Beslutsunderlag
Utfärdat: 2023-11-01
Diarienummer 0012/23

Handläggare: Petra Willquist

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

Rapport regelefterlevnadsfunktion kvartal 3

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar rapport från regelefterlevnadsfunktionen kvartal 3.

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 3

Ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 3 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 3 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 två gånger per år.

Bolagets bedömning

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

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 juli - 30 september 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 tredje 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 tredje kvartal. Dessa finns återgivna i sin helhet i bilaga 2.

- Sanktionsavgift mot Spotify AB.
- Sanktionsavgift mot Bonnier News AB.
- Krav på IKT-riskhantering som kompletterar DORA.
- Beslut om adekvat skyddsnivå för USA.
- Sanktionsavgift mot Trygg-Hansa
- FiDA-förordningen.

2.2 Kontroll av Bolagets regelefterlevnad

Övrig regelefterlevnad

a) Uppföljning och kontroll av eventuella intressekonflikter samt hantering av potentiella intressekonflikter. Kontrollen har syftat till att säkerställa att potentiella intressekonflikter i verksamheten identifieras och hanteras.

   Intressekonflikter är en stående punkt på styrelsens agenda och följs således upp löpande samt dokumenteras. Därtill utför funktionen för regelefterlevnad en årlig uppföljning där samtliga anställda samt styrelsens ledamöter får rapportera potentiella intressekonflikter, vilket utförts under år 2023.

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

b) Uppföljning av Bolagets hantering av frågor rörande kunskap och kompetens i enlighet med lagen om försäkringsdistribution. Kontrollen har syftat till att säkerställa att det finns planering för utbildning samt att utbildning och erforderligt prov genomförs under respektive verksamhetsår.

   Bolagets anställda har genomfört erforderlig utbildning under året i enlighet med lagen om försäkringsdistribution samt erlagt godkända test. Utbildningen dokumenteras även av Bolaget för respektive anställd.

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

c) Uppföljning av kompetens och kunskapsnivå hos styrelsen (fit & proper) inkl. samlad kompetens. Kontrollen har syftat till att säkerställa att Bolaget årligen kontrollerar att ledamöterna i styrelsen uppfyller de ställda krav som Bolaget dokumenterat i underlaget för lämplighetsbedömning.

   Bolaget har redogjort för arbetet avseende styrelsens samlade kompetens samt de egenutvärderingar som utförs av ledamöterna. På uppdrag av Bolaget har funktionen för regelefterlevnad bistått vid utvärderingen och hållit intervjuer med samtliga nya ledamöter för att få en oberoende bild av nuläget samt var eventuella utbildningsinsatser är nödvändiga. Detta arbete har redovisats för styrelsen och en utbildningsplan har tagits fram.

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 25 oktober 2023

Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 3, 2023

	Område	*Kontroll*	*Anmärkning*
	Övrig regelefterlevnad	Intressekonflikter.	Ingen anmärkning.
		Kompetens och kunskapsnivå hos personalen (IDD).	Ingen anmärkning.
		Kompetens och kunskapsnivå hos styrelsen (fit & proper) inkl. samlad kompetens.	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- 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-riktlinjer.	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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. sanktionsavgift mot Spotify AB

---

3 juli 2023

1 Bakgrund

Under sommaren 2019 har Integritetsskyddsmyndigheten, nedan IMY, inlett ett tillsynsärende mot Spotify AB, nedan Spotify, där IMY granskat vilka processer och rutiner som Spotify tillämpat för att uppfylla kraven i artikel 15 dataskyddsförordningen, nedan GDPR, om kunders tillgång till personuppgifter. Tillsynen har inletts mot bakgrund av att IMY hade tagit del av klagomål från kunder till Spotify, dvs. de registrerade, som påstått att deras personuppgifter inte behandlats på sådant sätt att deras rätt till tillgång enligt artikel 15 GDPR varit uppfylld.

Rätten till tillgång enligt GDPR innebär att de registrerade har rätt att få reda på vilka personuppgifter som en verksamhet hanterar om personen i fråga samt att få information om hur uppgifterna används. IMY har konstaterat att det funnits brister i sättet som Spotify hanterat enskildas rätt till tillgång på. Det handlar främst om att Spotify inte informerat tillräckligt om hur uppgifterna använts i verksamheten. Mot bakgrund av denna brist har Spotify tilldelats en sanktionsavgift om 58 miljoner kronor.

2 Redogörelse för tillsynen

2.1 Tillhandahållande av information

Spotify har uppgett att bolaget vid tillfället för tillsynen tillhandahållit information i enlighet med GDPR via en onlinefunktion som möjliggjort tillgång på flera olika språk. Kunderna har informerats om lagringen på flera olika sätt. Informationen har varit tillgänglig online via Spotifys webbplats samt via en länk i samband med att Spotify tillhandahållit kunder en kopia av behandlade uppgifter. I detta hänseende har IMY konstaterat att Spotifys rutiner varit tillräckliga för att säkerställa att den registrerade vid begäran fått tillgång till uppgifterna.

2.2 Innehållet i lämnad information

Den information som Spotify har lämnat har varit generellt utformad och samma information har lämnats oberoende av vem som begärt tillgång till informationen. Mot bakgrund av det har IMY prövat om den information som lämnats varit tillräcklig.

2.2.1 Kategorier av personuppgifter, ändamål, mottagare och källa

Information som Spotify lämnat avseende ändamål med behandlingen, mottagare av personuppgifter och källor från vilka uppgifterna samlats in har delats in i olika kategorier av personuppgifter. Beskrivning av kategorierna har dock saknats och det har inte varit möjligt för de registrerade att förstå vilka personuppgifter som innefattats i de olika kategorierna. Det har därför inte heller varit möjligt för de registrerade att förstå för vilka ändamål som personuppgifterna har behandlats, från vilka källor som personuppgifterna hämtats eller vilka som varit mottagare av personuppgifterna. IMY har därför ansett att Spotify inte lämnat tillräckligt tydlig information om ändamålen med behandlingen, de kategorier av personuppgifter som behandlingen gällt, mottagare, eller källor från vilka uppgifterna samlats in som krävs för att uppfylla kraven i GDPR om registrerades rätt till tillgång. Spotify har därmed inte uppfyllt syftet att de registrerade ska vara medvetna om den behandling som sker av deras personuppgifter samt att de ska kunna kontrollera om behandlingen är laglig.

