inträffat och Finansinspektionens bedömning i ärendet.

2 Incidenten och dess konsekvenser

Incidenten hos Swedbank föranleddes av att det genomfördes en ändring i ett IT-system för att banken skulle kunna hantera nya EU-sanktioner. Det aktuella IT-systemet är ett av de mest kritiska systemen som är av betydelse för Swedbanks verksamhet och det påverkar 49 olika drift- och affärskritiska tjänster. Trots systemets betydelse och potentiella påverkan på annan verksamhet i Swedbank efterlevdes inte de befintliga interna reglerna och processerna för hantering av ändringar i bankens IT-system, som bl.a. syftar till att minimera negativa effekter i verksamheten. Inte heller hade det genomförts någon risk- och konsekvensbedömning. Dessutom saknades det en återställningsplan. Hade Swedbank efterlevt interna regler och processer hade detta utförts.

Incidenten innebar att cirka 1,7 miljoner transaktioner till omkring 1,1 miljoner konton, som tillhörde närmare 960 000 kunder, stoppades. Den ursprungliga incidenten orsakade dessutom ett antal följdfel och ytterligare incidenter.

3 Reglering och Finansinspektionens bedömning

Kreditinstitut likt Swedbank ska identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som rörelsen är förknippad med. Kreditinstitut ska se till att det finns en tillfredsställande intern kontroll och det är styrelsen som ansvarar för att kraven efterlevs.

Andra finansiella aktörer under Finansinspektionens tillsyn omfattas av motsvarande näringsrättslig reglering.

Mot bakgrund av att ingen av bankens kontrollmekanismer förmått att fånga upp avvikelsen och säkerställa att processen följdes, trots att det handlade om ändringar i ett system som är ytterst centralt och verksamhetskritiskt för Swedbank. Ändringen som genomfördes var dessutom föranledd av yttre regelverkskrav som Swedbank behövde säkerställa att banken följde. Enligt Finansinspektionen visar detta tydligt att de kontrollmekanismer som fanns inte var ändamålsenliga på det sätt som krävs och Swedbank har således haft en bristande intern styrning och kontroll. Swedbank har visserligen redogjort för styrdokument, processer och rutiner för IT-ändringshantering och uppgett att det finns en omfattande uppföljning och intern kontroll. Det bedöms dock inte som tillräckligt att rutinerna är tillfredsställande utan även kontrollen av att rutinerna följs ska vara det.

Bland de omständigheter som är av betydelse vid prövning av ingripande och sanktionsavgift kan särskilt framhållas att den bristande interna kontrollen gällde en ändring i ett kritiskt IT-system och bidrog till en IT-incident som drabbade ett mycket stort antal personer. Härigenom har det i förlängningen funnits en risk för negativ påverkan på den finansiella stabiliteten. Samtidigt rör det sig inte om någon långvarig eller systematisk överträdelse. Finansinspektionen beaktar vid bedömningen av sanktionsavgiftens storlek även att Swedbank har vidtagit och avser att vidta åtgärder för att stärka sin interna kontroll efter incidenten. Vid en sammantagen bedömning om sanktionsavgiftens storlek, som ska bestämmas så att den står i proportion till den aktuella överträdelsens allvar, har Finansinspektionen beslutat om en avgift om 850 000 000 kronor. Det kan noteras att detta är ett belopp som ligger väl under den högsta möjliga avgiften i det aktuella fallet (7,1 miljarder kronor).

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Swedbank är ett systemviktigt institut och innefattas i Finansinspektionens högsta tillsynskategori. Detta ställer givetvis enormt höga krav på riskhantering och ju större och mer komplexa risker, desto högre krav på intern styrning och kontroll. Risker kan också ändras relativt snabbt, framförallt när det genomförs förändringar i organisationen eller i system. Wesslau Söderqvist Advokatbyrå rekommenderar därför att finansiella aktörer kontinuerligt identifierar risker i verksamheten och fastställer riskaptit samt aktivt arbetar med riskreducering och kontroller.

