Beslutsunderlag
Utfärdat: 2023-06-02
Diarienummer 0012/23

Handläggare: Petra Willquist

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

Rapport regelefterlevnadsfunktion kvartal 1

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar rapport från regelefterlevnadsfunktionen kvartal 1.

Sammanfattning

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

Bedömning ur ekonomisk dimension

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

Bedömning ur ekologisk dimension

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

Bedömning ur social dimension

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

Samverkan

Ingen samverkan har genomförts.

Bilagor

1. Rapport regelefterlevnadsfunktionen kvartal 1

Ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 1 2023.

För att ta del av rapporten hänvisas till bilaga 1.

Beskrivning av ärendet

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

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan.

Under kvartal 1 2023 har regelefterlevnadsfunktionen utförda kontroller inte föranlett någon anmärkning för bolaget. Det finns kvarstående anmälningar från kontroller 2021 där arbete pågår. Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för bolagets tillståndspliktiga verksamhet.

Göta Lejon arbetar löpande med att åtgärda utfärdade rekommendationer. Rekommendationerna uppdateras i bolagets styrnings- och ledningssystem Stratsys minst 2 gånger per år.

Bolagets bedömning

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

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 januari - 31 mars 2023 avseende regelefterlevnad

1 Inledning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senast genomförd kontroll av Försäkrings AB Göta Lejons, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen för regelefterlevnad har vidtagit under det första kvartalet 2023.

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

2 Händelser av relevans under perioden

2.1 Regelbevakning

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

- DORA-förordningen.
- IMY ger If Skadeförsäkring AB (publ) en reprimand.
- Dataskyddsombud varnar för brister i arbetet med GDPR.
- 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

GDPR

Uppföljning och kontroll av Bolagets personuppgiftshantering. Kontrollen har syftat till att säkerställa dels att Bolagets riktlinjer avseende personuppgiftshantering är upprättade enligt gällande regler, dels att Bolagets personuppgiftsregister är upprättat i enlighet med gällande regler.

Funktionen för regelefterlevnad har mottagit relevanta styrdokument avseende personuppgiftshantering samt Bolagets personuppgiftsregister och granskat dessa. Funktionen för regelefterlevnad har vidare tagit del av granskningsunderlag från Bolagets dataskyddsombud där vissa rekommendationer avgivits som Bolaget meddelat att man löpande arbetar med för att se över.

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

Rapportering

Uppföljning och kontroll av Bolagets rapportering till Finansinspektionen samt processen för ORSA-arbetet. Rapporten ska efter färdigställandet kommuniceras med Finansinspektionen.

Bolaget har redogjort för gällande rapporteringsrutiner samt att detta arbete huvudsakligen fungerar på ett bra och tillfredsställande sätt. Beträffande ORSA-rapporten så kommer underlag presenteras för styrelsen under året och i anslutning till detta kommer vissa scenarier i rapporten att diskuteras och ses över.

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

Övrig regelefterlevnad

Uppföljning och kontroll av Bolagets riktlinjer för riskhantering. Kontrollen har syftat till att säkerställa att Bolagets riktlinjer avseende riskhantering är upprättade enligt gällande regler.

Funktionen för regelefterlevnad har mottagit och granskat riktlinjerna.

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 Deltagande vid styrelsemöte

Funktionen för regelefterlevnad har den 26 januari 2023 deltagit vid styrelsemöte i Bolaget och därvid redogjort för föregående års årsrapport samt innevarande års årsplan.

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 24 april 2023

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 1, 2023

	Område	*Kontroll*	*Anmärkning*
	GDPR (fokuskontroll)	Hantering av personuppgifter.	Ingen anmärkning.
		Interna rutiner och riktlinjer för hantering av personuppgifter.	Ingen anmärkning.
	Rapportering	Rapportering till Finansinspektionen.	Ingen anmärkning.
	Övrig regelefterlevnad	Efterlevnad av regler för riskhantering.	Ingen anmärkning.

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

2 Översikt regelefterlevnad från föregående kontroller

	Kvartal	*Område*	*Kontroll*	*Anmärkning*
	Q3 2021	IT- och informations-säkerhet	IT-säkerhet och informationssäkerhet inkl. cyberrisker.	Se kommentar i 2.2 i kvartalsrapporten.
			Avbrottsfri verksamhet.	Se kommentar i 2.2 i kvartalsrapporten.
	Q3 2021	IKT-anpassning	IKT-riktlinje.	De interna riktlinjerna bedöms hålla en god miniminivå, dock behöver de interna riktlinjerna ses över mot bakgrund av den GAP-analys som genomförts av Transcendent Group AB där en rad brister identifierats.