2.2.2 Lagringsperiod

Det krävs att de registrerade får information om hur länge personuppgifterna ska lagras. Spotify har bl.a. angett att personuppgifterna bevarats i 90 dagar, såvida inte längre period valts på grund av ett legitimt affärsskäl. Även denna information har varit generellt utformad och inte tydligt kopplad till en särskild kategori av personuppgifter. IMY har också noterat att det varit svårt för en registrerad att förstå vad som menas med ”legitimt affärsskäl” och att det därmed varit svårt att förstå hur länge uppgifterna lagrats. Därför har inte kraven i GDPR uppfyllts i detta hänseende heller. .

2.2.3 Tredjelandsöverföring

I rätten till tillgång av information ingår att den registrerade ska kunna få information om en eventuell tredjelandsöverföring skett av uppgifterna. Även i detta fall har Spotify tillhandahållit information som varit generellt utformad. IMY har konstaterat att detta varit otillräckligt för att uppfylla kraven i GDPR.

2.2.4 Bekräftelse på behandlingen och tillgång till kopia

Den registrerade har också rätt att få en bekräftelse för det fall personuppgifter som rör denne behandlas av Spotify samt att få en kopia av uppgifterna.

Eftersom Spotify behandlar en stor mängd personuppgifter har Spotify tagit fram särskilda rutiner för att hantera de registrerades rätt att erhålla registerutdrag genom att dela upp personuppgifterna i tre kategorier. IMY har konstaterat att informationen som Spotify lämnat i detta avseende varit tillräckligt tydlig för att den registrerade skulle kunna förstå hur uppdelningen av de tre kategorierna varit gjord och vad detta inneburit. IMY har dock belyst det faktum att det ska vara enkelt för den registrerade att begära ut uppgifterna, varför rutinen med de olika typerna inte får försvåra processen. IMY har i denna del kommit till slutsatsen att Spotifys rutiner med att tillhandahålla dessa uppgifter varit tillräckligt lättillgängliga för att uppfylla kraven enligt GDPR. Spotify har däremot brustit i sina rutiner vad gällt de beskrivningar som Spotify givit över utlämnade tekniska loggfiler. Dessa beskrivningar har som standard tillhandahållits på engelska, vilket inte ansetts tillräckligt.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Ett genomgående resonemang i IMY:s bedömning har varit att personuppgiftsansvariga måste ta hänsyn till vad syftet är med bestämmelserna om rätten till tillgång i GDPR. Det handlar om att de registrerade ska vara medvetna om att uppgifterna behandlas samt kunna kontrollera om behandlingen som sker är laglig. För att det ska vara möjligt krävs att personuppgiftsansvariga anpassar den information som lämnas till de registrerade i specifika situationer. Informationen får inte vara för generellt utformad. Informationen som lämnas ska vara koncis, klar, tydlig och lättillgänglig för att uppfylla de krav som finns i GDPR.

Wesslau Söderqvist Advokatbyrå rekommenderar att personuppgiftsansvariga ser över rutiner och processer för att säkerställa den registrerades rätt till tillgång. Vid en sådan genomgång bör särskilt säkerställas att rutinerna för utlämnande av uppgifter sker på ett sådant sätt att det är förenligt med syftet som beskrivits ovan samt att informationen som lämnas är koncis, klar, tydlig och lättillgänglig.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. sanktionsavgift mot Bonnier News AB

---

3 juli 2023

1 Bakgrund

Inom Bonnierkoncernen finns ett samarbete mellan Bonnier News AB, nedan Bonnier, och ett antal anslutna bolag som ingår i koncernen. De anslutna bolagen samlar in personuppgifter från sina kunder och personer som besöker bolagens webbplatser. Personuppgifterna överförs till två koncerngemensamma databaser, en kunddatabas och en beteendedatabas. I dessa databaser skapas profiler om enskilda personer. Uppgifter i beteendedatabasen och i kunddatabasen kan i vissa fall knytas samman. Till profilerna knyts även information hämtad från Bisnode Sverige AB.

Integritetsskyddsmyndigheten, nedan IMY, har beslutat att Bonnier ska betala en administrativ sanktionsavgift om 13 miljoner kronor. Beslutet grundas på att Bonnier bl.a. har använt sig av profilering av enskilda som skett i vinstsyfte både när profileringen skett för att visa anpassade annonser och när den skett för att lämna ut kontaktuppgifter för telefonförsäljning och postal marknadsföring. IMY har bedömt att Bonnier har överträtt artikel 6.1 i dataskyddsförordningen, nedan GDPR, vid sin behandling av personuppgifter som skett i syfte att visa anpassade annonser och att tillgängliggöra kontaktuppgifter till anslutna bolag för telefonförsäljning och direktmarknadsföring. Nedan lämnas en sammanfattning av tillsynen och rekommendationerna med anledning av beslutet.

2 Redogörelse för tillsynen

Tillsynen omfattar behandling av personuppgifter som sker genom att skapa profiler och tillgängliggörande av sådana uppgifter för de anslutna bolagen för att visa anpassade annonser. Tillsynen omfattar också behandling av personuppgifter, skapande av profiler och tillgängliggörande av uppgifter till de anslutna bolagen för att användas vid telefonförsäljning och direktmarknadsföring.

De anslutna bolagen får tillgång till kund- och beteendedatabaserna genom ett sökverktyg kopplat till beteendedatabasen där de anslutna bolagen kan beställa ett segment av kunduppgifter utifrån sina valda variabler. Därefter får de anslutna bolagen en kod som

möjliggör att de kan rikta marknadsföring. De anslutna bolagens behandling av personuppgifter omfattas inte av denna tillsyn.

2.1 Behandlingen utgör profilering

IMY har konstaterat att både den behandling av personuppgifter som skett för ändamålet att tillgängliggöra uppgifterna för anslutna bolag i syfte att visa anpassade annonser har innefattat profilering av registrerade enligt definitionen i artikel 4.4 i GDPR. Detta eftersom det varit fråga om automatisk behandling av personuppgifter som syftat till att kategorisera de registrerade utifrån deras tidigare beteendemönster vilket i sin tur gjort det möjligt att bedöma vissa av deras personliga egenskaper. Även behandlingen av personuppgifter som skett i syfte att tillgängliggöra kontaktuppgifter för telefonförsäljning och direktmarknadsföring innefattar profilering.