Risken för att utsättas för en IT-incident kan inte elimineras. Riskerna kan dock minimeras med relativt enkla medel. Beslutet visar bl.a. på vikten av att fastställda interna regler och processer

är väl förankrade bland medarbetare i verksamheten. Detta kräver bl.a. att medarbetare får den utbildning som krävs för att dels vara medvetna om de interna reglerna och processerna liksom externa regleringen, dels ha god insikt kring hur de ska tillämpas rent praktiskt. Beslutet visar även på hur IT- och informationssäkerhet inte bara är en fråga för IT-avdelningen, utan att ledningen ständigt behöver bedöma och kontrollera processerna. Wesslau Söderqvist Advokatbyrå rekommenderar därför att det regelbundet genomförs utbildningsinsatser för samtliga medarbetare och ledning för att minimera att incidenter inträffar. Även om medarbetarnas medvetenhet och kunskap är en viktig del fordras även komplettering i form av tekniskt stöd då man inte helt kan bortse från den mänskliga faktorn.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2)

---

16 mars 2023

1 Bakgrund

Digitaliseringen innebär att en allt större andel av samhällets aktiviteter i olika grad är beroende av nätverk och informationssystem. Den digitala utvecklingen ställer därmed krav på att informations- och cybersäkerhetsområdet ständigt utvecklas för att kunna säkerställa en hög säkerhetsnivå. För att öka säkerheten har EU nyligen antagit NIS2-direktivet, som ersätter det tidigare NIS-direktivet.[1] Det ursprungliga NIS-direktivet, som antogs år 2016, syftar till att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhetsarbetet i unionen. De leverantörer av samhällsviktiga tjänster som omfattas av direktivet är bl.a. tvungna att vidta lämpliga åtgärder för att hantera risker och incidenter i nätverks- och informationssystem. Direktivet har genomförts i svensk rätt genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) (NIS-lagen), förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster samt genom föreskrifter utfärdade av Myndigheten för samhällsskydd och beredskap (MSB).

Syftet med det NIS2 är att föreskriva minimiregler för ett samordnat regelverk inom unionen. NIS2 medför att kraven skärps bl.a. genom ett utökat tillämpningsområde, uppställda minimikrav för vilka åtgärder aktörer som omfattas måste vidta samt detaljerade sanktions- och ingripandebestämmelser.

Med anledning av detta har regeringen tillsatt en särskild utredning som senast den 23 februari 2024 ska presentera förslag på vilka anpassningar av svensk rätt som är nödvändiga för att kunna genomföra NIS2.[2] De huvudsakliga delarna som ingår i utredarens uppdrag redogörs för nedan.

---

[1] *Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS).*

[2] *Dir. 2023:30, Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (NIS2).*

2 Utredarens uppdrag

2.1 Utreda vilka aktörer som ska omfattas av regleringen

Inledningsvis har utredaren att ta ställning till vilka aktörer som ska omfattas. Som tidigare nämnts utökas tillämpningsområdet i NIS2 då fler sektorer kommer att omfattas än tidigare. I NIS2 är bl.a. offentlig förvaltning utsedd som en ny sektor. Översatt till svensk rätt innebär det att statliga myndigheter och regioner omfattas. Kommuner omfattas däremot inte per automatik utan det är upp till utredaren att överväga om det är en lämplig lösning att även de ska omfattas vid införandet i svensk rätt. Forskningssektorn är ytterligare en ny sektor i NIS2 som medför att utredaren måste ta ställning till om universitet och högskolor ska omfattas av regleringen. Ytterligare tillkommande sektorer är avloppsvatten, förvaltning av IKT-tjänster (mellan företag), rymden, post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkning och digitala leverantörer.

Entiteter som omfattas av NIS2 ska klassificeras antingen som väsentliga eller som viktiga entiteter, utifrån deras betydelse för den sektor de verkar inom eller den tjänst de tillhandahåller, liksom utifrån deras storlek.

