Till
Styrelsen i S:t Erik Försäkrings AB

Rapport för perioden 12 maj - 15 september 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.

- Digitala bolags- och föreningsstämmor.
- Årlig rapport från MSB om IT-incidenter.
- IMY utfärdar sanktionsavgift mot Regionstyrelsen i Region Skåne.
- Dataskydd mellan EU och USA.
- Operativ motståndskraft i finanssektorn.
- Sanktionsavgift mot Meta (Facebook).
- Rapport om anmälda personuppgiftsincidenter 2022.
- Sanktionsavgift mot Bonnier.
- Sanktionsavgift mot Spotify.
- Beslut om adekvat skyddsnivå för USA.

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 som redogörs för närmare nedan.

Område	*Kontroll*	*Compliancerisk (Grön/Gul/Röd)*
Försäkringsverksamhet	Kunskap och kompetens (inkl. fortbildningskravet) enligt försäkringsdistributions-regelverket (IDD).	Kontrollen har inte föranlett några synpunkter.
Försäkringsverksamhet	Riktlinjer för uppdragsavtal inkl. uppföljning av uppdragstagare.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Intressekonflikter.	Kontrollen har inte föranlett några synpunkter.
Övrig regelefterlevnad	Styrelsens samlade kompetens.	Kontrollen har inte föranlett några synpunkter.

Kunskap och kompetens

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

Bolaget har redogjort för Bolagets interna rutiner för fortbildning och kunskapstest som omfattar de anställda som direkt deltar i Bolagets försäkringsdistribution. Bolaget bedöms ha goda rutiner för löpande fortbildning.

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

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

Riktlinjer för och uppföljning av uppdragstagare

Granskning av Bolagets interna riktlinjer för uppdragsavtal. Kontrollen har syftat till att säkerställa att Bolagets interna riktlinjer är anpassade enligt såväl FRL som EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer. Även EIOPA:s IKT-riktlinjer har tagits i beaktande. Därtill har Bolagets kontroll och uppföljning av uppdragstagare diskuterats. Uppföljningen utförs, dokumenteras och presenteras därefter för styrelsen i regel i slutet av året.

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

Försäkringsverksamhet

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

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

Övrig regelefterlevnad

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

   Bolagets styrelse har under år 2022 genomfört den årliga ”fit & proper” övningen där samtliga styrelseledamöter skattat dels sin egen enskilda kunskap och kompetens, dels styrelsens samlade kompetens. I denna övning identifieras eventuella behov av kompetensutveckling och Bolaget följer upp och justerar styrelsens utbildningsplan för kommande år. Årets fit & proper kommer att genomföras i slutet av september 2023.

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

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

   Bolaget har redogjort för Bolagets interna rutiner för att identifiera och hantera intressekonflikter. Funktionen för regelefterlevnad har vidare tagit del av Bolagets interna riktlinjer för hantering av intressekonflikter som omfattar samtliga anställda och Bolagets ledning. Funktionen för regelefterlevnad har även noterat att Bolaget dessutom omfattas av Stockholm Stads riktlinjer för hantering av intressekonflikter.

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

Uppföljning av tidigare kontroller

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

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

2.3 Råd och stöd

Funktionen för regelefterlevnad har under perioden funnits tillgänglig för att svara på frågor och lämna råd och stöd till Bolagets anställda.

2.4 Styrelsemöten

Funktionen för regelefterlevnad har den 26 maj 2023 närvarat vid styrelsemöte hos Bolaget och därvid redogjort för bl.a. föregående kvartals rapport.

3 Funktionen för regelefterlevnads bedömning

Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att Bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för Bolagets tillståndspliktiga verksamhet.

Stockholm den 15 september 2023

Johan Grenefalk

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Digitala bolags- och föreningsstämmor

4 maj 2023

1 Bakgrund

Justitiedepartementet har presenterat förslag till ändring i aktiebolagslagen (2005:551) och förslag till ändring i lagen (2018:672) om ekonomiska föreningar. Förslagen består i att det från och med 1 januari 2024 ska bli möjligt för aktiebolag och ekonomiska föreningar att hålla helt digitala bolags- och föreningsstämmor. Förslagen har utan anmärkning tillstyrkts av Finansinspektionen.

Med dagens reglering är det möjligt att hålla hybridstämmor innebärande att stämman leds från den av lag och bolagsordning utpekade stämmoplatsen men att vissa deltar på distans. Det är dock inte möjligt att genomföra en helt digital bolags- eller föreningsstämma om inte samtliga aktieägare eller medlemmar samtycker till det.

Under Covid-19 pandemin infördes lagen (2020:198) om tillfälliga undantag för att underlätta genomförandet av bolags- och föreningsstämmor för att minska risken för smittspridning. Genom lagändringar blev det möjligt för aktiebolag och ekonomiska föreningar att genomföra bolags- och föreningsstämmor utan fysiskt deltagande. Justitiedepartementet har hållit i samrådsmöten för att diskutera ett permanent införande av möjligheten till digitala bolags- och föreningsstämmor och intresset för denna möjlighet har visat sig vara stort. Det är mot bakgrund av detta som Justitiedepartementet i sin promemoria föreslår införandet av möjligheten att hålla digitala bolags- eller föreningsstämmor, vilket redogörs för nedan.