2.2 Rättslig grund

Bonnier har gällande rättslig grund angett att (i) Bonnier har ett berättigat intresse, (ii) behandlingen är nödvändig för det berättigade intresset och (iii) de registrerades intresse av skydd för sina personuppgifter väger inte tyngre, dvs. rättslig grund enligt artikel 6.1 f) GDPR. Intresset består enligt Bonnier i ett behov av att förstå kundernas och användarnas önskemål och behov för att kunna uppnå relevans i innehåll och annonsering som riktas mot kunder och användare och därigenom kunna erbjuda konkurrenskraftiga produkter/tjänster och attraktiva annonsytor. Behandling av personuppgifter för att visa anpassade annonser baserat på den enskildes profil är en grundförutsättning för att journalister och publicister ska kunna få intäkter och i förlängningen kunna bedriva journalistik. Bonniers intresse väger således tyngre än de registrerades enligt Bonnier.

2.3 IMY:s bedömning

Av European Data Protection Boards, nedan EDPB, riktlinjer om riktad annonsering i sociala medier framgår att när det gäller uppgifter som den registrerade aktivt och medvetet tillhandahållit så kan både samtycke och berättigat intresse utgöra en rättslig grund för behandlingen. Av riktlinjerna framgår dock att för sådan data som samlats in genom observation (exempelvis genom kakor) kan berättigat intresse inte fungera som en lämplig rättslig grund när den riktade annonseringen baseras på att enskilda spåras över flera webbplatser och platser.

IMY har ansett att Bonnier kan ha haft ett berättigat intresse då intresset varit lagenligt, verkligt och faktiskt. IMY har också funnit att kravet på nödvändighet varit uppfyllt eftersom hänsyn ska

tas till principen om uppgiftsminimering och Bonnier har vidtagit åtgärder för uppgiftsminimering och begränsning av hur länge uppgifter lagrats.

När det gäller frågan hur tungt detta intresse väger har IMY konstaterat att intresset i sig inte är journalistiskt, utan av kommersiell natur. Genom profileringen skapas kunskap om kunder och potentiella kunder som möjliggör intäkter från anpassad annonsering. IMY har bedömt att Bonniers och de anslutna bolagens kommersiella intresse inte väger så tungt som Bonnier påstår. IMY har ansett att profileringen varit omfattande till sin karaktär och att en sådan profilering inte är något en registrerad kan förvänta sig utan att ha samtyckt till sådan personuppgiftsbehandling. IMY har även ansett vid en sammanvägd bedömning att den registrerades integritetsintresse således väger tyngre. Behandlingen har därmed skett i strid med artikel 6.1 f) GDPR. Rättslig grund har även saknats då profilering skett baserad på de registrerades kompletterade kunddatabasprofiler i syfte att tillgängliggöra kontaktuppgifter till anslutna bolag för telefonförsäljning och marknadsföring.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

I en digitaliserad värld där datainsamling och datadriven teknik blir alltmer utbredd är det viktigare än någonsin att endast behandla personuppgifter om man har en rättslig grund. Varje personuppgiftsbehandling som utförs är laglig endast om det finns en rättslig grund för behandlingen enligt artikel 6 GDPR.

Wesslau Söderqvist Advokatbyrå rekommenderar att personuppgiftsansvariga löpande ser över personuppgiftsregistret där en rättslig grund för behandlingen ska framgå. Behandling av personuppgifter utan en rättslig grund kan få allvarliga konsekvenser både för individen vars uppgifter behandlas och för organisationen som är ansvarig för behandlingen.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Krav på IKT-riskhantering som kompletterar DORA

---

7 juli 2023

1 Bakgrund

ESA har inlett ett samråd om ett av utkasten till tekniska standarder som ska komplettera DORA.[1] Föremål för detta nyhetsbrev är två av fyra nya förslag till tekniska standarder (RTS) som ESA tagit fram.[2] Båda förslagen rör IKT-riskhantering. Enligt utkasten finns det vissa policys och regler som aktörer som omfattas av DORA måste upprätta, men vilka som blir tillämpliga beror på vilken klassificering som aktören i fråga har enligt DORA.

IKT-riskhantering

Aktörer som omfattas av art 15 DORA omfattas av Del I i förslaget till RTS om IKT-riskramverk. För dessa aktörer kan ett flertal policys behöva upprättas om ESA:s första utkast antas, se avsnitt 2 nedan.

Förenklad IKT-riskhantering.

Vissa bolag, baserat på verksamheternas omfattning och komplexitet, omfattas av DEL II i RTS-förslaget om IKT-riskhantering samt lättare krav och undantag. De ska enligt art 16 DORA upprätta ett förenklat ramverk för IKT-riskhantering. För den förenklade IKT-riskhanteringen ställs krav på nödvändiga åtgärder för att effektivt hantera IKT-risker. Med undantag för informationssäkerhetspolicyn ska inga nya policys upprättas utan reglerna i utkastet ska komplettera befintlig IKT-riskhanteringsram enligt DORA, se avsnitt 3 nedan.

2 IKT-riskhantering

2.1 Policy om IKT-riskhantering (art 3 RTS om riskramverk)

En policy om ISK-riskhantering bör upprättas och läsas i enlighet med art 8 DORA. Policyn möjliggör för aktörer att effektivt bedöma och hantera exponering för IKT-risker och således även att proaktivt minska risker för intrång och missbruk av data och säkerställa övergripande

[1] *Förordningen om digital operativ motståndskraft inom den finansiella sektorn.*
[2] *Övriga utkast till tekniska standarder är RTS om kriterier för klassificering av IKT-relaterade incidenter och RTS om specificering av policyn för IKT-tjänster som utförs av tredjepartsleverantörer av IKT.*

nätsäkerhet. Det möjliggör även en korrekt dataöverföring utan onödiga avbrott och förseningar.

Policyn ska omfatta nödvändiga riktlinjer och förfaranden för att effektivt hantera IKT-risker. En metod för att genomföra IKT-riskhanteringen bör fastställas. Metoden ska dels möjliggöra upptäckt av sårbarheter och hot som kan påverka affärsfunktioner, IKT-system och stöttande IKT-tillgångar, dels innehålla indikatorer för att mäta effekt och sannolikhet för att sårbarheter och hot inträffar. Godkända risktoleransnivåer för varje identifierad risktyp ska definieras.

