Trygg-Hansa Försäkring filial

Diarienummer:
DI-2021-1905

Datum:
2023-08-28

Beslut efter tillsyn enligt dataskyddsförordningen – Trygg-Hansa Försäkring filial

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Trygg-Hansa Försäkring filial (organisationsnummer 516403-8662) har behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen[1] genom att under perioden oktober 2018 – februari 2021 inte ha vidtagit lämpliga tekniska åtgärder och därigenom möjliggjort obehörig åtkomst till integritetskänsliga personuppgifter om dess kunder.

Integritetsskyddsmyndigheten beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Trygg-Hansa Försäkring filial ska betala en administrativ sanktionsavgift på 35 000 000 (trettiofem miljoner) kronor för överträdelsen av artiklarna 5.1 f och 32.1.

Redogörelse för tillsynsärendet

Bakgrund

Integritetsskyddsmyndigheten (IMY) mottog i december 2020 tips om att Moderna Försäkringar, filial till Tryg Forsikring A/S (Moderna Försäkringar) hade möjliggjort åtkomst för obehöriga personer till personuppgifter som berörde uppgifter av känslig karaktär om Moderna Försäkringars kunder. IMY inledde i mars 2021 tillsyn mot Moderna Försäkringar i syfte att granska om Moderna Försäkringar hade vidtagit lämpliga åtgärder för att säkerställa en säkerhetsnivå som var lämplig i förhållande till risken med personuppgiftsbehandlingen, i enlighet med artiklarna 5.1 f och 32 i dataskyddsförordningen.

IMY har som ett led i sin granskning tagit del av de 16 dokument som tipset avser. Det är fråga om flera olika typer av försäkringshandlingar, bland annat skadeanmälningar, fakturor, försäkringsbrev, försäkringsbeslut, svarskort avseende försäkringsersättning, omfattningsändring och begäran om kompletterande uppgifter för försäkringsutredning. Dokumenten innehåller ett stort antal kategorier av personuppgifter, såsom bl.a. namn, kontaktuppgifter, hälsouppgifter, personnummer, ekonomiska uppgifter, försäkringsinnehav, händelseförlopp (exempelvis tid, plats, ageranden och andra

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

uppgifter som den registrerade lämnat i fritextfält) och uppgifter avseende ägarskap och sakskador.

I april 2022 gick Moderna Försäkringar samman med Trygg-Hansa. Moderna Försäkringar bytte därefter namn till Trygg-Hansa filial (Trygg-Hansa) men fortsatte att bedriva verksamhet under samma organisationsnummer som tidigare (516403-8662). IMY kommer i beslutet att genomgående använda tillsynsobjektets nya namn, Trygg-Hansa, vid redogörelsen för det inträffade.

Redogörelse från tillsynsobjektet

Trygg-Hansa har i huvudsak uppgett följande.

Trygg-Hansa blev den 30 november 2020 kontaktat av en person per telefon som informerade om bristen. Mottagaren av tipset hos Trygg-Hansa förstod inte att det rörde sig om en möjlig incident, och bristen rapporterades därför inte vidare inom Trygg-Hansas organisation.

Säkerhetsbristen har inträffat på följande sätt:

1. En existerande eller ny potentiell kund har kontaktat kundtjänst per telefon och önskat få en offert för försäkring. Kundtjänsthandläggaren har efter avslutat telefonsamtal skickat ett SMS eller e-postmeddelande till kunden.
2. SMS:et eller e-postmeddelandet har innehållit en unik webbadress till en offertsida på Trygg-Hansas webbplats.
3. På offertsidan har det funnits klickbara länkar med webbadresser som leder till dokument med försäkringsinformation. Den person som kontaktat Trygg-Hansa enligt ovan har kunnat öppna dokumenten genom att klicka på länkarna.
4. Dessa dokument har haft webbadresser som vid tillfället kunnat modifieras av personen i dennes webbläsare genom att byta ut siffror mot andra siffror. På så sätt har personen kunnat hämta andra kunders dokument.

