Integritetsskydds myndigheten

Länsförsäkringar AB

106 50 Stockholm

Diarienummer:
DI-2021-5568

Ert diarienummer:

Datum:
2024-12-19

Beslut efter tillsyn enligt dataskyddsförordningen - Länsförsäkringar AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Länsförsäkringar AB (organisationsnummer 502010-9681) behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1] genom att under perioden den 10 mars 2021 till och med den 4 juni 2021 inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgifter vid användning av analysverktyget Meta-pixeln.

Integritetsskyddsmyndigheten ger Länsförsäkringar AB en reprimand enligt artikel 58.2 b i dataskyddsförordningen för den konstaterade överträdelsen.

Redogörelse för tillsynsärendet

Utgångspunkt för tillsynen

Integritetsskyddsmyndigheten (IMY) mottog den 7 juni 2021 en anmälan om en personuppgiftsincident från Länsförsäkringar AB och ytterligare 26 bolag inom Länsförsäkringsgruppen. Av anmälan framgick att bolagen vid användning av Facebooks (ägarbolaget numera Meta) tjänst Facebook-pixel (numera Meta-pixel) obehörigen fört över personuppgifter till Meta för matchning mot Facebookprofiler om ett okänt antal personer som besökt webbplatsen www.lansforsakringar.se och som där lämnat information i formulär. Överföringen orsakades av att funktionen Avancerad matchning aktiverats av misstag. Överföringen till Meta pågick under perioden den 10 mars 2021 till och med den 4 juni 2021. Bland de uppgifter som förts över fanns identifierande information och kontaktinformation. Länsförsäkringar AB fick kännedom

[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

om det inträffade av en utomstående. Så snart Länsförsäkringar AB fick kännedom om det inträffade avaktiverade Länsförsäkringar AB funktionen.

Den 8 juni 2021 kompletterades anmälan om personuppgiftsincident till att omfatta ytterligare ett bolag i Länsförsäkringsgruppen. Med hänsyn till att det av anmälan framgick att samtliga bolag som omfattades av anmälan var personuppgiftsansvariga för den incident som inträffat på webbplatsen www.länsförsäkringar.se inledde IMY tillsyn mot Länsförsäkringar AB och de övriga bolag inom Länsförsäkringsgruppen som omfattades av personuppgiftsincidenten i syfte att utreda de uppgifter som förekom i bolagens anmälan om personuppgiftsincident. Detta ärende har mot den bakgrunden handlagts tillsamman med tillsynsärendena mot de övriga bolagen. Tillsynerna har avgränsats till att avse i vad mån bolagen vidtagit lämpliga tekniska och organisatoriska åtgärder för att skydda webbplatsbesökares personuppgifter i enlighet 32.1 i dataskyddsförordningen under perioden den 10 mars 2021 till och med den 4 juni 2021 i samband med den överföring av personuppgifter som skett till Meta genom Meta-pixelns funktion Avancerad matchning.

Handläggningen vid IMY har skett genom skriftväxling.

Vad Länsförsäkringar AB har uppgett

Länsförsäkringar AB och de övriga bolag inom Länsförsäkringsgruppen som omfattas av IMY:s tillsyn har yttrat sig gemensamt till IMY. Av yttrandet och bolagens anmälan om personuppgiftsincident framgår i huvudsak följande gällande de frågor som är föremål för IMY:s granskning.

Personuppgiftsansvar
Länsförsäkringar AB och de övriga bolag som omfattas av IMY:s tillsyn är personuppgiftsansvariga för införandet av Meta-pixeln, funktionen Avancerad matchning och den efterföljande överföringen av personuppgifter till Meta.

Den ursprungliga implementeringen av Meta-pixeln
Länsförsäkringar AB har interna styrdokument och formaliserade rutiner för behandling av personuppgifter. Till exempel finns en för personalen lättillgänglig handbok om behandling av personuppgifter med innehåll om vad som ska iakttas angående pågående eller planerade nya personuppgiftsbehandlingar. Handboken innehåller även checklistor som ska användas så att tillräckligt underlag ska kunna tas fram för de bedömningar, beslut och åtgärder som krävs innan nya personuppgiftsbehandlingar påbörjas eller pågående personuppgiftsbehandlingar förändras. Syftet är att bestämmelserna i dataskyddsförordningen och övrig tillämplig dataskyddslagstiftning ska kunna efterlevas. Sådana dokument och rutiner är tillämpliga bland annat vid införande av nya funktioner på webbplatsen.