De IKT-risker som kvarstår trots åtgärder ska identifieras och integreras i riskhanteringsprocessen. Utöver det ska en plan upprättas för inventering av IKT-risker inklusive en förklaring till varför de accepteras. Även roller och ansvar för acceptansen av de kvarvarande IKT-riskerna som överskrider aktörens bestämda risktoleransnivå ska tilldelas.

Finansiella aktörer måste minst en gång om året se över och anpassa IKT-riskhanteringen till potentiella affärsstrategiska förändringar och strategier för digital motståndskraft. Ytterligare granskning fordras vid betydande förändringar i IKT-tjänster eller IKT-tillgångar som stöder affärsfunktioner.

2.2 Policy för hantering av IKT-tillgångar (art 4 RTS om riskramverk)

Finansiella aktörer ska implementera en policy för hantering av IKT-tillgångar i syfte att bevara tillgänglighet, autenticitet, integritet och konfidentialitet för data. Policyn ska föreskriva övervakning och hantering av livscykeln på IKT-tillgångar som är identifierade och klassificerade i art 8.6 DORA om krav på inventering av IKT-tillgångar och informationstillgångar.

Dessutom ska policyn innehålla föreskrifter om att den finansiella enheten ska föra ett register vilket bland annat ska innehålla olika IKT-tillgångar samt deras klassificering, identitet och affärsfunktioner.

2.3 Policy för kryptering och kryptografiska kontroller (art 6 RTS om riskramverk)

Finansiella aktörer ska upprätta en omfattande policy för kryptering och kryptografiska kontroller. Policyn ska upprättas i syftet att upprätthålla skydd för integritet, autenticitet och tillgänglighet avseende IKT-system och data.

Policyn ska innehålla centrala element för att säkerställa en effektiv hantering av säkerhetsåtgärder. Det ska finnas regler för olika säkerhetsåtgärder, däribland om kryptering av data, hur data som inte kan krypteras ska behandlas avskilt, hur interna nätverksanslutningar krypteras. Det ska även finnas regler om trafik med externa parter, hantering av kryptonycklar

och kriterier för val av kryptografiska tekniker och hur de används med beaktande av bland annat ledande praxis. De mest effektiva metoderna utifrån omständigheterna bör eftersträvas. Policyn behöver innehålla bestämmelser om övervakning av utvecklingen inom kryptoanalys, vilket kan leda till att tekniken för att vara motståndskraftig mot cyberhot kan komma att behöva uppföljas och revideras.

2.4 Policy för hantering av kryptonycklar (art 7 RTS om riskramverk)

Finansiella enheter ska upprätta en policy för hantering av kryptonycklar som en integrerad del av den övergripande krypteringspolicyn. Policyn ska bestå av riktlinjer för skydd och hantering av kryptonycklar genom hela livscykeln samt hur de på ett säkert sätt ska genereras, lagras, distribueras och bortskaffas. Dessutom ska policyn innehålla metoder för hur kryptonycklar ska återställas om de förloras.

Kryptografisk teknik bör uppdateras eller ändras när det är nödvändigt för att förbli motståndskraftiga mot cyberhot. Om uppdatering inte är möjlig bör alternativa åtgärder antas.

2.5 Policy för IKT-säkerhet (art 8-12 RTS om riskramverk)

Finansiella enheter ska upprätta en IKT-säkerhetspolicy. Den ska bland annat innehålla en policy för hantering av driften av IKT-tillgångar i syfte att säkerställa säkerhet i nätverk mot intrång och missbruk av data. Policyn ska innehålla beskrivningar av IKT-system såsom installation, underhåll, avinstallation och hantering av informationstillgångar. Den ska även innehålla olika krav på kontroll och övervakning av IKT-system samt felhantering.

För IKT-säkerheten tillkommer även krav på identifiering och hantering av kapaciteten på IKT-system, sårbarhetshantering för intrång, införande av riktlinjer för data- och systemsäkerhet samt dokumentering av förfaranden, protokoll och verktyg för loggning.

2.6 Policy för IKT-projektledning (art 15-17 RTS om riskramverk)

Policyn ska omfatta projektmål, projektstyrning som roller och ansvarsområden, projektplanering, riskbedömning av projektet, milstolpar, krav på förändringshantering och testning av alla krav vid driftsättning av ett IKT-system. För arbetat med IKT-projekt ska det finnas personal som har nödvändig kunskap och som representerar affärsområdena eller funktionerna som kommer påverkas av projektet. Projekt som påverkar viktiga funktioner och risker kopplade till projektet ska regelbundet rapporteras till ledningen.

Policyn är till för att skydda nätverk mot intrång och missbruk. Det görs genom att maximera fördelar förknippade med projekt, förvärv och förändringar och minimera negativa effekter som kan uppstå av sådana åtgärder.

2.7 Policy om förvärv, utveckling och underhåll av IKT-system (art 16 RTS om riskramverk)

Policyn som finansiella enheter ska upprätta ska fokusera på testning av systemet och vilka säkerhetsåtgärder som bör antas utifrån testerna. Policyn ska identifiera säkerhetspraxis, säkerhetsmetoder och funktionella samt icke-funktionella krav i samband med förvärv, utveckling och underhåll av IKT-system. Dessutom ska åtgärder definieras för hur risker, oavsiktliga ändringar och avsiktlig manipulation kan undvikas.

Policyn ska innehålla regler för hur IKT-system, genom olika metoder och i olika omfattning beroende på riskernas storlek, ska testas och godkännas före användning och efter underhåll eller utveckling. Testerna ska utföras i en miljö åtskild från produktionsmiljön. Policyn ska även innehålla ytterligare krav på hur testerna ska gå till för att skydda integritet och sekretess för data.

2.8 Policy för säkerhet i den fysiska omgivningen (art 18 RTS om riskramverk)

Policyn som ska upprättas syftar till säkra lokaler, datacenter, särskilt känsliga områden och hårdvarututrustning. Genom att säkra det kan IKT-tillgångar skyddas från obehörig åtkomst, attacker, olyckor och andra faror. Policyn ska anpassas utifrån risker och den hotbild som finns för IKT-tillgångar.