Det har funnits åtkomstmöjlighet via internet till uppgifter om ungefär 650 000 kunder under perioden oktober 2018 till och med då IMY kontaktade bolaget i slutet av februari 2021. De uppgifter som omfattas är namn, personnummer, kontaktuppgifter (adress, e-postadress, telefonnummer), försäkringsnummer, skadenummer, ekonomiska uppgifter, hälsouppgifter, försäkringsinnehav, uppgifter om ägarskap (såsom djurinnehav, fordonsuppgifter, fastighetsuppgifter), sakskador (såsom uppgifter om verkstad, ersättningsbesked), händelseförlopp (exempelvis tid, plats, ageranden och andra uppgifter som registrerade lämnat i fritextfält) och andra fritextfält. Det kan inte uteslutas att det även framgått uppgifter om lagöverträdelser (såsom i samband med skadeanmälningar) eller uppgifter om medlemskap i en fackförening (såsom när försäkring har tecknats med fackförening).

Analys av beteendemönster i loggar indikerar att 202 kunder sannolikt är direkt berörda på så sätt att uppgifter om dem (dokument) kan ha visats för någon obehörig. Såvitt Trygg-Hansa kunnat konstatera, efter granskning av loggar, är det endast tipsaren och IMY som fått åtkomst till dokumenten. För att liknande säkerhetsbrister inte skulle uppkomma, hade Trygg-Hansa före den aktuella händelsen vidtagit åtgärder genom att ta fram en IT-säkerhetspolicy, genomföra regelbundna penetrationstester och loggning på noder, transaktioner och system för kundhantering samt genom att hålla en årlig utbildning i dataskydd och säkerhet och löpande

utbildning för anställda med särskilt ansvar för frågor om dataskydd. Trygg-Hansa följer ISO 27001-standarden, vilket bl.a. innebär kontinuerliga penetrationstester och segmentering av nät. Trygg-Hansa genomförde inte en konsekvensbedömning rörande den aktuella behandlingen innan behandlingen påbörjades. Detta hade dock genomförts om personuppgiftsbehandlingen påbörjats idag eftersom Trygg-Hansa numera har rutiner för detta. Sedan ungefär mitten av 2019 implementerar Trygg-Hansa ett compliance-system där Trygg-Hansa på ett strukturerat sätt beskriver processer, data, lagring, avtal, leverantörer etc. tillsammans med konsekvensbedömningar.

För att komma åt dokument med information om andra kunder har det enligt Trygg-Hansa krävts kunskap om internetadressers struktur och hur man tar del av det underliggande innehållet med exempelvis en webbläsare. Vidare har det krävts ändring av en del av webbadressens siffror i Dokument-ID.

Sedan den aktuella händelsen identifierats har Trygg-Hansa vidtagit ytterligare säkerhetsåtgärder, såsom att åtgärda den aktuella bristen genom att kryptera och säkerställa att åtkomst endast kan ske av någon som är behörig. Efter att händelsen identifierats har Trygg-Hansa även genomfört två av varandra oberoende penetrationstester av två olika externa säkerhetsbolag, uppdaterat IT-säkerhetspolicyn, vidtagit åtgärder i syfte att förbättra rutinerna för testaktiviteter, beslutat att etablera ett arkitekturråd med säkerhetskontroll och kodgranskning vid utveckling, sett över den interna kundklagomålsprocessen och beslutat att genomföra ytterligare utbildning för anställda inom kundtjänst samt för utvecklare och testare.

Trygg-Hansa har också kontaktat registrerade via brev, samt i vissa fall via telefon, för att informera om vad som inträffat samt informerat på sin webbsida.

Motivering av beslutet

Har Trygg-Hansa säkerställt en lämplig säkerhetsnivå för personuppgifterna?

Tillämpliga bestämmelser
Enligt artikel 5.1 f i dataskyddsförordningen ska den personuppgiftsansvarige behandla personuppgifterna på ett sätt som säkerställer lämplig säkerhet, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

Enligt artikel 9.1 i dataskyddsförordningen är det som utgångspunkt förbjudet att behandla särskilda kategorier av personuppgifter (så kallade känsliga personuppgifter), bland annat uppgifter om hälsa. I artikel 9.2 anges vissa undantag från förbudet.

Av artikel 32.1 i dataskyddsförordningen följer att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Det ska, enligt samma bestämmelse, ske med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Vid bedömningen av lämplig säkerhetsnivå ska,

enligt artikel 32.2, särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Integritetsskyddsmyndighetens bedömning

Trygg-Hansa är personuppgiftsansvarig

Trygg-Hansa har uppgett att Trygg-Hansa är personuppgiftsansvarig för de personuppgiftsbehandlingar som tipset har avsett, vilket stöds av utredningen i ärendet. IMY bedömer att Trygg-Hansa är personuppgiftsansvarig för den behandling som tillsynen omfattar.