2.2 Se över tillsynsmekanismen

Mot bakgrund av de nya krav som uppställs i NIS2 har utredaren i uppdrag att se över den tillsyn som utförts av nuvarande tillsynsmyndigheter samt vilka befogenheter dessa bör ha.[3] Utgångspunkten är att tillsynen i den mån det är möjligt bör utgå från samma struktur som finns idag. Viss förändring kan dock bli nödvändig med anledning av de tillkommande sektorerna. Utredaren har också i uppdrag att analysera vilka ändringar som krävs för att MSB i enlighet med NIS2 ska kunna fortsätta utöva uppdraget som nationell gemensam kontaktpunkt, CSIRT-enhet[4] och cyberkrishanteringsmyndighet samt deltagare i de samarbetsnätverk som direktivet ligger till grund för.

2.3 Analysera genomförandet av riskhanteringsåtgärder och incidentrapportering

NIS2-direktivet innehåller som tidigare nämnts minimikrav på åtgärder som de aktörerna som omfattas ska vidta. Kraven omfattar bl.a. rutiner för riskanalys och säkerhet i informationssystem, incidenthantering samt rutiner för kryptografi och, om det är lämpligt,

[3] *De nuvarande tillsynsmyndigheterna är Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket samt Post- och telestyrelsen.*
[4] *Behöriga myndigheter eller enheter för hantering av IT-säkerhetsincidenter (Computer Security Incident Response Teams).*

kryptering. NIS2 ålägger även medlemsstaterna att säkerställa att entiteterna har en fungerande incidentrapportering. Mot bakgrund av detta har utredaren i uppdrag att analysera hur kraven på riskhanteringsåtgärder och incidentrapportering ska genomföras i svensk rätt.

2.4 Analysera genomförandet av NIS2 i förhållande till sekretess och dataskydd

När entiteter uppfyller sina skyldigheter enligt NIS2, bl.a. vid incidentrapportering och tillsyn, kommer de att behöva tillhandahålla känslig information. Mot bakgrund av det krävs att det finns ett tillräckligt starkt skydd i svensk rätt för de uppgifter som ska rapporteras. När NIS-direktivet genomfördes konstaterades att bestämmelserna i offentlighets- och sekretesslagen (2009:400) (OSL), erbjöd tillräckligt skydd. Denna fråga behöver emellertid ses över igen inför genomförandet av NIS2 för att ta ställning till om befintliga bestämmelser uppfyller de nya kraven som uppställs.

Det framgår också av NIS2 att behandling av personuppgifter ska ske i enlighet med tillämpliga dataskyddsbestämmelser. Mot bakgrund av det ska utredaren också analysera vilken personuppgiftsbehandling som kan bli aktuell och om en sådan behandling har stöd i nuvarande reglering.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Förändringarna i NIS2 förväntas kunna implementeras i nationell lagstiftning i slutet av år 2024. Den som tror sig kunna omfattas av det nya regelverket bör i första hand kontrollera huruvida de bedriver verksamhet inom någon av de angivna sektorerna. De som omfattas av det nya regelverket bör påbörja planering för att lyckas uppnå efterlevnad till en försvarbar kostnad. Att tänka på är bl.a. att i) inleda samtal i ledningen för att ta upp frågan på agendan så tidigt som möjligt, ii) avsätta tid och resurser för att planera arbetet och identifiera behov av resurser, iii) planera budget för att ta höjd för implementering av åtgärder och en eventuell ny organisation, samt iv) utvärdera risker och åtgärder löpande.

NIS2 ger större ansvar till ledningen för säkerhetsåtgärder och övervakning av implementeringen. Ledningen kan hållas personligt ansvarig för bristande efterlevnad och sanktionen kan vara straffrättslig eller administrativ, vilket beslutas av medlemsstaterna. Beslut om en organisations riskaptit för informationssäkerhet är en fråga för ledningen, inte bara IT-avdelningen. Detta kan förväntas höja informationssäkerheten hos de berörda aktörerna.

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