Policyn ska innehålla proportionella åtgärder för att skydda anläggningar, datacenter och känsliga enheter där IKT-tillgångar finns. Dessutom ska det framgå hur IKT-tillgångarna säkras. Policyn ska också innehålla en skrivbordspolicy för papper och en skärmpolicy för anläggningar för informationsbehandling.

2.9 Policy för personalpolitik (art 20 RTS om riskramverk)

Policy om personalpolitik och åtkomstkontroll ska innehålla identifiering och ansvarsfördelning för olika ansvarsområden för informationssäkerhet och krav på personal och tredjepartsleverantörer av IKT-tjänster. Kraven består av att de ska informeras om och följa den finansiella enhetens IKT-policys, rapporteringsrutiner för upptäckt av avvikande aktivitet samt krav på återlämnande av IKT-tillgångar vid upphörande av anställning.

2.10 Policy för identitetshantering (art 21 RTS om riskramverk)

Identitetshantering säkerställer identifiering och autentisering av vilka fysiska personer och system som har åtkomst till den finansiella aktörens information, vilka ska finnas med i en policy om identitetshantering. Policyn ska innehålla riktlinjer om att varje identitet, anställd eller tredjepartsleverantör ska ha ett unikt användarkonto till den finansiella enheten. Det ska även

finnas riktlinjer om användarkontons livscykelhantering, dvs. när de skapas, ändras, förnyas, inaktiveras och avslutas.

2.11 Policy för åtkomstkontroll (art 22 RTS om riskramverk)

En policy för åtkomstkontroll ska upprättas och skydda mot obehörigas åtkomst till information och system. Policyn ska innehålla riktlinjer för vilka som ska få åtkomst till IKT-tillgångar. Vilka som får åtkomst ska baseras på behovet av tillgång eller användning av informationen. Policyn ska även innehålla riktlinjer om hur användningen ska begränsas och hur detta kontrolleras samt hur man kan bevilja, ändra eller återkalla åtkomsträttigheter. Det ställs flera detaljerade krav på åtkomstkontroller och kontohantering, vilka också finnas med i policyn.

2.12 Policy för hantering av IKT-relaterade incidenter (art 23 RTS om riskramverk)

En policy ska upprättas för att införa riktlinjer om att IKT-relaterade incidenter och hanteringsprocesser ska dokumenteras och bevis ska bevaras i den mån det är nödvändigt. Det ska även finnas en lista över involverade i IKT-verksamhetens säkerhet. Policyn ska även innehålla riktlinjer om vilka mekanismer som ska inrättas för att analysera mönster för återkommande IKT-relaterade incidenter.

2.13 Komponenter till kontinuitetspolicyn (art 25 RTS om riskramverk)

I utkastet föreslås minimiförslag på komponenter som ska finnas i kontinuitetspolicyn enligt art 11(1) DORA, bland annat föreslås att kontinuitetspolicyn ska innehålla olika definitioner och beskrivningar för kontinuitetsplanen, dess omfattning, begränsningar, tidsramar, kriterier för att aktivera kontinuitetsplaner samt bestämmelser om exempelvis styrning, organisation och anpassning av kontinuitetspolicyn.

3 Förenklad IKT-riskhantering

3.1 Informationssäkerhetspolicy (art 32 RTS om riskramverk)

Finansiella enheter ska upprätta en informationssäkerhetspolicy för att fastställa övergripande mål, principer och riktlinjer för tillgänglighet, äkthet, integritet och konfidentialitet av information.

Policyn ska fastställa och genomföra IKT-säkerhetsåtgärder för att minska exponering för IKT-risker. Säkerhetsåtgärderna består bland annat av att IKT-tillgångar ska klassificeras så att

lämpliga säkerhetsåtgärder kan vidtas. Andra säkerhetsåtgärder är bland annat hantering av IKT-relaterade incidenter, åtkomstkontroll, fysisk säkerhet, miljösäkerhet och IKT-driftsäkerhet.

3.2 Komponenter som kompletterar IKT-riskhanteringsramen

Styrning och organisation (art 30 RTS om riskramverk)

Det ska tilläggas regler som säkerställer att ledningsorganet bär det övergripande ansvaret för IKT-riskhanteringsramverket. Ledningsorganet ska fastställa tydliga roller och ansvar, mål för informationssäkerhet och IKT-krav. De ska även godkänna och regelbundet granska informationstillgångar, risker, konsekvensanalys och planer för kontinuitet samt utbilda personal i tillräcklig mån för att förstå och bedöma IKT-risker.

Identifiering och klassificering (art 32 RTS om riskramverk)

Finansiella enheter ska identifiera, klassificera och dokumentera kritiska eller viktiga funktioner, informationstillgångar och IKT-tillgångar som stöder verksamheten. Även kritiska funktioner som stöds av tredjepartsleverantörer av IKT-tjänster ska identifieras.

IKT-riskhantering (art 33 RTS om riskramverk)

Finansiella enheter ska regelbundet bedöma IKT-risker, fastställa risktoleransnivåer, ta fram riskreduceringsstrategier och följa upp IKT-riskerna vid större förändringar.

Fysisk och miljömässig säkerhet (art 34 RTS om riskramverk)
Finansiella enheter ska identifiera säkerhetsåtgärder för IKT-risker som exempelvis åtkomst och stöld. Därför ska åtgärder vidtas för att säkra lokaler, datacenter, servrar, nätverk och andra kritiska tillgångar.

Åtkomstkontroll (art 35 RTS om riskramverk)

Finansiella enheter ska införa rutiner för åtkomstkontroll som regelbundet ska ses över. Rutinerna ska definiera åtkomsträttigheter och kritiska platser, utforma ett användaransvar och ett förfarande för kontohantering samt införa proportionerliga autentiseringsmetoder.

Säkerhet för IKT-verksamhet (art 36 RTS om riskramverk)

Finansiella enheter ska bland annat bevaka och hantera livscykeln för IKT-tillgångar, se till att IKT-tillgångar stöds av leverantörer, identifiera kapacitetskrav och åtgärder för att förbättra

tillgängligheten, utföra sårbarhetsskanning och andra åtgärder för att upptäcka hot eller dataintrång.