Behandlingen har inneburit stora integritetsrisker och krävt en hög skyddsnivå

Den personuppgiftsansvarige ska säkerhetsställa en säkerhet som är lämplig utifrån riskerna med behandlingen. Bedömningen av lämplig skyddsnivå ska göras med beaktande av bland annat behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Vid bedömningen ska särskild hänsyn tas till de risker som behandlingen medför, bland annat obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

IMY konstaterar att behandlingen av personuppgifter har omfattat ett stort antal registrerade inom Trygg-Hansas kärnverksamhet. Enligt Trygg-Hansas egna uppgifter har det varit fråga om uppgifter om ca 650 000 kunder.

IMY konstaterar vidare att behandlingen avsett ett stort antal personuppgifter om varje registrerad, vilket möjliggjort kartläggning av enskildas personliga förhållanden. De 16 dokument som IMY tagit del av inom ramen för tillsynsärendet innehåller ett stort antal kategorier av personuppgifter, såsom namn, kontaktuppgifter, hälsouppgifter, personnummer, ekonomiska uppgifter, försäkringsinnehav, händelseförlopp (exempelvis tid, plats, ageranden och andra uppgifter som den registrerade lämnat i fritextfält) och uppgifter avseende ägarskap och sakskador. Trygg-Hansa har även framfört att det inte kan uteslutas att det framgått uppgifter om lagöverträdelser eller uppgift om medlemskap i en fackförening.

Det har genom tillgång till ett dokument varit möjligt att direkt utläsa ett stort antal uppgifter om en enskild person. Det har således i vissa fall gått att få en utförlig bild av den registrerades personliga förhållanden med hjälp av dokumenten. Den omfattande personuppgiftsbehandlingen har varit särskilt integritetskänslig genom användningen av personnummer och andra identifieringsuppgifter som möjliggjort en tydlig och direkt koppling till enskilda individer.

IMY bedömer vidare att personuppgifternas karaktär i sig medfört en hög risk. Handlingarna har innehållit känsliga personuppgifter, bl.a. uppgifter om hälsa, som enligt huvudregeln i artikel 9.1 i dataskyddsförordningen inte får behandlas. Sådana uppgifter har getts ett utökat skydd, eftersom behandling av dem kan utgöra ett synnerligen allvarligt ingrepp i de grundläggande rättigheterna avseende respekt för privatlivet och skydd för personuppgifter.[2] Uppgifterna om hälsa har dessutom haft en

[2] EU-domstolens dom i mål C-184/20, Vyriausioji tarnybinės etikos komisija, EU:C:2019:773, punkt 126.

hög detaljnivå, så att det exempelvis gått att utläsa hur ett hälsoproblem uppkommit eller exakt vilket hälsotillstånd det rör sig om, vilket inneburit en ännu högre risk.

Materialet har även innehållit andra typer av uppgifter som är särskilt skyddsvärda. Detta gäller bland annat uppgifter om personnummer som omfattas av ett särskilt skydd enligt artikel 87 i dataskyddsförordningen och 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Enligt Trygg-Hansa kan det inte heller uteslutas att det förekommit uppgifter om lagöverträdelser som omfattas av ett starkt skydd enligt artikel 10 i dataskyddsförordningen, eftersom behandling av dem kan ha allvarliga effekter för enskilda. Det har också förekommit uppgifter om enskildas ekonomiska förhållanden.

Av handlingarna i ärendet framgår också att det har varit möjligt för registrerade att själva lämna information i formulär. I vissa skadeanmälningar har de registrerade lämnat ingående information i löptext avseende hälsoproblem och om hur skador uppkommit. Genom att Trygg-Hansa gett möjligheten att lämna uppgifter i löptext har det varit svårt för Trygg-Hansa att fullt ut kontrollera innehållet och vilka typer av uppgifter som framgår. Detta har medfört särskilda krav på att hantera dokumenten på ett säkert sätt.

Sammantaget har det stora antalet registrerade, den omfattande mängden uppgifter om varje person och den känsliga karaktären på uppgifterna medfört en hög risk för fysiska personers rättigheter och friheter. Obehörigt röjande av eller obehörig åtkomst till personuppgifterna har kunnat leda till allvarliga konsekvenser för de berörda personerna. Det har medfört krav på en hög skyddsnivå för behandlingen.