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

3 Färggradering

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

Bilaga 2

Nyhetsbrev

Ang. DORA-förordningen

---

19 januari 2023

1 Inledning

Wesslau Söderqvist Advokatbyrå har tidigare informerat om förordningen om digital operativ motståndskraft i den finansiella sektorn, nedan DORA, som nu blivit slutligt antagen och ska börja tillämpas den 17 januari 2025. I syfte att uppnå en hög nivå av digital operativ motståndskraft fastställs krav i DORA avseende säkerhet i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser.

DORA omfattar som huvudregel försäkringsföretag. Försäkringsföretag kan dock undantas från DORA om förutsättningarna nedan är tillämpliga.

2 Undantag från tillämpningsområdet

Punkt 1

DORA är inte tillämpligt på försäkringsföretag som uppfyller **samtliga** följande villkor[1]:

a) Företagets årligen tecknade bruttopremieinkomster överstiger inte 5 miljoner EUR.

b) Företagets totala försäkringstekniska avsättningar brutto, inklusive belopp som kan återvinnas enligt återförsäkringsavtal och från specialföretag enligt artikel 76, överstiger inte 25 miljoner EUR.

c) Om företaget ingår i en grupp och gruppens totala försäkringstekniska avsättningar, inklusive de belopp som kan återvinnas brutto enligt återförsäkringsavtal och från specialföretag, inte överstiger 25 miljoner EUR.

d) Företagets verksamhet omfattar inte försäkrings- eller återförsäkringsverksamhet som täcker försäkringsrisker avseende åtagande av ansvar, kredit- och borgensförbindelser, såvida de inte utgör underordnade risker.

[1] *Samma villkor som gäller för undantag från Solvens II beroende på storlek.*

e) Företagets verksamhet omfattar inte återförsäkringsverksamhet som överstiger de tecknade bruttopremieinkomsterna med mer än 0,5 miljoner EUR, eller de försäkringstekniska avsättningarna brutto av belopp som kan återvinnas enligt återförsäkringsavtal och från specialföretag med mer än 2,5 miljoner EUR, eller de tecknade bruttopremieinkomsterna med mer än 10 procent eller de försäkringstekniska avsättningarna brutto av belopp som kan återvinnas enligt återförsäkringsavtal och från specialföretag med mer än 10 procent

Punkt 2

Om något av de belopp som anges under punkt 1 ovan överskrids under tre på varandra följande år ska DORA tillämpas från och med det fjärde året.

Punkt 3

Genom undantag från punkt 1 ska DORA tillämpas på alla företag som ansöker om auktorisation att bedriva försäkrings- och återförsäkringsverksamhet och vilkas årliga tecknade bruttopremieinkomster eller försäkringstekniska avsättningar brutto av belopp som kan återvinnas enligt återförsäkringsavtal och från specialföretag förväntas överskrida något av de belopp som nämns under punkt 1 inom de följande fem åren.

Punkt 4

Även Finansinspektionen ska kunna fastslå att DORA inte är tillämplig om vissa givna förutsättningar är uppfyllda.

3 DORA för mikroföretag och mindre företag

Om DORA ska tillämpas på verksamheten kommer rutiner och processer för bl.a. riskhantering, incidentrapportering, testning av IKT-system och outsourcingarrangemang ses över. Vissa lättnadsregler införs för s.k. mikroföretag, små företag och medelstora företag, vilka definieras nedan.

Mikroföretag

En finansiell entitet som har färre än tio anställda och en årsomsättning och/eller årlig balansomslutning som inte överstiger 2 miljoner EUR.

Litet företag

En finansiell entitet med tio eller fler anställda men färre än 50 anställda och en årsomsättning och/eller årlig balansomslutning som överstiger 2 miljoner EUR men som inte överstiger 10 miljoner EUR.

Medelstort företag

En finansiell entitet som inte är ett litet företag och som har färre än 250 anställda och en årsomsättning som inte överstiger 50 miljoner EUR och/eller en årlig balansomslutning som inte överstiger 43 miljoner EUR.