2 För- och nackdelar med införandet

I promemorian konstateras att digitala stämmor redan är något som är tillåtet i våra grannländer. I Danmark har det sedan år 2003 varit möjligt med digitala stämmor under förutsättning att styrelsen bl.a. ser till att den digitala stämman kan genomföras på ett betryggande sätt. [1] Motsvarande reglering finns även i Norge där det stadgas att digitala stämmor är tillåtna om inte bolagsordning eller stadgar anger något annat.[2] I Finland regleras

[1] *77 § lov nr. 470 af 12 juni 2009 om aktie og anpartsselskaber – selskabsloven.*
[2] *5 kap. 8 § lov 13 juni 1997 nr 44 om aksjeselskaper och 5 kap. 8 § lov 13 juni 1997 nr 45 om allmennaksjeselskaper.*

det på ett liknande sätt och det krävs även att rätten att delta och rösträkningens riktighet kan kontrolleras på ett sätt som kan jämställas med förfarandena vid en traditionell bolagsstämma.[3]

Möjligheten till digitala stämmor skulle innebära fördelar i form av bl.a. färre resor och mindre lokalhyreskostnader. En nackdel som tas upp är att det försvårar möjligheten att delta för mindre teknikvana personer. Mot bakgrund av att många genomförde sina stämmor digitalt under pandemin bör många redan ha viss erfarenhet av detta. Utredningen konstaterar vidare att det bör vara upp till de enskilda bolagen och föreningarna att överväga om en sådan lösning passar dem. Dessutom har som nämnts våra grannländer redan infört en sådan lösning.

3 Utformningen på en eventuell reglering

I utredningen konstateras att en utgångspunkt är att det ska vara upp till aktieägarna och medlemmarna att i bolagsordningen och stadgarna bestämma om möjligheten att hålla digitala bolagsstämmor. I både aktiebolag och ekonomiska föreningar får stämman idag hållas på annan ort än den i lag eller bolagsordning respektive stadgar, om extraordinära omständigheter kräver det.

Ytterligare en förutsättning för att få hålla digitala stämmor bör vara att de är teknikneutrala. Stämmorna ska organiseras på ett sådant sätt att alla aktieägare och medlemmar har möjlighet att delta och utöva sina rättigheter. Det måste finnas lämpliga rutiner för att identifiera deltagarna och för rösträkning. Vad som är lämpliga tekniska lösningar kan skilja sig åt mellan olika bolag och föreningar. Mer detaljerade former för hur en digital stämma ska organiseras är främst en teknisk fråga som inte lämpar sig för lagstiftning utan det ligger inom ramarna för bolagsordningen respektive stadgarna.[4]

Förslaget innehåller inte bestämmelser om följder vid eventuella teknikproblem vid digitala stämmor. Det konstateras att en bestämmelse om fördelningen av teknikrisken skulle bli en allt för vag bestämmelse. Frågan om huruvida stämman genomförts i strid med lag, bolagsordning eller stadgar kan i stället prövas i en klanderprocess. Det ska inte heller införas en bestämmelse om krav på att digitala stämmor ska kombineras med poströstning utan även detta är upp till bolagen och föreningarna att reglera i sina bolagsordningar respektive stadgar. Vad gäller utomståendes rätt att närvara vid stämmor konstateras att denna reglering föreslås förbli oförändrad.[5]

---

[3] 5 kap. 16 § aktiebolagslagen 624/2006 och 5 kap. 17 § lag om andelslag 421/2013.
[4] Prop. 2004/05:85 s.301, prop. 2009/10:247 s.42 och 47 samt prop. 2015/16:4 s.147.
[5] Se 7 kap. 6 och 55 §§ aktiebolagslagen respektive 7 kap. 8 § lagen om ekonomiska föreningar.

Slutligen föreslås det att det ska införas krav på kallelsens innehåll när det gäller digitala stämmor för aktiebolag och ekonomiska föreningar för att deltagarna ska få information i kallelsen om hur de ska gå till väga för att delta i den digitala stämman.

4 Wesslau Söderqvist Advokatbyrås rekommendationer

Ett bolag som vill utnyttja möjligheten till digitala stämmor ska ange det i bolagsordningen respektive stadgarna. De nya reglerna kan tillämpas på alla stämmor som hålls från och med ikraftträdandet den 1 januari 2024. Wesslau Söderqvist Advokatbyrå rekommenderar därför, om möjligheten ska utnyttjas, att redan före det datumet ta in stöd för digitala stämmor i bolagsordning eller stadgar och att kalla till en stämma i enlighet med de nya reglerna, så länge stämman hålls tidigast den 1 januari 2024. Wesslau Söderqvist Advokatbyrå bevakar lagförslaget och avser att återkomma med ytterligare information.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Årlig rapport från MSB om IT-incidenter

---

9 maj 2023

1 Inledning

MSB har publicerat en årsrapport över IT-incidenter som inträffat under år 2022. Rapporten har sin grund i den IT-incidentrapportering som MSB mottar från både statliga myndigheter och från leverantörer av samhällsviktiga och digitala tjänster.[1] Rapporten riktar sig främst till beslutsfattare, informations- och säkerhetsansvariga, samt omvärldsbevakande och analyserande funktioner hos både statliga myndigheter och NIS-leverantörer[2]. Innehållet kan även vara värdefullt för motsvarande roller hos andra organisationer, finansiella aktörer inräknat.

2 Lärdomar och rekommendationer från MSB

Under år 2022 har 330 IT-incidenter rapporterats in till MSB av myndigheter och NIS-leverantörer. Detta innebär en liten minskning från år 2021 (343 rapporterade incidenter) vilket innebär att rapportering från myndigheter har minskat. Den vanligaste orsaken till rapporterade incidenter under år 2022 har varit systemfel, följt av misstag och sedan angrepp. MSB lyfter en analys som visar att uppdateringar och andra ändringar som inte genomförs på ett kontrollerat och riskminimerande sätt kan öka risken för incidenter.