IMY konstaterar vidare att sammanhanget för personuppgiftsbehandlingen medfört ett ännu högre krav på skyddsnivån. Personuppgiftsbehandlingen har skett inom ramen för Trygg-Hansas kärnverksamhet. Dessutom har de registrerade berättigade förväntningar på en hög grad av konfidentialitet och ett robust skydd mot obehörig åtkomst till personuppgifter som behandlas i försäkringsverksamhet.[3] Uppgifterna har vidare samlats in för att kunna göra bedömningar och fatta beslut avseende registrerade, vilket är en typ av behandling av personuppgifter som kan innebära högre risker och kräver högre skydd.

Sammanfattningsvis har behandlingen varit av sådant slag att det ställts höga krav på säkerheten för uppgifterna, exempelvis genom behörighetskontroll, kryptering, loggning, åtkomstkontroll och hantering av tekniska sårbarheter.

Uppgifterna har inte skyddats på ett lämpligt sätt

IMY ska därefter bedöma om Trygg-Hansa har säkerställt den höga skyddsnivå som krävts.

IMY konstaterar att det inte har krävts att den som berett sig åtkomst till uppgifterna verifierat sin identitet för Trygg-Hansa eller på annat sätt verifierat sin behörighet att få åtkomst till dessa. Den som har haft tillgång till webbadresserna har således kunnat besöka webbplatserna och därigenom få tillgång till dokumenten med personuppgifter utan att det säkerställts att det varit fråga om en behörig person. Uppgifterna i

[3] Europarådet har i en rekommendation uttalat att medlemsstaterna ska säkerställa att anställda i försäkringsbolag som får del av personuppgifter ska omfattas av regler om tystnadsplikt (Recommendation rec[2002]9 on the protection of personal data collected and processed for insurance purposes). Se också prop. 2009/10:241 s. 43 och Ds 2011:7.

dokumenten har inte heller skyddats genom kryptering utan varit tillgängliga i klartext. Det har vidare varit fråga om uppgifter som direkt identifierat enskilda individer, dvs. uppgifterna har inte skyddats genom pseudonymisering. Trygg-Hansa har alltså gjort en stor mängd direkta personuppgifter av integritetskänslig karaktär tillgängliga på internet utan att vidta skyddsåtgärder i form av behörighetskontroll eller kryptering.

Trygg-Hansa har anfört att det krävs särskilda kunskaper för att komma åt dokument med personuppgifter via webbadresserna. IMY har dock observerat genom handlingarna och webbadresserna i ärendet att det har varit möjligt att komma åt dokumenten genom att ändra de sista siffrorna i webbadresserna. I vissa fall har de första sex siffrorna av åtta varit desamma i de olika webbadresserna, vilket betyder att få siffror i dessa fall har behövt ändras för att någon obehörig ska ha kunnat komma åt dokument.

Det har vidare gått att vidarebefordra webbadresserna, som leder till oskyddade uppgifter om försäkringstagare, till andra obehöriga personer. Dessa personer har i sin tur, utan att behöva ändra på några siffror, kunnat ta del av uppgifterna i dokumenten endast genom att klicka på webbadressen. Att det i vissa fall krävts att en enskild ändrat siffror i webbadressfältet för att komma åt dokument innebär inte att Trygg-Hansa vidtagit lämpliga åtgärder, till exempel autentisering och behörighetskontroll, för att hindra obehöriga från att ta del av de aktuella uppgifterna.

IMY har obehindrat kunnat ta del av uppgifter i dokumenten, enbart genom att besöka webbadresserna och utan att behöva ändra i adressfältet på webbläsaren.

IMY konstaterar mot denna bakgrund att Trygg-Hansa gjort en stor mängd integritetskänsliga personuppgifter åtkomliga i klartext på internet. Det har inte krävts någon autentisering för att säkerställa att endast rätt personer kunnat komma åt uppgifterna. Personer som fått eller berett sig obehörig åtkomst till de utskickade webbadresserna – eller manipulerade versioner av de utskickade webbadresserna – har således kunnat få tillgång till de integritetskänsliga personuppgifterna.

Utifrån dessa omständigheter gör IMY bedömningen att det funnits stora brister i skyddet av uppgifterna. Av utredningen framgår också att bristerna har lett till obehörig åtkomst till uppgifterna. IMY konstaterar att Trygg-Hansas egna loggar indikerar att 202 kunder sannolikt varit direkt berörda på så sätt att deras uppgifter kan ha visats för någon obehörig. Det bör dock framhållas att det faktum att det varit enkelt för obehöriga att bereda sig tillgång till en stor mängd personuppgifter av det aktuella slaget i sig är en allvarlig brist, oberoende av hur många inträffade fall av obehörig åtkomst som varit möjligt att konstatera.