Säkerhet för data, system och nätverk (art 37 RTS om riskramverk)

Finansiella enheter ska införa skyddsåtgärder för att säkerställa nätverkssäkerhet och motverka intrång och missbruk av data, bland annat genom åtgärder för att skydda data i olika delar av livscykeln, åtgärder för att förhindra och upptäcka obehöriga anslutningar till nätverk, åtgärder för att radera data på lokaler eller enheter där de inte behövs och åtgärder för att säkerställa att distansarbete och användning av privata enheter inte äventyrar säkerheten.

Testning av IKT-säkerhet (art 38 RTS om riskramverk)

En plan för att testa IKT-säkerheten ska införas och tester ska göras med beaktning av verksamhetens övergripande riskprofil. Testerna ska övervakas och utvärderas.

Förvärv, utveckling och underhåll av IKT-system (art 39 och 40 RTS om riskramverk)

En metod för förvärv, utveckling och underhåll av IKT-system ska införas. Metoden ska bland annat säkerställa att krav på informationssäkerhet följs vid utveckling av IKT-system, säkerställa testning och godkänna IKT-system innan de implementeras och identifiera åtgärder för att minska riskerna. Utöver det ska roller och ansvar vid de olika tidpunkterna under IKT-projektledning eller förändringar definieras.

Kontinuitetshantering (art 41 och 42 RTS om riskramverk)

Till kontinuitetspolicyn ska en konsekvensanalys för exponering och affärsstörningar införas. Konsekvensanalysen ska bland annat identifiera potentiella hot för IKT-tillgångar, möjliga skyddsåtgärder och riktlinjer för säkerhetskopiering. Kontinuitetspolicyn ska följas upp minst en gång per år.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar aktörer som omfattas av DORA att initialt undersöka om undantag i DORA kan tillämpas, dvs. om bolaget i fråga kan träffas av definitionerna för mikroföretag, litet företag eller medelstora företag, se art 3 DORA. Därefter bör det genomföras en riskanalys i syfte att kunna sätta in resurser och arbete för implementering av DORA där behovet är som störst. En sådan riskanalys bör omfatta de fem huvudområdena i) riskhantering, ii) incidenthantering och rapportering, iii) tredjepartsrisker, iv) testramverk, och iv) informationsdelning.

Även om kraven i DORA till vissa delar liknar de riktlinjer som EBA och EIOPA tagit fram om IKT är DORA ett helt nytt regelverk som ska implementeras, vilket kommer kräva planering inför att DORA ska börja tillämpas den 17 januari 2015. Wesslau Söderqvist Advokatbyrå kan bistå med att dels genomföra en riskanalys och fastställa en prioriteringslista, dels med själva implementeringen.

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

Nyhetsbrev

Ang. Beslut om adekvat skyddsnivå för USA

---

28 augusti 2023

1 Bakgrund

Wesslau Söderqvist Advokatbyrå har tidigare informerat om processen för att anta ett beslut om adekvat skyddsnivå inom EU:s och USA:s ram för dataskydd. Inte mindre än tre förslag till överenskommelse mellan EU och USA har ogiltigförklarats av EU-kommissionen, nedan Kommissionen, sedan processen inletts. Den 10 juli 2023 har dock Kommissionen fattat det efterlängtade beslutet om adekvat skyddsnivå för USA, det s.k. *EU-U.S. Data Privacy Framework*. Beslutet har trätt i kraft vid samma datum. Kommissionen kommer löpande att övervaka utvecklingen i USA och hur beslutet efterlevs. En första utvärdering kommer att äga rum inom ett år.

2 Kommissionens beslut

2.1 Adekvat skyddsnivå

Enligt Kommissionens beslut säkerställer USA en adekvat skyddsnivå som är jämförbar med EU:s för personuppgifter som överförs från EU till amerikanska företag. Detta innebär att personuppgifter kan skickas från EU till amerikanska företag utan att de behöver införa ytterligare dataskyddsåtgärder.

Beslutet medför att det införs nya bindande säkerhetsåtgärder för att åtgärda alla de problem som EU-domstolen tidigare har tagit upp, bl.a. genom att de amerikanska underrättelsemyndigheternas tillgång till uppgifter från EU begränsas till vad som är nödvändigt och proportionerligt och genom att en dataskyddsdomstol inrättas som EU-medborgare kan vända sig till. Privatpersoner i EU kommer därmed att kunna vända sig till dataskyddsdomstolen om deras personuppgifter har hanterats på ett felaktigt sätt av de amerikanska företagen. Detta innebär bl.a. att privatpersoner i EU kommer att ha tillgång till en oavhängig och opartisk prövningsmekanism avseende de amerikanska underrättelsemyndigheternas insamling och användning av uppgifter. Dataskyddsdomstolen kommer även att självständigt utreda och lösa klagomål.

2.2 Certifiering

Att observera är att överenskommelsen är baserad på krav på certifiering och att beslut om adekvat skyddsnivå därför endast anses föreligga avseende företag i USA som blivit certifierade. Dessa företag måste uppdatera sin certifiering på en årlig basis. De amerikanska företagen kan endast ansluta genom att åta sig att följa en detaljerad uppsättning av principer och krav. Detta inkluderar till exempel krav på ändamålsbegränsning, dataminimering och datalagring samt specifika skyldigheter gällande säkerhet och delning av data med tredje part. Per dagens datum är 2 489 amerikanska företag certifierade.

2.3 Amerikanska underrättelsetjänsters tillgång till data

President Joe Biden har undertecknat en presidentorder i oktober 2022 och därefter har det antagits förordningar i USA. I och med presidentordern har det bl.a. införts bindande skyddsåtgärder som begränsar amerikanska underrättelsemyndigheters tillgång till data, förbättrad övervakning av underrättelsemyndigheterna och inrättande av den oberoende och opartiska dataskyddsprövningsdomstolen.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Kommissionens beslut innebär stora förbättringar jämfört med mekanismen enligt ”privacy shield” för skydd av privatliv, som ogiltigförklarats i och med Schrems II-domen. Oaktat vilka regler som är tillämpbara på en överföring rekommenderar Wesslau Söderqvist Advokatbyrå att det alltid genomförs en dokumenterad konsekvensanalys avseende överföring av personuppgifter till tredje land, innan sådan överföring sker.