När beroendet av fungerande digitala lösningar och sammanlänkningar ökar skapas även nya sårbarheter. Rapporteringen av IT-incidenter till MSB är av stor betydelse eftersom den ger viktig information om hot och sårbarheter kopplade till samhällets informations- och cybersäkerhet och därmed utgör ett viktigt underlag för att vidta åtgärder för att stärka informations- och cybersäkerheten. Sedan oktober 2022 har Polismyndigheten och MSB därför samverkat gällande inrapporterade och polisanmälda IT-incidenter. Ju mer information som tillhandahålls kring incidenter, desto bättre kan det förebyggande arbetet utvecklas och struktureras.

Ökad kommunikation mellan myndigheter och andra aktörer kommer även att möjliggöras när DORA[3] ska börja tillämpas. Finansiella entiteter ska sinsemellan kunna utbyta information och

---

[1] *Direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverks- och informationssystem inom unionen (NIS).*
[2] *Samhällsviktiga leverantörer.*
[3] *Förordningen om digital operativ motståndskraft inom den finansiella sektorn (DORA).*

underrättelser om cyberhot, inbegripet indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden i syfta att öka kunskaperna och den digitala motståndskraften inom den finansiella sektorn.

MSB lyfter att komplexiteten i IT-miljöer ofta är hög och kräver ingående kunskap för att kunna orientera sig i och för att på ett säkert sätt kunna optimera systemet. Detta tydliggör att samverkan bör etableras även på operativ nivå. MSB lyfter också vikten av att göra en medveten riskbedömning. Organisationer som bedriver ett systematiskt informations- och cybersäkerhetsarbete och som har arbetssätt för att identifiera risker och som inte lämnar risker utan åtgärd, är bättre rustade från hot. Även leverantörskedjor behöver kartläggas och riskbedömas genom bl.a. sårbarhetsanalyser.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Det är i MSB:s rapport tydligt att medvetenhet och kunskap är viktiga komponenter för att öka motståndskraften samt kunna identifiera och freda sig mot olika typer av cyberhot.

Wesslau Söderqvist Advokatbyrå rekommenderar att arbete snarast påbörjas för att implementera regelverken. Det bör initialt säkerställas att det finns kunskap och kompetens kring området. DORA har trätt i kraft och ska börja tillämpas den 17 januari 2025 och NIS2 ska implementeras i svensk rätt och beräknas träda i kraft i slutet av år 2024.

Wesslau Söderqvist Advokatbyrå rekommenderar att aktörer kontrollerar i vilken utsträckning verksamheten omfattas av NIS2 respektive DORA. Det finns flera undantagsregler för mindre aktörer och de aktörer som omfattas av båda regelverken behöver bl.a. ha klart för sig hur rapporteringskraven ska tillämpas när en incident inträffar. Aktörer bör proaktivt se över vilka rapporteringskrav som gäller för olika typer av IT-incidenter för att kunna agera snabbt och korrekt om och när en incident inträffar då rapportering kan behöva ske till mer än en myndighet. Börja planera i tid för att lyckas uppnå efterlevnad till en försvarbar kostnad.

Har ni frågor med anledning av det ovanstående eller är i behov av hjälp med att implementera DORA och/eller NIS2 är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. IMY utfärdar sanktionsavgift mot Regionstyrelsen i Region Skåne

---

10 maj 2023

1 Integritetskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) har beslutat att Regionstyrelsen i Region Skåne, nedan Regionen, ska betala en administrativ sanktionsavgift för att ha behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen (GDPR). IMY bedömer att Regionen har behandlat känsliga personuppgifter utan att ha säkerställt en lämplig säkerhetsnivå i förhållande till risken för förlust, obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Mot bakgrund av detta har IMY beslutat att Regionen ska betala en administrativ sanktionsavgift för överträdelsen om 200 000 kronor.

2 Bakgrund och motivering av beslutet

IMY har mottagit en anmälan om en personuppgiftsincident från Regionen den 18 november 2020. Av anmälan framgår att ett USB-minne innehållande personnummer och känsliga personuppgifter om 1 934 registrerade glömts bort av en medarbetare i fickan på dennes arbetskläder. Arbetskläderna har därefter lagts i en tvättpåse för transport till ett regionalt tvätteri. USB-minnet har inte återfunnits. IMY har därefter mottagit två klagomål med anledning av personuppgiftsincidenten och har därför beslutat att inleda tillsyn.

Mot bakgrund av att det är Regionen som har bestämt ändamål och medel för behandlingen av personuppgifterna i förevarande fall är det Regionen som är personuppgiftsansvarig. Det innebär att Regionen är ansvarig för att se till att behandlingen av personuppgifter sker i enlighet med GDPR:s bestämmelser. Ansvaret ligger på Regionen även om incidenten orsakats av ett misstag eller felbedömning av anställd så länge detta skett inom ramen för den anställdes tjänst.

I det ansvar som åligger den personuppgiftsansvarige ingår att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna med behandlingen.

IMY framhåller att vad som är en lämplig säkerhetsnivå varierar i förhållande till bl.a. behandlingens art, omfattning, sammanhang och ändamål. Det är också beroende av vad för typ av personuppgifter det är som behandlas. I det förevarande fallet var det fråga om uppgifter

om patienters hälsa vilket anses särskilt skyddsvärt och borde ha föranlett att Regionen säkerställt ett starkt skydd. Mot bakgrund av det anser IMY att det förelegat en hög risk vid hanteringen av personuppgifterna.