Bristerna har varit av sådan grundläggande karaktär att Trygg-Hansa borde ha upptäckt och åtgärdat dem innan systemet infördes. Trygg-Hansa har dock infört systemet med bristerna och inte heller under den långa period då systemet användes förmått identifiera och åtgärda dem. Detta trots att Trygg-Hansa fick information om bristerna genom ett tips utifrån. IMY konstaterar vidare att personuppgiftsbehandlingen är en del av försäkringsbolagets kärnverksamhet och att Trygg-Hansa därmed borde ha haft god förmåga att säkerställa en säkerhet som varit lämplig utifrån behandlingens omfattning och känslighet.

IMY bedömer sammantaget att Trygg-Hansa inte har vidtagit lämpliga tekniska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Trygg-Hansa har således behandlat personuppgifter i strid med artikel 32.1 i

dataskyddsförordningen. Att ett stort antal personuppgifter, inklusive känsliga uppgifter, under en längre tid har behandlats på ett sätt som inneburit risk för obehörig åtkomst innebär enligt IMY att bristen i säkerheten varit av sådant allvarligt slag att den även innebär en överträdelse av artikel 5.1 f i dataskyddsförordningen.

Val av ingripande

Rättslig reglering
Om det har skett en överträdelse av dataskyddsförordningen har IMY ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 i dataskyddsförordningen.

Av artikel 58.2 i dataskyddsförordningen följer att IMY i enlighet med artikel 83 ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 i dataskyddsförordningen.

I artikel 83.2 anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras, men också vad som ska påverka sanktionsavgiftens storlek. Av betydelse för bedömningen av överträdelsens allvar är bland annat dess karaktär, svårighetsgrad och varaktighet.

Enligt artikel 83.4 ska det vid överträdelser av bland annat artikel 32 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Enligt artikel 83.5 ska det vid överträdelser av bland annat artikel 5 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i förordningen.

IMY:s bedömning

Sanktionsavgift ska påföras

IMY har gjort bedömningen att Trygg-Hansa har behandlat personuppgifter i strid med artikel artikel 32.1 samt att överträdelsen är av sådant allvarligt slag att det också är fråga om en överträdelse av principen om integritet och konfidentialitet i artikel 5.1 f.

Överträdelsen har skett genom att Trygg-Hansa behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har medfört risk för att obehöriga personer kunnat få åtkomst till ungefär 650 000 kunders uppgifter under perioden oktober 2018 till och med februari 2021. Personuppgifterna har bl.a. utgjorts av känsliga personuppgifter och personnummer, och obehörig åtkomst till dessa uppgifter medför en hög risk för de registrerades fri- och rättigheter.

IMY anser inte att det är frågan om mindre allvarliga överträdelser. Trygg-Hansa ska därför påföras en administrativ sanktionsavgift för överträdelserna. Vid bestämmande av sanktionsavgiftens storlek ska IMY beakta de omständigheter som anges i artikel 83.2 samt säkerställa att den administrativa sanktionsavgiften är effektiv, proportionell och avskräckande.

Moderbolagets årsomsättning ska läggas till grund för beräkningen

Vid bestämmande av maxbeloppet för en sanktionsavgift som ska påföras ett företag ska den definition av begreppet företag användas som EU-domstolen använder vid tillämpning av artiklarna 101 och 102 i EUF-fördraget (se skäl 150 i dataskyddsförordningen). Av domstolens praxis framgår att detta omfattar varje enhet som utövar ekonomisk verksamhet, oavsett enhetens rättsliga form och sättet för dess finansiering samt även om enheten i juridisk mening består av flera fysiska eller juridiska personer.