Har ni frågor med anledning av det ovanstående eller är i behov av en konsekvensbedömning är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. Sanktionsavgift mot Trygg-Hansa

---

15 september 2023

1 Integritetskyddsmyndighetens beslut

Integritetsskyddsmyndigheten, nedan IMY, fick i december 2020 tips om att Moderna Försäkringar, filial till Tryg Forsikring A/S, hade möjliggjort för obehöriga att få tillgång till känsliga personuppgifter om dess kunder. Med anledning av detta har IMY i mars 2021 inlett tillsyn mot Moderna Försäkringar för att granska om bolaget hade vidtagit lämpliga åtgärder för att säkerställa en adekvat säkerhetsnivå i samband med behandlingen av personuppgifterna i enlighet med dataskyddsförordningen, nedan GDPR.

Moderna Försäkringar har i april 2022 gått samman med Trygg-Hansa varefter bolaget bytt namn till Trygg-Hansa filial. IMY hänvisar i sitt beslut till Trygg-Hansa, men händelserna har ägt rum i dåvarande Moderna Försäkringar.

IMY har den 28 augusti 2023 beslutat att Trygg-Hansa ska betala en administrativ sanktionsavgift om 35 miljoner kronor för överträdelsen av GDPR. Nedan redogörs mer utförligt för bakgrunden till beslutet samt den bedömning som ligger till grund för beslutet.

2 Bakgrund till beslutet

Moderna Försäkringar har den 30 november 2020 kontaktats av en person per telefon som uppgett att personen varit i kontakt med Moderna Försäkringar för att få en offert för försäkring och i samband med det upptäckt brister i personuppgiftsbehandlingen. Personen som tagit emot samtalet hos Moderna Försäkringar har inte uppfattat att det kunde röra sig om en incident och har därför inte rapporterat det vidare inom organisationen. Personen som ringt in har därför tipsat IMY och redogjort för det inträffade som bedömts som en incident.

Personen som tipsat IMY har mottagit ett SMS eller e-postmeddelande med en unik webbadress till en offertsida på Moderna Försäkringars webbplats. På denna offertsida har det funnits länkar med webbadresser som lett till dokument innehållande försäkringsinformation. Personen som tipsat IMY har noterat att dokumenten haft webbadresser som vid tillfället kunnat modifieras av personen i dennes webbläsare genom att byta ut siffror i webbadressen. Genom att göra det har personen i fråga lyckats få tillgång till andra kunders dokument.

Den totala åtkomstmöjligheten har varit till cirka 650 000 kunder. Handlingarna som har varit åtkomliga för obehöriga har i vissa fall innehållit känsliga personuppgifter, bl.a. detaljerade uppgifter om hälsa.

3 IMY:s bedömning

3.1 Höga krav på behandlingen av uppgifterna

IMY konstaterar att behandlingen av personuppgifterna omfattat ett stort antal registrerade. Behandlingen har avsett ett stort antal personuppgifter om varje registrerad och genom tillgång till ett enda dokument har det varit möjligt att direkt utläsa ett stort antal uppgifter om en enskild person. IMY betonar att behandlingen varit särskilt integritetskänslig genom användningen av personnummer och andra identifieringsuppgifter som möjliggjort en tydlig och direkt koppling till enskilda individer.

IMY konstaterar vidare att personuppgifternas karaktär i sig medfört en hög risk eftersom de innehållit sådana känsliga personuppgifter om hälsa som endast behandlas får behandlas i undantagsfall enligt GDPR. Även personnummer och uppgifter om lagöverträdelser utgör särskilt skyddsvärda uppgifter som omfattats av behandlingen. Uppgifterna har därmed ansetts behöva ett extra skydd. De uppgifter som gått att få tillgång till genom behandlingen har som tidigare nämnts varit av hög detaljnivå vilket ytterligare medfört en hög risk för de enskilda vars uppgifter behandlats.

Enskilda har givits möjligheten att lämna vissa uppgifter i skadeanmälningar i löpande text. Detta är något som IMY menar medfört ett särskilt högt krav på att hantera dokumenten på ett säkert sätt, eftersom Moderna Försäkringar inte fullt ut kunnat kontrollera innehållet och typen av uppgifter som lämnats i dokumentet.

Sammantaget har behandlingen varit av sådant slag att det ställts höga krav på säkerheten för uppgifterna.

3.2 Uppgifterna har inte skyddats på ett lämpligt sätt

IMY konstaterar att det inte har krävts att den som fått åtkomst till uppgifterna verifierat sin identitet eller på annat sätt verifierat sin behörighet. Det enda som krävts för att få åtkomst till uppgifterna har varit tillgången till webbadresserna. Det har inte funnits någon funktion på plats som säkerställt att det varit en behörig person som tillerkänts åtkomst. Uppgifterna har inte heller skyddats av kryptering. Det har också varit möjligt att vidarebefordra webbadresserna.

Alla som fått tillgång till webbadresserna har således kunnat få tillgång till de integritetskänsliga personuppgifterna.

IMY konstaterar att det faktum att det varit möjligt för obehöriga att få tillgång till personuppgifter är en tillräckligt allvarlig brist i sig, oberoende av hur många som faktiskt haft tillgång till personuppgifterna i det aktuella fallet. Bristerna har varit av sådan grundläggande karaktär att Moderna försäkringar borde ha upptäckt och åtgärdat dem innan systemet införts. Systemet har använts sedan det införts år 2018 tills att IMY tipsats år 2020 utan att bristerna identifierats eller åtgärdats. IMY menar också att Moderna försäkringar borde ha haft god förmåga att säkerställa en lämplig skyddsnivå för behandlingen då personuppgiftsbehandlingen är en del av försäkringsbolagets kärnverksamhet.

IMY bedömer därmed att lämpliga tekniska åtgärder inte vidtagits för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Personuppgifter har således behandlats i strid med GDPR och på grund av att överträdelsen är så pass allvarlig åläggs Trygg-Hansa, oaktat att händelsen inträffade hos dåvarande Moderna försäkringar, att betala en sanktionsavgift om 35 miljoner kronor.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att alla personuppgiftsansvariga ser över sina rutiner och säkerställer att de uppfyller en lämplig säkerhetsnivå för den enskilda verksamheten. Det är särskilt beaktansvärt att personuppgifter behandlas kärnverksamheten varför det borde ha funnits god förmåga att säkerställa den skyddsnivå som krävs enligt GDPR. Samma bör gälla även andra uppgifter av betydelse för verksamheten, inte minst med beaktande av regelverk på informationssäkerhetens område, som DORA och NIS2.