IMY konstaterar att behandlingen av personuppgifterna har skett på ett okrypterat USB-minne. Som uppgifterna behandlats i det aktuella fallet har det gått att direkt av uppgifterna utläsa att det rör uppgifter om patienters hälsa kopplade till personnummer. Det går alltså att identifiera de registrerade. Eftersom USB-minnet tappats bort finns en påtaglig risk för att någon som inte har rätt att ta del av uppgifterna ändå gör det, vilket i sin tur kan leda till att uppgifterna riskerar att spridas vidare till fler obehöriga.

Eftersom IMY konstaterat att Regionen är personuppgiftsansvarig och att det förelegat en hög risk vid behandling av dessa personuppgifter så kan Regionen inte anses ha säkerställt en lämplig säkerhetsnivå i förhållande till risken för förlust, obehörigt röjande eller obehörig åtkomst till personuppgifterna.

Sammantaget har alltså IMY funnit att Regionen inte vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Regionen har därför behandlat personuppgifter i strid med GDPR. IMY anser inte att det är fråga om en mindre överträdelse som hade kunnat resultera i en reprimand och utfärdar därför en sanktion om 200 000 kronor.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att företag som behandlar personuppgifter ser över sina rutiner och säkerställer att de uppfyller en lämplig säkerhetsnivå för den enskilda verksamheten.

Precis som IMY framför i sitt beslut kan vad som utgör en lämplig säkerhetsnivå enligt GDPR variera i förhållande till behandlingens art, omfattning, sammanhang och ändamål. Det varierar även beroende på vad för typ av personuppgifter det är som ska behandlas. Kravet på säkerhetsnivå ställs högre om känsliga personuppgifter behandlas inom verksamheten. Wesslau Söderqvist Advokatbyrå rekommenderar därför att varje enskild organisation gör en egen riskanalys av sin verksamhet och anpassar rutinerna för personuppgiftsbehandling efter riskanalysen. Riskanalysen bör ses över löpande och särskilt vid förändringar av mängden, typen och hanteringen av personuppgifter i verksamheten.

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

Nyhetsbrev

Ang. Dataskydd mellan EU och USA

---

19 maj 2023

1 Inledning

Wesslau Söderqvist Advokatbyrå har tidigare informerat om att EU-kommissionen, nedan Kommissionen, och USA i mars 2022 på ett principiellt plan kommit överens om ett nytt regelverk för överföringar av personuppgifter. Den 7 oktober 2022 skrev Joe Biden under presidentorder (EO 14086) om förstärkta skyddsåtgärder för USA:s signalunderrättelseverksamhet. EO 14086 syftade till att implementera vad som varit överenskommet sedan mars 2022 i amerikansk lag. Den 13 december 2022 inledde Kommissionen processen för att anta ett beslut om adekvat skyddsnivå inom EU:s och USA:s ram för dataskydd. Detta är det tredje försöket att åstadkomma en överenskommelse mellan USA och EU. Kommissionen har nu, liksom vid de tidigare försöken, beslutat att ogiltigförklarat förslaget.

2 Kommissionens skäl

När Kommissionen granskar skyddsnivån i ett tredjeland är Kommissionen skyldig att bedöma innehållet i de regler som är tillämpliga i det landet samt den praxis som utformats i landet. Om en sådan bedömning skulle visa sig vara otillfredsställande i fråga om adekvat skyddsnivå och likvärdighet bör Kommissionen avstå från att anta ett beslut om skyddsnivå. Kommissionen har avstått från att anta ett beslut om skyddsnivå mot bakgrund av bl.a. följande skäl.

- Statliga aktörers omfattande massövervakning, massinsamling av data inbegripen, skadar europeiska medborgares och företags förtroende för digitala tjänster och i förlängningen för den digitala ekonomin. Amerikanska organ är förbjudna att samla in massdata om amerikanska medborgare som bor i USA, men detta förbud gäller inte EU-medborgare.

- De materiella definitionerna om principer för proportionalitet och nödvändighet stämmer inte överens med definitionerna i EU-rätten och EU-domstolens tolkning av dem. Dessa

principer tolkas enbart mot bakgrund av amerikansk lagstiftning och praxis och inte mot EU:s, när det gäller ramen för dataskydd mellan EU och USA.

- Förteckningen över legitima nationella säkerhetsmål kan ändras och utökas av USA:s president, som inte måste offentliggöra de relevanta uppdateringarna eller informera EU.

- EO 14086 erbjuder inte tillräckliga skyddsåtgärder vid massinsamling av data. Det föreligger avsaknad av oberoende förhandstillstånd, avsaknad av tydliga och strikta datalagringsregler, ”tillfällig” massinsamling och avsaknad av striktare skyddsåtgärder för spridning av data som erhållits genom massinsamling. Det finns en specifik oro för att brottsbekämpande myndigheter utan ytterligare restriktioner för spridning till amerikanska myndigheter skulle komma att få tillgång till uppgifter som de annars inte skulle ha tillgång till.

- Ett krav är att EU-medborgare ska ha samma rättigheter och privilegier som amerikanska medborgare när det gäller den verksamhet som USA:s underrättelseorgan bedriver samt tillgång till rättslig prövning i amerikansk domstol. Ett underliggande problem är därför att personer som inte är amerikanska medborgare övervakas enligt amerikansk rätt och att EU-medborgare inte har möjlighet att begära effektiv rättslig prövning i det avseendet. Det kan även noteras att det föreslagna prövningsförfarandet inte ger någon möjlighet att överklaga i en federal domstol och att det därför bl.a. inte ger klaganden någon möjlighet att begära skadestånd.