Vad som utgör ett företag ska således utgå från konkurrensrättens definitioner. Reglerna för koncernansvar i EU:s konkurrenslagstiftning kretsar kring begreppet ekonomisk enhet. Ett moderbolag och ett dotterbolag betraktas som en del av samma ekonomiska enhet när moderbolaget utövar ett avgörande inflytande över dotterbolaget. Det avgörande inflytandet (dvs. kontrollen) kan antingen uppnås genom ägande eller genom avtal. Av rättspraxis framgår att ett hundraprocentigt eller nästan hundraprocentigt ägande innebär en presumtion för att kontroll ska anses föreligga. Presumtionen kan dock motbevisas om företaget lämnar tillräcklig bevisning för att styrka att dotterbolaget agerar självständigt på marknaden.[4] För att motbevisa presumtionen måste företaget alltså tillhandahålla bevis som rör de organisatoriska, ekonomiska och rättsliga kopplingarna mellan dotterbolaget och dess moderbolag som visar att de inte utgör en ekonomisk enhet trots att moderbolaget innehar 100 procent eller nästan 100 procent av aktierna.[5]

Trygg-Hansa utgör en filial till det danska bolaget Tryg Forsikring A/S. Tryg Forsikring A/S utgör i sin tur ett helägt dotterbolag till Tryg A/S (”Tryg”). Enligt den ovan beskrivna presumtionen är det därför Trygs omsättning som ska läggas till grund för beräkning av det maximala sanktionsavgiftsbeloppet. För att frångå presumtionen krävs att Trygg-Hansa lämnar tillräcklig bevisning om att en annan omsättning ska läggas till grund för beräkningen.

Trygg-Hansa har anfört att det är den del av Trygs omsättning som motsvarar omsättningen för Moderna Försäkringar som bör läggas till grund för beräkningen av den maximala sanktionsavgiften. Trygg-Hansa har uppskattat denna omsättning till 2 406 294 859 danska kronor. I andra hand anser Trygg-Hansa att den maximala sanktionsavgiften bör baseras på Moderna Försäkringar och Trygs omsättning, varvid omsättningen för de bolag som har förvärvats av Tryg efter den tidsperiod som granskningen rör bör exkluderas från beräkningen av sanktionsavgiften. Trygg-Hansa har uppskattat denna omsättning till 23 622 304 333 danska kronor.

IMY har uppfattat Trygg-Hansas inställning så att den maximala sanktionsavgiften i första hand bör beräknas på den hypotetiska omsättning som filialen Moderna Försäkringar skulle ha haft under 2022 om inte Trygg-Hansa och Moderna Försäkringar hade gått samman i april 2022. Vidare har IMY uppfattat att Trygg-Hansa

[4] Mål C-97/08, punkt. 59-61
[5] Jfr. EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 125 och där redovisade avgöranden.

i andra hand anser att det är Tryg i den organisation som gällde när bristen fanns, i vilken Moderna Försäkringar är inkluderad, som utgör den ekonomiska enhet på vilken en maximal sanktionsavgift ska beräknas. Vid fastställande av den relevanta årsomsättningen för Tryg ska således den uppskattade omsättningen för de bolag som förvärvats efter överträdelsetidpunkten undantas.

Trygg-Hansa har till stöd för sin uppfattning sammanfattningsvis anfört att Moderna Försäkringar vid tidpunkten för granskningen var att se som en fristående verksamhet från Tryg i tekniskt och organisatoriskt hänseende. Trygg-Hansa har därvid lyft fram i huvudsak följande. Moderna Försäkringar var en filial enbart av skattemässiga skäl. Moderna Försäkringar bestämde självständigt över sitt agerande och hade en egen ledningsgrupp. Den servermiljö där den aktuella personuppgiftsbehandlingen skedde drevs och utvecklades av Moderna Försäkringar som också hade en egen IT-chef och IT-organisation. Endast kunder hos Moderna Försäkringar är berörda i detta ärende. Den personuppgiftsbehandling som granskats i ärendet var inte heller sanktionerad av Tryg och försäkringssystemen för de två verksamheterna var olika och skilda från varandra utan någon logisk, organisatorisk eller teknisk koppling.

De förvärvade bolagens omsättning bör enligt Trygg Hansa under alla omständigheter exkluderas från Trygs omsättning vid fastställandet av det maximala sanktionsbeloppet då ansvaret för en överträdelse enligt konkurrensrättslig praxis ska tillskrivas den som hade bestämmande inflytande över verksamheten vid tidpunkten för incidenten.

