Till
Styrelsen i S:t Erik Försäkrings AB

Rapport för perioden 1 januari - 9 februari 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.

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

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)*
Personuppgiftsbehandling (GDPR)	Hantering av personuppgifter samt interna rutiner och riktlinjer.	Bolaget bör se över dataskyddsombudets roll och oberoende enligt nedan.
Rapportering	Rapportering till Finansinspektionen.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Efterlevnad av regler för riskhantering.	Kontrollen har inte föranlett några synpunkter.

Personuppgiftsbehandling

Granskning av Bolagets interna rutiner och riktlinjer i syfte att säkerställa att Bolaget uppfyller kraven på personuppgiftshantering i enlighet med dataskyddsförordningen.

Funktionen för regelefterlevnad har begärt in och granskat dels Bolagets interna riktlinjer för personuppgiftshantering, dels information som tillhandahålls publikt på hemsidan. Bolaget har redogjort för interna rutiner och riktlinjer för hantering av personuppgifter och därvid informerat funktionen för regelefterlevnad om att några större förändringar inte har varit påkallade sedan funktionens senaste kontroll och att det inte inträffat några personuppgiftsincidenter.

Bolaget har vidare 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 Bolaget att se över situationen med dataskyddsombudets oberoende. Dataskyddsombudet är nu att betrakta som alltför inskränkt med anledning av övriga roller i Bolagets verksamhet.

I övrigt har kontrollen inte föranlett några synpunkter.

Rapportering

Granskning av Bolagets interna rutiner och riktlinjer för rapportering till Finansinspektionen. Kontrollen har syftat till att säkerställa att Bolaget vidtar rimliga åtgärder för att säkerställa ändamålsenlig rapportering till Finansinspektionen samt att det finns dualitet i Bolaget och rutiner för att rapportera till Finansinspektionen inom utsatt tid.

Vid mötet har Bolaget redogjort för Bolagets rutiner för att säkerställa ändamålsenlig rapportering i enlighet med ovan.

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

Övrig regelefterlevnad

Uppföljning av Bolagets riktlinjer för riskhantering. Kontrollen har syftat till att säkerställa att riktlinjerna är ändamålsenliga och har det innehåll som krävs enligt bl.a. försäkringsrörelselagen (2010:2043) och Finansinspektionens föreskrifter och allmänna råd (FFFS 2015:8) om försäkringsrörelse.

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.

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 9 februari 2023

Johan Grenefalk

Bilaga 1

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.