- Tillämpningen av EO 14086 är inte tydlig, exakt eller förutsebar i sin tillämpning, eftersom den när som helst kan ändras eller hävas av USA:s president, som också har befogenhet att utfärda hemliga presidentorder.

- Till skillnad från alla andra tredjeländer som har mottagit ett beslut om adekvat skyddsnivå enligt GDPR, saknar USA fortfarande en federal dataskyddslag.

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Möjligheten att överföra personuppgifter över gränserna kan bli en viktig drivkraft för innovation, produktivitet och ekonomisk konkurrenskraft så länge det finns adekvata skyddsåtgärder. Dessa överföringar bör göras med full respekt för rätten till uppgiftsskydd och rätten till integritet.

Europaparlamentet uppmanar Kommissionen att fortsätta förhandlingarna med USA i syfte att skapa en mekanism som skulle ge den adekvata skyddsnivå som krävs enligt GDPR. Beslutet om

adekvat skyddsnivå bör dock inte tas förrän alla rekommendationer i Kommissionens resolution och yttrande från EDPB har genomförts fullt ut. Det kommer sannolikt att dröja innan en lösning för överföring mellan EU och USA finns på plats. Till dess att en lösning finns på plats kan företag som vill använda sig av t.ex. amerikanska molntjänster implementera standardklausuler som har godkänts av EU i avtal med amerikanska företag. Wesslau Söderqvist Advokatbyrå rekommenderar att personuppgiftsansvariga alltid dokumenterar en konsekvensanalys avseende överföring av personuppgifter till tredje land.

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

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Operativ motståndskraft i finanssektorn

---

23 maj 2023

1 Bakgrund

Digitaliseringen i den finansiella sektorn skapar möjligheter men även risker för företag och vårt samhälle. De flesta tjänsterna inom den finansiella sektorn är idag digitala vilket innebär en risk för såväl cyberangrepp som andra tekniska störningar. Vid den nationella konferensen om informations- och cybersäkerhet inom finanssektorn konstaterade Andreas Heed, rättschef för området Betalningar på Finansinspektionen, att finansiella företag behöver stärka sin motståndskraft mot cyberangrepp. Han menade även att den statliga styrningen måste förbättras och att Finansinspektionen delvis behöver nya verktyg för att kunna genomföra detta.

2 Den finansiella sektorns sårbarhet

Finansiella företag är beroende av allmänhetens och de finansiella marknadernas förtroende samt att dessa företag är tätt sammanlänkade. Att kunder inte kan utföra grundläggande finansiella tjänster på grund av tekniska störningar kan påverka förtroendet för de finansiella företagen. Sammanlänkningen består dels av olika typer av finansiella exponeringar som lån eller derivatkontrakt, dels av att hela det finansiella tjänsteutbudet är beroende av tekniska system som är sammankopplade globalt. På grund av dessa sammanlänkningar kan IT-relaterade störningar och incidenter samt bristande kapacitet att hantera sådana skada hela systemet och innebära stora samhällsekonomiska kostnader.

3 Risker

Finansinspektionen konstaterat att de på flera plan ser ökade operativa risker, bl.a. ökade cyberhot. Finansiella företag utsätts ständigt för intrångsförsök och cyberattacker. Det senaste året har framför allt överbelastningsattacker periodvis varit intensiva. Denna ökade risk beror mycket på det försämrade säkerhetspolitiska läget i vår omvärld.

Finansinspektionen anser att finansiella företag måste bli bättre på att i sin kontinuitetsplanering beakta de förändringar som sker både i den interna och den externa miljön. Företag måste, förutom att beakta sin kontinuitetsplanering, prioritera förebyggande åtgärder och bygga väldimensionerade skydd mot externa hot.

En annan riskfaktor är att finansiella företag i allt höge grad lägger ut kritisk verksamhet till tredjepartsleverantörer som i sin tur lägger ut verksamhet till andra leverantörer. Med en lång leverantörskedja är det svårt för de finansiella företagen att utöva tillräckligt god styrning och kontroll över verksamheten som de är ansvariga för. Färre leverantörer innebär också en minskad risk för det fall ett intrång skulle ske eftersom det inte påverkar lika många aktörer.

4 Nödvändiga åtgärder

4.1 Förväntningar på de finansiella företagen

Finansinspektionen understryker vikten av att alla finansiella företag själva ansvarar för att öka sin digitala motståndskraft. Det är en pågående process som kräver ständig uppmärksamhet och ansträngning från företagen. Att notera är också att regelverk förändras vilket innebär nya omfattande krav. Ett exempel på det är DORA som kommer att kräva investeringar, tid och förberedelser från företagen.

4.2 Samspel mellan det offentliga och det privata

En gemensam styrning har länge efterfrågats vad gäller verksamhet som rör samhällets cybersäkerhet. Finansinspektionen har därför föreslagit att regeringen ser över formen för nationellt cybersäkerhetscenter (NCSC) för att hitta den mest ändamålsenliga organisationsmodellen på längre sikt.

Finansinspektionen har också föreslagit en ny struktur för krishantering i Sverige. Finansinspektionen anser att det finns ett behov av en centralt placerad aktör som kan hantera operativa kriser för finansiella företag. Ett sådant forum bör omfatta både privata finansiella aktörer och relevanta myndigheter.