Wesslau Söderqvist Advokatbyrås rekommendationer

DORA har trätt i kraft och ska börja tillämpas den 17 januari 2025. Wesslau Söderqvist Advokatbyrå uppmuntrar finansiella entiteter att redan nu kontrollera om undantag från DORA enligt punkt 1 ovan är tillämpligt. Om undantag inte är tillämpligt ska samtliga moment i DORA efterlevas. Det finns dock vissa lättnadsregler och därför bör samtliga finansiella entiteter kontrollera om definitionen för mikroföretag eller litet och medelstort företag är tillämplig. Först därefter går det att utföra en analys av i vilken utsträckning som DORA kommer att påverka den enskilda verksamheten. Utifrån riskanalysen kan därefter en åtgärdsplan tas fram i god tid för att säkerställa att riskerna kan hanteras på ett ändamålsenligt sätt. Wesslau Söderqvist Advokatbyrå kan vara behjälplig i detta arbete.

Wesslau Söderqvist Advokatbyrå kommer fortsätta att bevaka lagstiftningsarbetet kring DORA och de tekniska standarderna som ska tas fram och ännu inte är publicerade.

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

Nyhetsbrev

IMY ger If Skadeförsäkring AB (publ) en reprimand

---

24 januari 2023

1 Sammanfattning

Integritetsskyddsmyndigheten (IMY) har beslutat att ge If Skadeförsäkring AB (publ), nedan If, en reprimand enligt dataskyddsförordningen, nedan GDPR, eftersom If har skickat känsliga personuppgifter till en registrerad i ett e-postmeddelande utan att använda en tillräckligt säker krypteringslösning. If anses därför inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen.

2 Ärendet

En person har gjort gällande att hälsorelaterade personuppgifter har överförts genom ett e-postmeddelande utan att ha varit krypterade hela vägen från avsändaren till mottagaren, s.k. end-to-end-kryptering. IMY har på grund härav inlett en utredning för att fastställa om If har säkerställt en lämplig säkerhetsnivå i enlighet med artikel 32 i GDPR. Däri stadgas att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå till skydd för de uppgifter som behandlas. Den personuppgiftsansvarige ska därvid beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter. Lämpliga skyddsåtgärder omfattar bl.a.:

- Pseudonymisering och kryptering av personuppgifter.
- Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och tjänsterna.
- Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.
- Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Vid bedömning av den lämpliga säkerhetsnivån ska särskild hänsyn tas till de risker som behandlingen medför avseende oavsiktlig förlust eller obehörig åtkomst till personuppgifterna som behandlas.

Fastställandet av de lämpliga åtgärderna innebär inte en godtycklig bedömning, utan en bedömning som är adekvat utifrån den relevanta behandlingen. Det aktuella ärendet har handlat om överföring av känsliga personuppgifter. För sådana uppgifter skärps kraven avseende vilka tekniska och organisatoriska åtgärderna som påkallas.

När e-postmeddelanden skickas över internet har avsändaren eller mottagaren i allmänhet ingen kontroll över vilka datorer och servrar som meddelandet passerar längs vägen. En konsekvens av det är att alla som förfogar över utrustning som oskyddade e-postmeddelanden passerar kan ta del av dessa utan att vara behörig. En lämplig lösning för att förhindra detta är att kryptera e-postmeddelandet alternativt kryptera överföringen av e-postmeddelandet. Ett exempel på en krypteringslösning som kan användas är tvingande TLS, vilket också använts av If vid den aktuella överföringen. Meddelandet var dock endast krypterat mellan If och mottagarens operatör. Således har krypteringen upphört innan meddelandet nått den avsedda mottagaren. Det har därför inte varit fråga om end-to-end-kryptering.

Eftersom meddelandet upphört att vara krypterat innan det nått mottagaren har det förelegat en risk för att obehöriga kunnat ta del av innehållet i klartext. If anses därför ha försummat att skydda uppgifterna på ett erforderligt sätt. Eftersom det varit fråga om känsliga personuppgifter har försummelsen utgjort en beaktansvärd risk för ett integritetsintrång. IMY har därför funnit att If vid det aktuella tillfället har behandlat personuppgifter i strid med artikel 32.1 GDPR.

Även om överträdelser av artikel 32.1 i GDPR kan föranleda sanktionsavgift har det ansetts vara fråga om en mindre överträdelse och IMY har beslutat om att ge If en reprimand. Det har varit fråga om ett enstaka e-postmeddelande och If har arbetat med att förbättra säkerheten avseende krypteringen. Därutöver har If, efter att den registrerade påtalat bristen, utvecklat och lanserat en ny kommunikationslösning för If:s kunder.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att företag som behandlar personuppgifter genom överföringar över internet, såsom vid e-postkorrespondens, ser över att rutinerna för kryptering uppfyller kraven på lämplighet. Det är särskilt viktigt om behandlingen avser känsliga personuppgifter och när sådana uppgifter kommuniceras externt med kunder.

