Sammanfattning av IMY:s sanktionsbeslut mot Trygg-Hansa Försäkring filial.

Bakgrunden till tillsynsärendet är att IMY mottog i december 2020 tips om Trygg-Hansa Försäkring filial (”Trygg-Hansa”)[1] möjliggjort att obehöriga personer haft åtkomst till personuppgifter av känslig karaktär. Enligt sanktionsbeslutet ska det genom hemsidan funnits tillgång till informationen utan större teknisk förmåga, kortfattat kunde obehöriga bereda sig tillträde till personuppgifter genom att ändra siffror i webbadressen. Det har funnits åtkomstmöjlighet, via internet, till uppgifter om ca 650 000 kunder från oktober 2018 till februari 2021.

Trygg-Hansa har behandlat personuppgifter med en otillräcklig säkerhetsnivå, vilket har medfört risk för att obehöriga personer kunnat få åtkomst till uppgifterna. Därtill har personuppgifterna i viss utsträckning varit känsliga som medför en hög risk för de registrerades fri- och rättigheter. Sammantaget fick Trygg-Hansa en administrativ sanktionsavgift på 35 miljoner kronor.

Behandlingen av personuppgifter har inneburit stora integritetsrisker och därmed krävt hög skyddsnivå

Enligt IMY:s granskning har det funnits tillgång till en stor mängd personuppgifter om de registrerade, och obehöriga har genom åtkomsten kunnat få en utförlig bild av registrerades personliga förhållanden. IMY anmärkte att personuppgifternas karaktär i sig medfört en hög risk, eftersom de har innehållit särskilt känsliga personuppgifter, till exempel medlemskap i fackförbund, som generellt sett är förbjuden att behandla.[2] Nämnda personuppgifter 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. Likaså har andra uppgifter behandlats, som exempelvis personnummer och eventuella uppgifter om lagöverträdelser av de registrerade, vilka anses särskilt skyddsvärda enligt GDPR.[3]

I ärendet har registrerade haft möjlighet att själva fylla i information i formulär, inklusive detaljer om hälsoproblem och skadeorsaker i löptext. Därmed har Trygg-Hansa haft det svårt att fullständigt kontrollera och säkerställa innehållet i dessa uppgifter, vilket även ställer krav på särskilda åtgärder för dokumenthantering av säkerhetsskäl.

Sammantaget medför behandlingen av personuppgifter att höga krav ställs på säkerheten för uppgifterna, exempelvis genom behörighetskontroll, kryptering, loggning, åtkomstkontroll och hantering av tekniska sårbarheter.

[1] Trygg-Hansa Försäkring filial hette ursprungligen Moderna Försäkringar när bolaget var filial till Tryg Forsikring A/S. Under 2022 gick Moderna Försäkringar tillsammans med Trygg-Hansa. I och med att bolagen gick samman bytte Moderna Försäkringar namn till Trygg-Hansa Försäkring filial, men fortsatte att bedriva sin verksamhet under samma organisationsnummer som tidigare.
[2] GDPR, artikel 9.
[3] GDPR, artikel 9 samt 87 och 3 kap. 10 § lagen (2018:218) med kompletterade bestämmelser till EU:s dataskyddsförordningen.

Uppgifterna har inte skyddats på ett lämpligt sätt

Trygg-Hansa har ur ett säkerhetsperspektiv inte vidtagit tillräckliga åtgärder för att säkerställa att obehöriga personer inte har tillgång till uppgifterna. Det krävdes enbart tillgång till webbplatsen för att bereda sig åtkomst till personuppgifter, således hade inte uppgifterna skyddats genom kryptering och pseudonymisering eller behörighetskontroll och autentisering. IMY:s bedömning är att det inte krävts särskilda kunskaper för att få tillgång till dessa uppgifter.

IMY har konstaterat allvarliga brister i Trygg-Hansas skydd av integritetskänsliga personuppgifter på internet. Dessa uppgifter har varit tillgängliga i klartext utan någon autentisering, vilket har möjliggjort obehörig åtkomst. Upp till 202 kunder kan ha drabbats av detta säkerhetshål enligt Trygg-Hansas egna loggar.

Enligt IMY var bristerna så grundläggande att de borde ha upptäckts och åtgärdats innan systemet infördes. Trots att bolaget fick information om problemen genom ett externt tips, lyckades de inte identifiera och åtgärda dem under en lång tidsperiod när systemet användes.

Bristerna är särskilt allvarliga med tanke på att personuppgiftsbehandlingen är en central del av försäkringsbolagets kärnverksamhet. IMY:s bedömning är att Trygg-Hansa borde ha haft kapacitet att säkerställa en lämplig säkerhetsnivå med tanke på behandlingens omfattning och känslighet. Sammantaget är detta ett allvarligt misslyckande i hanteringen av integritetskänsliga data och en potentiell risk för många individers personlig information.

Medskick till SFM:s medlemmar

Försäkringsförmedlare bör ha en god förståelse för vilka personuppgifter som den behandlar i sin verksamhet. Detta inbegriper att identifiera vilka särskilt känsliga personuppgifter som försäkringsförmedlaren behandlar. Eftersom många av de personuppgifter som ett försäkringsföretag behandlar också kan vara föremål för personuppgiftsbehandling hos försäkringsförmedlare kan det aktuella sanktionsbeslutet vara en anledning att se över vidtagna åtgärder kopplat till säkerhetsnivån för personuppgifter. Av sanktionsbeslutet framgår att behandlingen av personuppgifter som är förenade med höga risker medför höga krav på säkerheten för uppgifterna. Ur detta perspektiv bör försäkringsförmedlare tillgodose lämpliga säkerhetsåtgärder genom exempelvis kryptering och pseudonymisering av personuppgifter samt behörighetskontroller och autentisering vid åtkomst till webbplatser.