Finansinspektionen anser vidare att regeringen bör överväga att inrätta ett särskilt cybersäkerhetsråd i Statsrådsberedningen som utifrån en gemensam och samlad hotbild över cyberhoten mot det svenska samhället fastställer en gemensam styrning för cybersäkerhetsfrågor.

Ett mer specifikt förslag är att privata e-legitimationer, såsom Bank-ID, bör stå under full tillsyn. Detta eftersom en cyberattack mot Bank-ID kan få allvarliga konsekvenser för flera delar av det svenska samhället eftersom tjänsten används i så stor omfattning.

4.3 Utökade befogenheter för Finansinspektionen

Finansinspektionen anser att de bör få utökade befogenheter när det gäller utkontraktering av ett finansiellt företags kritiska IT-verksamhet. Idag kan Finansinspektionen enbart ta emot anmälningar om sådana avtal. En ökad befogenhet för Finansinspektionen hade bidragit till en större möjlighet att hantera de risker som kan uppstå genom en ökad utkontraktering inom finansiella sektorn.

5 Wesslau Söderqvist Advokatbyrås rekommendationer

Wesslau Söderqvist Advokatbyrå rekommenderar att finansiella företag i sin kontinuitetsplanering är uppmärksamma på förändringar som sker både internt och externt. Det är också viktigt att företag, särskilt med det rådande omvärldsläget, arbetar förebyggande och ser till att det finns ett starkt skydd mot cyberhot. En del i det förebyggande arbetet är att se över vilka risker som finns relaterade till de tjänster som eventuellt lagts ut på tredjepartsleverantörer.

Nyligen tilldelade Finansinspektionen en bank en anmärkning och sanktionsavgift som en följd av en IT-incident. Det var inte IT-incidenten som sådan eller avsaknad av rutiner och processer som ledde till en sanktion utan det faktum att banken saknade de kontrollmekanismer som krävs för att säkerställa att dessa rutiner och processer efterlevs.

För att ha en god motståndskraft mot cyberhot krävs att företag håller sig uppdaterade och anpassar sin verksamhet efter de regulatoriska krav som uppställs. DORA ska börja tillämpas den 17 januari 2025, men det finns ingen anledning att avvakta med implementeringsarbetet då det kommer att krävas både tid och investeringar. Wesslau Söderqvist Advokatbyrå rekommenderar att ni börjar med att detektera kryphålen och prioritera de största riskerna.

Har ni frågor med anledning av det ovanstående eller vill diskutera implementeringen av DORA är ni välkomna att kontakta Wesslau Söderqvist Advokatbyrå.

WESSLAU SÖDERQVIST

Nyhetsbrev

Ang. Sanktionsavgift mot Meta (Facebook)

---

14 juni 2023

1 Bakgrund

Wesslau Söderqvist Advokatbyrå har tidigare informerat om att USA inte uppfyller adekvat skyddsnivå vid överföring av personuppgifter från EU/EES enligt EU:s allmänna dataskyddsförordning, nedan GDPR. Den irländska dataskyddsmyndigheten (DPC) har genomfört en utredning av Meta Platforms Ireland Limited, nedan Meta, tidigare känt som Facebook Ireland Limited. Utredningen har syftat till att undersöka på vilken grund som Meta överför personuppgifter från EU/EES till USA i samband med leveransen av sin Facebook-tjänst.

Meta har brutit mot artikel 46.1 GDPR då Meta fortsatt att överföra personuppgifter från EU/EES till USA efter att EU-domstolen avkunnat dom i det s.k. Schrems II-målet. Även om Meta genomfört dessa överföringar grundat på standardsavtalsklausuler som antagits av EU-kommissionen har det konstaterats att åtgärderna inte avhjälpt de risker för de registrerades grundläggande fri- och rättigheter som identifierats av EU-domstolen i Schrems II-målet.

På grund av den överträdelse av GDPR som detta inneburit har Meta ålagts att betala 1,2 miljarder euro i sanktionsavgift. Detta är den högsta sanktionsavgiften någonsin för en överträdelse av GDPR. Beslutet följer den Europeiska dataskyddsstyrelsens (EDPB) beslut tidigare i år där EDPB bland annat instruerat DPC att besluta om sanktionsavgiften mot Meta.

EDPB har som roll att bl.a. ge allmän vägledning för att klargöra begrepp inom europeisk dataskyddslagstiftning och därmed ge en enhetlig tolkning av de rättigheter och skyldigheter som följer av regelverket. EDPB har även befogenhet att fatta bindande beslut gentemot nationella tillsynsmyndigheter för att säkerställa en enhetlig tillämpning. I detta fall har EDPB tagit ett s.k. bindande beslut som DPC fått rätta sig efter. Nedan redogörs för de skäl som ligger bakom beslutet och vad Wesslau Söderqvist Advokatbyrå rekommenderar att företag bör vidta för åtgärder med anledning av det.

2 Närmare om DPC:s beslut

Undersökningen som genomförts har inletts på initiativ av DPC i Irland. Som nämnts ovan har utredningen i Irland avsett Metas behandling av personuppgifter, närmare bestämt överföringar

av personuppgifter från EU/EES till USA med stöd av standardavtalsklausuler för tredjelandsöverföring som antagits av EU-kommissionen år 2021.[1]

Omfattningen av undersökningen har omfattat två frågor:

1. Lagenligheten av de överföringar av personuppgifter för EU/EES-medborgare som besöker, har tillgång till, eller på annat sätt interagerar med Facebook-tjänsten som utförs av Meta, till Meta Platforms Inc. (tidigare Facebook Inc.) i enlighet med EU-domstolens s.k. Schrems II-mål.[2]

2. Huruvida (och/eller vilka) korrigerande befogenheter bör utövas av DPC enligt GDPR i händelse av att slutsatsen nås att Meta agerar olagligt och i strid med GDPR.