Det är inte säkert att en och samma teknik är förenlig med GDPR i olika verksamheter. Det krävs därför att personuppgiftsansvariga utför en riskanalys av den enskilda verksamheten och hur personuppgifter behandlas. Utgångspunkten måste därefter vara att utvärdera vilka åtgärder som måste vidtas. För att uppfylla kraven i GDPR räcker det dock inte med att implementera

funktioner för lämplig kryptering. Klara och tydliga rutiner måste finnas på plats som möjliggör för alla berörda medarbetare att bidra till företagets regelefterlevnad. Vikten av att rutinerna verkligen följs i verksamheten illustreras i IMY:s beslut som avser ett enstaka e-postmeddelande, vilket varit tillräckligt för att tillsynsmyndigheten skulle ingripa.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Dataskyddsombud varnar för brister i arbetet med GDPR

---

7 februari 2023

1 Bakgrund

Integritetsskyddsmyndigheten (IMY), publicerade år 2019 sin första undersökning om dataskyddsarbetet i praktiken i sin rapport ”Nationell integritetsrapport 2019”. IMY har nu publicerat en ny rapport, ”Dataskyddsarbetet i praktiken”, om förutsättningarna för arbetet med dataskyddsfrågor i de verksamheter som är skyldiga att ha dataskyddsombud. Denna rapport bygger på studier genomförda av IMY där dataskyddsombud i närmare 800 verksamheter har deltagit genom att svara på en enkät med frågor om deras arbete med dataskyddsfrågor. Frågorna behandlar bl.a. huruvida dataskyddsombudens resurser är tillräckliga, hur arbetet bör vara organiserat samt vilka de största utmaningarna är med deras arbete kring dataskyddsfrågor.

Studien syftar till att utreda hur väl frågor om integritet och dataskydd är integrerade i offentliga och privata verksamheter. Studien syftar även till att ge en bild av hur långt olika verksamheter kommit i sitt arbete med integritet och dataskydd. De huvudsakliga slutsatserna och påpekandena som framförs i rapporten är följande.

2 Rapportens innehåll

2.1 Tillräckligt med tid och rätt resurser viktigt för effektivt dataskyddsarbete

Det praktiska dataskyddsarbetet utförs till stor del av landets dataskyddsombud. Det kräver att det finns tillräckliga resurser för ombuden att kunna genomföra arbetet väl. Med resurser avses bl.a. tillgången till nödvändig information och tid för att utföra uppgifterna. Resultatet av studien i denna del visar att var fjärde dataskyddsombud inte har någon särskild tid avsatt för att arbeta med dataskyddsfrågor. Hälften av dataskyddsombuden anser att den avsatta tiden de har är tillräcklig. Sju av tio dataskyddsombud anser sig få tillräcklig utbildning och ha tillräcklig kompetens för sin roll.

Vad gäller den avsatta tiden för arbetet med dataskyddsfrågor framgår det av studien att en större andel dataskyddsombud i privata företag än i offentlig sektor anser sig ha tillräcklig tid avsatt för dataskyddsarbetet. Det framgår även att fler heltidsanställda än deltidsanställda dataskyddsombud anser sig ha tillräckligt mycket avsatt tid. IMY påpekar i denna del att det är

viktigt att alla landets dataskyddsombud får likvärdiga och tillräckliga förutsättningar för att kunna utföra sitt dataskyddsarbete väl.

Vad gäller utbildning och kompetensutveckling framhåller IMY att dataskyddsarbetet till sin karaktär ställer höga kunskapskrav på dataskyddsombuden. För att det ska vara möjligt att etablera en god dataskyddskultur är det nödvändigt att dataskyddsombuden får tillräcklig utbildning och kompetensutveckling. IMY noterar att det finns mer kvar att göra i vissa verksamheter på denna punkt för att resultatet ska vara tillfredsställande.