Vad som utgör en lämplig säkerhetsnivå enligt GDPR kan således variera i förhållande till behandlingens art, omfattning, sammanhang och ändamål varför det är lämpligt att varje personuppgiftsansvarig gör en egen riskanalys av sin verksamhet och anpassar rutinerna för personuppgiftsbehandling efter riskanalysen. Denna riskanalys bör ses över löpande och anpassas efter mängden och typen av personuppgifter som hanteras i verksamheten.

Har ni frågor med anledning av det ovanstående eller vill ha hjälp med att utföra en riskanalys är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. FiDA-förordningen

---

19 september 2023

1 Införandet av FiDA-förordningen

EU-kommissionen har publicerat ett förslag om en ny förordning vid namn ”Förordning om ett ramverk för tillgång till finansiella data” nedan FiDA. Syftet med förordningen är att kunder hos finansiella institut ska kunna dela sina finansiella data till tredjepartsbolag. FiDA ska tillämpas på bl.a. fondbolag, värdepappersbolag, försäkringsförmedlare och försäkringsföretag.

1.1 Nuvarande reglering

För närvarande finns det dels reglerade, dels oreglerade öppna finansiella tjänster. De reglerade är baserade på EU:s betaltjänstedirektiv som inkluderar delning av betalkontoinformation mellan olika bolag. Betaltjänstedirektivet har inkorporerats i svensk rätt genom lagen (2010:751) om betaltjänster. Lagen är emellertid endast tillämpbar för betaltjänster varvid andra som erbjuder öppna finansiella tjänster som faller utanför detta begrepp inte omfattas av något regelverk, s.k. oreglerade öppna finansiella tjänster. Det som är signifikativt för dessa är att kunden utan datainnehavarens kännedom ger medgivande till tredjepartsbolaget att inhämta kundens data.

1.2 Varför införs en ny förordning?

Eftersom dataanvändare varit kritiska till hur datadelningen fungerat i praktiken samt att det inte delas mycket data inom finanssektorn, vilket hämmar användningen av öppna finansiella tjänster, har förslaget presenterats av EU-kommissionen. Förslaget är en del av EU-kommissionens strategi för digitalisering av finanssektorn och syftet med strategin är att stärka innovation och konkurrenskraft inom EU:s finanssektor. Konkret innebär detta att förslaget ska leda till nya, billigare och bättre datadrivna finansiella produkter och tjänster, t.ex. verktyg för jämförelse av finansiella produkter och personlig rådgivning via onlinetjänster. Förslaget ska förbättra kundernas tillit och därmed öka viljan att dela med sig av data, förhindra att datainnehavare ska kunna neka datadelning samt minska kostnaderna som uppstår till följd av bristande enhetlighet.

1.3 Vad innehåller förslaget?

Om förslaget träder i kraft kommer kunder kunna begära ut sina data och ge medgivande till datadelning. Tillämpningsområdet för kundernas ökade rättigheter avser:

1. Bolåneavtal, lån och konton. Betalkonton är emellertid undantagna.
2. Sparande, investeringar i finansiella instrument, försäkringsbaserade investeringsprodukter, kryptotillgångar, fastigheter och andra relaterade finansiella tillgångar och förmåner från sådana tillgångar.
3. Data som samlats in för att genomföra ändamålsenlighets- och lämplighetsbedömningar i samband med marknader för finansiella instrument.
4. Pensionsrättigheter för tjänstepensionsplansplaner
5. Pensionsrättigheter för att tillhandahålla paneuropeska privata pensionsprodukter (s.k. PEPP-produkter).
6. Icke-livförsäkringsprodukter med undantag av sjukdoms-, hälso- eller medicinförsäkringsprodukter.
7. Data som samlats in för kreditvärdighetsbedömningar till företags låneansökningar och kreditbetyg.

Både kunder och bolag kan begära tillgång till kunders data. För att en kund ska få ut sin egendata krävs det att kunden begär detta. Om kunden begär detta ska kunden få ta del av data utan avgift och obefogat dröjsmål. Om ett bolag begär ut en kunds data krävs det att två omständigheter föreligger. För det första krävs det att kunden lämnar sitt medgivande. För det andra krävs det att bolaget som begär data har ett tillstånd från behörig myndighet. För att tillstånd ska ges krävs det antingen att det rör sig om ett finansiellt företag som anges i förordningen eller att ett antal villkor uppfylls. Villkoren är att bolaget ska beskriva sin verksamhet, hur de planerar att använda delade data samt ha adekvat intern styrning och tillräckliga skyddsåtgärder för att motverka IT-relaterade risker såsom cyberattacker. Om tillstånd givits till dataanvändaren samt ett medgivande finns från kunden får datadelning ske från ett bolag till ett annat.

2 Wesslau Söderqvist Advokatbyrås rekommendationer

FiDA har potential att öka konkurrensen på finansmarknaden och stimulera till innovation av nya tjänster. FiDA kommer också bidra till att nya typer av aktörer kommer omfattas av reglering vid datadelning inom den finansiella sektorn. Om datadelning ska vara möjligt kommer det dock vara av central betydelse att kunder känner tillit till ramverkets risker, framförallt om FiDA blir obligatorisk. Tillräckliga krav måste ställas på kunders samtycke, att data lagras säkert

och att särskilt känsliga data skyddas. Kunder måste få tydlig och koncis information om vilka data som ska delas, hur länge och vad de ska användas till.

Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer som kommer att omfattas av FiDA bevakar regelverket och säkerställer att kunder, vid tidpunkten när FiDA ska tillämpas, ges fullständig information vid delning av data. Likaså behöver ersättningsmodeller bevakas eftersom det är oklart vilka kostnader som kan tas ut vid framtagande av kundinformation, som exempelvis passande- och lämplighetsbedömningar. Det kan därför finnas behov av att se över ersättningsmodeller i god tid innan regelverket träder i kraft. Eftersom mängden data som ska kunna göras tillgänglig ökar, kommer det ställa höga krav på säkerhet. Detta går hand i hand med DORA och Wesslau Söderqvist Advokatbyrå rekommenderar att implementeringen av DORA påbörjas med detsamma, oaktat när FiDA eventuellt ska börja tillämpas.

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