EU-domstolen har i Schrems II-målet konstaterat att Privacy Shield-avtalet mellan EU och USA inte utgör ett tillräckligt skydd för personuppgifter när de förs över till USA. Det har dock konstaterats att det i vissa fall kan vara tillräckligt att använda standardavtalsklausuler som EU-kommissionen beslutar om för att överföra personuppgifter till USA. I situationer där mottagarlandets nationella lagstiftning inte anses uppfylla kraven i GDPR, vilket alltså är fallet med USA, krävs dock ytterligare skyddsåtgärder.

I den aktuella situationen menar DPC att det inte varit tillräckligt att Meta använt standardavtalsklausulerna som grund för överföring av personuppgifterna. DPC menar att överföringarna i det aktuella fallet genomförts på ett sådant sätt att det inte kan garanteras en tillräcklig skyddsnivå för personuppgifter på sätt som föreskrivs i GDPR. Meta har argumenterat för att Meta borde omfattas av undantaget i art. 49 GDPR och således ha tillåtelse att föra över uppgifterna till ett tredje land som USA. En grund för att undantaget ska vara tillämpligt är bland annat att det föreligger samtycke från användarna till överföringen. Meta menar att de har haft ett sådant samtycke mot bakgrund av det sätt som Meta samlar in sina personuppgifter på. DPC menar dock att det inte anses föreligga giltiga samtycken varför undantaget inte varit tillämpligt.

EDPB har konstaterat i sitt beslut att överträdelsen av GDPR i det aktuella fallet är mycket allvarlig eftersom det rör sig om systematiska, upprepade och kontinuerliga överföringar. Meta har därför ålagts att avbryta personuppgiftsöverföringarna samt att betala en administrativ sanktionsavgift om 1,2 miljarder euro med anledning av överträdelsen av GDPR.

---

[1] *Kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679.*

[2] *Europeiska unionens dom meddelad den 16 juli 2020 i mål C-311/18.*

3 Wesslau Söderqvist Advokatbyrås rekommendationer

Beslutet är en tydlig signal till företag om att överträdelser av GDPR kan få långtgående konsekvenser och det måste tas på allvar. Det finns ännu inget avtal på plats som kan garantera en adekvat skyddsnivå för personuppgifter vid överföring mellan EU och USA. Det återstår att se om något avtal som kan garantera detta kan komma på plats, om inte USA reformerar sina dataskyddslagar.

Wesslau Söderqvist Advokatbyrå rekommenderar att personuppgiftsansvariga ser över företagets personuppgiftshantering och utan undantag genomför en konsekvensanalys avseende eventuella överföringar av personuppgifter som sker till ett tredje land. Wesslau Söderqvist Advokatbyrå bistår gärna med att genomföra en sådan konsekvensbedömning för det fall behovet skulle uppstå.

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

Nyhetsbrev

Ang. Rapport om anmälda personuppgiftsincidenter 2022

---

22 juni 2023

1 Statistik över personuppgiftsincidenter

1.1 Uppföljning av personuppgiftsincidenter

Integritetsskyddsmyndigheten, nedan IMY, har publicerat en rapport över de anmälningar om personuppgiftsincidenter som IMY tagit emot under år 2022. Totalt har 5 331 anmälningar mottagits av IMY. En personuppgiftsincident uppstår när de uppgifter som en verksamhet ansvarar för drabbas av en säkerhetsincident som leder till ett brott mot kraven på konfidentialitet, tillgänglighet och integritet. Enligt dataskyddsförordningen måste en personuppgiftsincident som utgör en risk för en enskilds rättigheter och friheter anmälas till IMY senast inom 72 timmar efter att verksamheten fått kännedom om den.

1.2 IMY följer upp personuppgiftsincidenter vilket kan leda till tillsyn vid generella brister eller brister i anmälan. Statistik över inkomna anmälningar

År 2022 minskade antalet anmälda personuppgiftsincidenter med 7,6 procent till 5 331 anmälningar. Det största delen av anmälningarna berodde på röjda personuppgifter, vilket kan bero på felskick eller annan felaktig hantering såsom att personuppgifter röjts för icke-behöriga. En annan stor del av anmälningarna berodde på att någon berett sig själv olovlig tillgång till personuppgifter, vilket dels kan bero på att de finns tillgängliga på en gemensam lagringsyta utan behörighetsstyrning, dels p.g.a. olika former av hackning, vilket var vanligast inom näringsliv, skola och utbildning samt kommuner. En mindre del av anmälningarna berodde dels på förlust, vilket innebär att uppgifter försvinner och uppgiftsansvarig förlorar kontroll över uppgifterna, vilket t.ex. kan bero på borttappade eller stulna datorer antingen från allmän plats eller genom inbrott, dels på antagonistiska angrepp vilket är när någon utanför organisationen försöker ta del av uppgifter. Flest anmälningar om antagonistiska angrepp skedde inom näringslivet.

Fördelat på olika sektorer stod den offentliga sektorn för 70 procent av alla anmälningar, privata sektorn för 25 procent, övriga sektorer för 2 procent och för resterande 3 procent saknas uppgift. En trolig orsak till den stora andelen anmälningar från den offentliga sektorn är att de behandlar en stor mängd uppgifter.