2.2 Systematiskt och kontinuerligt dataskyddsarbete

Jämfört med år 2019 är dataskyddsarbetet inne i en ny fas. Tidigare problem med att förstå och implementera dataskyddsförordningen (GDPR) i den egna verksamheten upplevs inte vara lika påtagliga nu. Resultaten från enkäten i denna studie tyder i stället på en uppfattning om att GDPR uppställer hinder för den egna organisationen vilket gör att det är problematiskt att få till fungerande rutiner och processer i dataskyddsarbetet. Resultaten av studien vittnar vidare om att fyra av tio dataskyddsombud anser att deras organisationer arbetar kontinuerligt och systematiskt med dataskyddsfrågor. Många dataskyddsombud upplever bristande engagemang och kunskap i organisationens ledning och upplever att de involveras för sent i projekt som rör dataskyddet.

Rapportens resultat ger en splittrad bild av hur situationen ser ut i olika organisationer. För att tillämpningen av GDPR ska vara väl fungerande krävs att såväl ledningen som den enskilda medarbetaren är införstådda i de riktlinjer och rutiner som organisationen har. Att många av dataskyddsombuden inte har kunskap om den egna organisationens interna riktlinjer och rutiner är oroväckande då de utgör förutsättningarna för att arbetet med personuppgifter ska kunna utföras. IMY påpekar att det finns ett tydligt samband mellan anmälda personuppgiftsincidenter och brist på förståelse, kunskap och acceptans hos medarbetarna i de organisationer där dessa inträffat. Därför påminner IMY om medarbetarnas eget ansvar att kontinuerligt utbilda sig för att säkerställa personuppgiftsbehandlingen.

2.3 Utmaningar med dataskyddsarbetet

Dataskyddsombuden som genomförde studien fick välja vilka utmaningar som de ansåg var de största med GDPR. Resultatet är att många dataskyddsombud anser att det är en utmaning att få till fungerande rutiner och processer, att reglerna i GDPR uppställer hinder för verksamheten och att ledningen i den egna organisationen har bristande engagemang och låg kunskap.

IMY anser sammantaget att utvecklingen är positiv gällande de svårigheter som funnits med att genomföra de krav som GDPR uppställer. I stället vittnar den nya studien om, som tidigare nämnts, att många dataskyddsombud upplever att GDPR:s bestämmelser hindrar arbetet i den egna organisationen. Detta ställer krav på alla nivåer i en organisation. IMY betonar att det är ledningen som fördelar och prioriterar resurser, sätter ambitionsnivån, anger tonen och beskriver vilka förväntningar som finns på medarbetarna vad gäller dataskyddsarbetet inom organisationen. Utan detta engagemang från ledningen kommer dataskyddsombuden fortsatt belastas tungt och verksamheten kommer att ha problem vad gäller att implementera och tillämpa dataskyddsreglerna på ett tillfredsställande sätt.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av den undersökning som genomförts och de resultat som IMY presenterar enligt ovan rekommenderar Wesslau Söderqvist Advokatbyrå att personuppgiftsansvariga tar ett helhetsgrepp om GDPR och ser över eventuella brister och behov av åtgärder. Följande frågor bör bl.a. beaktas; Hur ser ledningens arbete ut för att möta kraven i GDPR? Finns dataskyddsombud eller en utsedd person som arbetar med dataskyddsfrågor? Är interna riktlinjer uppdaterade? Har personalen fått utbildning? Är registerförteckningen uppdaterad? Finns personuppgiftsbiträdesavtal där det krävs? Behandlas känsliga personuppgifter? Vilka säkerhetsåtgärder vidtas? Denna typ av översyn bör genomföras med viss regelbundenhet.

Ledningen har det yttersta ansvaret för att GDPR är implementerat i verksamheten och efterlevs på ett ändamålsenligt sätt. För att undvika eventuella sanktioner är kunskap och kompetens om GDPR lika viktigt i ledningen som hos övriga anställda. Att regelbundet utbilda organisationen är ett effektivt sätt att öka medvetenheten kring GDPR.

För de personuppgiftsansvariga som bedömt det nödvändigt att ha ett dataskyddsombud är det ytterst viktigt att denne dels har den kunskap och kompetens som krävs, dels har de resurser som fordras för att kunna uppfylla sin funktion som dataskyddsombud på ett effektivt sätt. Detta är minst lika viktigt för de organisationer som saknar ett dataskyddsombud, men som har en utsedd ansvarig för dataskyddsfrågor i organisationen. Annars faller syftet med att ha denna funktion i verksamheten, vilket i sin tur kan öka sanktionsriskerna.

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

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.