IMY gör följande bedömning. Trygg-Hansa är en filial till Tryg Forsikring A/S, och är därmed inte en självständig juridisk person. Trygg-Hansas omsättning ingår som en integrerad del av Trygs totala omsättning, och är helt integrerad med omsättningen för Tryg Forsikring A/S. Dessa omständigheter talar starkt för att Trygg-Hansa, Tryg Forsikring A/S och Tryg ska betraktas som en och samma ekonomiska enhet. De omständigheter som Trygg-Hansa lyft fram om att filialen, när den gick under namnet Moderna Försäkringar, haft en egen ledningsgrupp, IT-system och IT-organisation är inte något som i sig motsäger att det är fråga om en och samma ekonomiska enhet. Sammantaget bedömer IMY att det inte finns skäl att frångå presumtionen om att det är Trygs omsättning som ska läggas till grund för beräkningen av den maximala sanktionsavgiften.

Vad avser Trygg-Hansas inställning att omsättningen för de förvärvade bolagen ska exkluderas från beräkningen av sanktionsavgiftens maxbelopp gör IMY följande bedömning. Vid tidpunkten för överträdelsen var Trygg-Hansa liksom idag en filial till Tryg. Det har således inte skett några organisatoriska förändringar som i sig påverkar ansvarsförhållandet mellan filialen och bolaget. Det kan vidare noteras att det faktum att den relevanta årsomsättningen vid beräkningen av sanktionsavgiften är den årsomsättning som fastställdes det år som närmast föregår tillsynsmyndighetens beslut kan medföra att stora förändringar av årsomsättningen har skett sedan tidpunkten för överträdelsen, såväl minskningar som ökningar. Sådana förändringar kan bero på affärshändelser, såsom ökande eller minskande marknadsandelar och lönsamhet, eller förändringar av företagets organisation, såsom försäljningar eller förvärv av företag. Det finns i viss utsträckning möjlighet att ta hänsyn till sådana förändringar inom ramen för den proportionalitetsbedömning som alltid ska göras vid påförande av sanktionsavgifter enligt dataskyddsförordningen för att säkerställa att den påförda sanktionsavgiften är proportionell i det enskilda fallet. IMY bedömer däremot att det maximala sanktionsavgiftsbeloppet ska utgå från den fastställda årsomsättningen, utan avdrag för hypotetiska belopp för de företag som har förvärvats under denna tidsperiod.

IMY beaktar dock, såväl det faktum att överträdelsen skett i en begränsad del av Trygs verksamhet som de organisationsförändringar Trygg-Hansa har lyft fram, inom ramen för proportionalitetsbedömningen, vilket redovisas nedan under rubriken *”Sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande”.*

IMY bedömer sammantaget att det företags omsättning som ska läggas till grund för beräkning av de administrativa sanktionsavgifter som Trygg-Hansa kan åläggas är Trygs omsättning. Av Trygs årsredovisning för år 2022 framgår att årsomsättningen år 2022 var ca 33 938 000 000 danska kronor, vilket motsvarar ca 54 000 000 000[6] svenska kronor. Det högsta sanktionsbelopp som kan fastställas i ärendet är fyra procent av detta belopp, det vill säga cirka 2 160 000 000 svenska kronor.

Överträdelsens allvar

IMY gör följande överväganden avseende överträdelsens allvar. Att det funnits en möjlig obehörig åtkomst till ungefär 650 000 kunders uppgifter innebär att det funnits en risk för ett högt antal personer. Uppgifterna har omfattat känsliga personuppgifter, såsom hälsouppgifter, och andra uppgifter av integritetskänslig karaktär, såsom personnummer och ekonomiska uppgifter. Det kan inte uteslutas att uppgifter om lagöverträdelser har kunnat framgå. Personuppgiftsbehandlingen har inneburit betydande risker. Enskilda personer varit direkt identifierbara, vilket inneburit att uppgifter av känslig karaktär kunnat kopplas till identifierade personer. Uppgifterna har behandlats i ett sammanhang där de registrerade har berättigade förväntningar på en hög nivå av konfidentialitet och ett robust skydd mot obehörig åtkomst.

Uppgifterna har samlats in för att kunna göra bedömningar och fatta beslut avseende registrerade, vilket är en typ av behandling av personuppgifter som kan innebära högre risker och kräver högre skydd. Uppgifter om exempelvis ägarskap, som skulle kunna medföra en stöldrisk, har vid obehörig åtkomst enkelt kunnat kopplas till namn och adress. Med anledning av uppgifternas karaktär, och då dokumenten innehållit ett flertal samlade uppgifter, har eventuell obehörig åtkomst inneburit en hög risk för skadat anseende och förlust av konfidentialitet. Trygg-Hansas analys av beteendemönster i loggar indikerar att 202 kunder sannolikt är direkt berörda på så sätt att uppgifter om dem i dokument faktiskt kan ha visats för obehöriga, och IMY konstaterar att obehörig åtkomst skett vid åtminstone ett tillfälle, i samband med att tipset om brist lämnades till IMY.