Av andelen anmälningar inom olika verksamhetsgrupper ökade offentliga myndigheter från 23 procent år 2021 till 26 procent av anmälningarna år 2022. Därutöver stod hälso- och sjukvården för 19 procent av anmälningarna. Näringslivet stod för 8 procent av anmälningarna och minskade således sin andel med nio procentenheter sedan år 2019. Det behöver inte ses som direkt negativt om ett verksamhetsområde ökar sina anmälningar, eftersom det kan bero på att verksamheten genom strukturer och rutiner skapat en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

Utöver de anmälningar som gjorts antas det finnas ca 10 000 oanmälda personuppgiftsincidenter.

1.3 Största orsak - Mänskliga faktorn

För de anmälningar som gjorts angavs mänskliga faktorn som orsak i sex av tio fall under år 2022. Brist i organisatoriska rutiner eller processer var den näst största faktorn på ett fall av tio.

Mänskliga faktorn handlar om individer som vid hantering av personuppgifter i verksamheten begår ett misstag. Misstag består i över hälften av fallen av felskickade brev, e-postmeddelanden eller sms. Andra misstag är att interna rutiner för personuppgiftshantering inte följs.

2 Förebygga personuppgiftsincidenter

2.1 Ett systematiskt informationssäkerhetsarbete

Att den mänskliga faktorn är den vanligaste orsaken till personuppgiftsincidenter kan bero på mänskliga misstag men även p.g.a. strukturella problem i verksamheten. Eftersom incidenterna kan innebära hög risk för enskildas friheter, även om de inte alltid gör det, är det viktigt att beakta den mänskliga faktorn i en verksamhets systematiska informationssäkerhetsarbete.

Enligt art. 32.1 i dataskyddsförordningen ska säkerhetsåtgärder vidtas i förhållande till risken för de enskildas friheter och rättigheter. I det ska behandlingens art, omfattning, sammanhang och ändamål beaktas så att en lämplig säkerhetsnivå kan säkerställas. Olika behandling krävs således för olika känsliga uppgifter. Arbetet måste därför pågå kontinuerligt genom planering, utvärdering och förbättring eftersom såväl verksamhet, teknik och risker förändras över tid.

2.2 Organisatoriska och tekniska säkerhetsåtgärder

Organisatoriska och tekniska säkerhetsåtgärder måste integreras i verksamhetens arbetssätt för att det ska bli enkelt att göra rätt och svårt att göra fel. Personuppgiftsansvariga måste ha ett löpande arbete med att skapa, implementera, kontrollera och följa upp de organisatoriska och tekniska åtgärder som krävs för att få ett lämpligt skydd för behandlingen av informationen och personuppgifterna – i förhållande till de risker den medför. Exempel på åtgärder för att skydda personuppgifter är att förhindra för medarbetare att spara ned information på löstagbar lagringsmedia, förhindra installation av program/appar som verksamheten inte godkänt och att lösenordskydda och kryptera e-post och bifogade filer.

Dessutom krävs en aktiv behörighetsstyrning i form av att medarbetare endast får tillgång till nödvändiga personuppgifter sett till vad de behöver för att kunna utföra sina arbetsuppgifter.

2.3 Processer som stärker det systematiska informationssäkerhetsarbetet

Dokumentation och implementering av processen för riskhanterings- och personuppgiftsincidenthanteringsprocesser behövs enligt 33.5 dataskyddsförordningen. Det bidrar till att förebygga, upptäcka och hantera personuppgiftsincidenter. Exempelvis kan en upptäckt av vad som orsakar personuppgiftsincidenter bidra till identifiering av utvecklingsbehov och vilka åtgärder och åtgärdsplaner som därmed bör vidtas.

2.4 En god säkerhetskultur

Med en säkerhetskultur avses värderingar, kunskaper, attityder och uppfattningar som chefer och anställda har till skyddet för personuppgifter.

Att säkerhetskulturen är god innebär att lärdomar från inträffade incidenter kommuniceras samt att det finns en medvetenhet om behovet av säkerhetsfrågor och kunskap om vad som ska göras i olika situationer. Ledningen bör dessutom vara engagerad i säkerhetsfrågor.

Wesslau Söderqvist Advokatbyrås rekommendationer

Att skydda personuppgifter är av yttersta vikt för att säkerställa integriteten och sekretessen för enskilda individer. För att minska den mänskliga faktorn som kan orsaka personuppgiftsincidenter rekommenderar Wesslau Söderqvist Advokatbyråföljande:

- Utbildning och medvetenhet: Säkerställ att anställda får adekvat utbildning om dataskydd och personuppgiftshantering. Det inkluderar att öka medvetenheten om riskerna, rättigheterna och skyldigheterna avseende personuppgifter.
- Starka autentiseringssystem: Inför robusta autentiseringssystem som kräver starka lösenord och eventuellt tvåfaktorsautentisering för att förhindra obehörig åtkomst till personuppgifter.
- Begränsa åtkomst och behörigheter: Se till att åtkomsten till personuppgifterna är begränsad till de anställda som behöver den för att utföra sina arbetsuppgifter.
- Datakryptering: Använd krypteringsteknik för att skydda känsliga personuppgifter både under lagring och överföring.
- Incidenthantering och rapportering: Etablera en tydlig process för rapportering av personuppgiftsincidenter och hur de ska hanteras. Detta innefattar att utbilda personalen om hur man identifierar och rapporterar incidenter.
- Uppdaterad IT-infrastruktur: Se till att den använda IT-infrastrukturen är uppdaterad med senaste säkerhetspatchar och att eventuella sårbarheter adresseras snabbt. Detta kan även förhindra eventuella incidenter.

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.

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.

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.