Överträdelsen har även pågått under en längre tid, mellan oktober 2018 och den tidpunkt då IMY kontaktade Trygg-Hansa och påtalade bristen i februari 2021. Trygg-Hansa fick genom ett externt tips i november 2020 information om bristerna i säkerheten som hade kunnat användas för att åtgärda bristerna och därigenom minska integritetsriskerna för enskilda. Trygg-Hansa förmådde dock inte använda informationen för att åtgärda bristerna. Överträdelsen har gällt Trygg-Hansas kärnverksamhet, där Trygg-Hansa kan förutsättas ha kunskap om risker och krav för skyddet av personuppgifter.

Av EDPB:s riktlinjer framgår att tillsynsmyndigheten ska bedöma om överträdelsen är av låg, medel, eller hög allvarlighetsgrad.[7]

IMY har konstaterat att överträdelsen är så allvarlig att den även utgör en överträdelse av den grundläggande principen om integritet och konfidentialitet enligt artikel 5.1 f i

[6] Baserat på växelkursen den 23 augusti 2023, publicerad på riksbanken.se
[7] EDPB:s riktlinjer Guidelines 04/2022 on the calculation of administrative fines under the GDPR, punkt 60.

dataskyddsförordningen vilket innebär att det den maximala sanktionsavgift är 4 procent av årsomsättningen istället för 2 procent som gäller vid överträdelse av artikel 32. IMY bedömer sammantaget, att den aktuella överträdelsen har en medelhög allvarlighetsgrad inom spannet för överträdelser av artikel 5.1 f dataskyddsförordningen.

Trygg-Hansa har vidtagit ett antal åtgärder innan och efter att bristerna identifierades. Trygg-Hansa har bland annat låtit genomföra två av varandra oberoende penetrationstester av två olika externa säkerhetsbolag och inlett åtgärder i syfte att förbättra rutinerna för testaktiviteter. Trygg-Hansa har vidare beslutat att etablera ett arkitekturråd med säkerhetskontroll och kodgranskning vid utveckling, beslutat att genomföra ytterligare utbildning för anställda inom kundtjänst samt för utvecklare och testare. Trygg-Hansa har också lämnat viss information till registrerade om det inträffade. Denna och övriga åtgärder som beskrivits av Trygg-Hansa genomfördes dock efter att IMY kontaktade bolaget för att informera om bristen, och går inte utöver vad som kan förväntas. Åtgärderna är inte av sådan karaktär att de påverkar IMY:s bedömning i ärendet i förmildrande riktning.

Sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande

Den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande. Det innebär att beloppet ska bestämmas så att den administrativa sanktionsavgiften leder till rättelse, att den ger en preventiv effekt och att den dessutom är proportionerlig i förhållande till såväl aktuella överträdelser som till tillsynsobjektets betalningsförmåga.

Vid proportionalitetsbedömningen väger IMY in att Trygs årsomsättning har höjts betydande med anledning av förvärv av bolag som inte ingick i bolagets samlade omsättning vid tidpunkten för överträdelsen.

IMY tillmäter därtill stor betydelse till det faktum att överträdelsen, såvitt framkommit i ärendet, enbart skett i den svenska filialen. Att utgå enbart från koncernens omsättning i detta fall, där överträdelsen berört en begränsad del av verksamheten, skulle medföra att sanktionsavgiften sätts allt för högt i förhållande till vad som inträffat. IMY ser därför skäl att vid en proportionalitetsbedömning, med hänsyn tagen till den omsättning för Moderna Försäkringar som Trygg-Hansa redogjort för, fastställa sanktionsavgiften till ett avsevärt lägre belopp än vad en bedömning enbart baserat på Trygs omsättning hade resulterat i.

IMY bestämmer utifrån en samlad bedömning att Trygg-Hansa ska betala en administrativ sanktionsavgift på 35 miljoner kronor.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Evelin Palmér. Vid den slutliga handläggningen har även rättschefen David Törngren och enhetschefen Catharina Fernquist samt it- och informationssäkerhetsspecialisten Magnus Bergström medverkat.

Lena Lindgren Schelin, 2023-08-28 (Det här är en elektronisk signatur)

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.