All personal genomgår en grundläggande utbildning i dataskydd och riktade utbildningsinsatser görs avseende vissa personalkategorier beroende på om och i vilken utsträckning deras arbetsuppgifter innebär att de deltar vid pågående eller planerade behandlingar av personuppgifter.

Meta-pixeln har införts på webbplatsen för att Länsförsäkringar AB ska kunna bedriva effektiv digital marknadsföring genom att rikta relevanta kommersiella budskap till användare utifrån vilka finansiella tjänster som användarna visat intresse för på webbplatsen.

Aktivering av delfunktionen Avancerad matchning i Meta-pixeln
Länsförsäkringar AB har inte i behörig ordning fattat beslut om att tjänsten Avancerad matchning skulle tas i bruk. Länsförsäkringar AB har inte haft för avsikt att aktivera tjänsten. Det har inte varit Länsförsäkringar AB:s avsikt att behandla andra personuppgifter än IP-adresser inom ramen för användningen av Meta-pixeln. Vid en närmare undersökning av orsaken till att tjänsten Avancerad matchning kom att aktiveras, har det kunnat konstateras att personal hade vidtagit vissa åtgärder utan att inse att åtgärderna ledde till att tjänsten togs i bruk av samtliga bolag som använder webbplatsen länsförsäkringar.se.

Länsförsäkringar AB:s överföring av personuppgifter via funktionen Avancerad matchning till Meta
Under den period som Avancerad matchning var i bruk har personuppgifter överförts till Meta i så kallad hashad krypteringsform[2] om de användare som har fyllt i uppgifter i formulär på webbplatsen.

Personuppgifterna har matchats med facebookprofiler för att rikta annonser på Facebook utifrån de sidor som användaren besökt på webbplatsen.

Exakt hur Avancerad matchning har påverkat annonseringen är inte fastställt. Att detta resulterat i riktad kommunikation från Länsförsäkringar AB på Facebook kan inte uteslutas. Funktionen bidrog till att följande uppgifter överfördes:

- För- och efternamn,
- Telefonnummer,
- E-postadress och
- Boendeort.

Det har dock inte i samtliga fall varit samtliga uppgifter för varje registrerad som förts över till Meta, utan det kan ha förekommit enskilda uppgifter, exempelvis enbart en e-postadress.

Uppgifterna lämnades ut från formulär på Länsförsäkringar AB:s webbplats och ingen särskiljning kring huruvida det var en kund eller inte som fyllde i formulären har gjorts. De formulär som kunde fyllas i av användare och som medförde att de ifyllda uppgifterna överfördes till Meta var exempelvis formulär för anmälan till nyhetsbrev eller intresse av att få veta mer om en produkt eller tjänst. Inga uppgifter om att en användare var eller blev kund framgick av den information i formulären som delades med Meta.

Enligt uppgift från Meta har personuppgifterna raderats inom 48 timmar efter mottagandet. På grund av att personuppgifterna överfördes till Meta i hashad krypteringsform och har raderats har det inte varit möjligt att identifiera vilka eller hur många registrerade som har påverkats av incidenten.

Åtgärder som vidtagits efter personuppgiftsincidenten
Med anledning av incidenten har Länsförsäkringar AB sett över sina rutiner och webbplatsens kodstruktur för att förhindra att liknande situationer inträffar. En dialog

[2] IMY:s tillägg: Hashning är en kryptografisk envägsfunktion som kan användas för att åstadkomma pseudonymisering, som är en möjlig säkerhetsåtgärd enligt artikel 32 i dataskyddsförordningen, genom att personuppgifter ersätts med en så kallad hashsumma. Det innebär att de ersatta personuppgifterna inte är tillgängliga i klartext och att det behövs kompletterande uppgifter för att det ska gå att identifiera den registrerade.

med Meta och distributörer av Metas tjänster har också inletts för att minimera risken för att personal oavsiktligt aktiverar Metas tjänster och funktioner som skett i detta fall.

Länsförsäkringar AB har vidtagit följande tekniska och organisatoriska säkerhetsåtgärder för att förebygga och upptäcka otillåten utgående trafik motsvarande den som upptäcktes den 4 juni 2021.

Ett flertal organisatoriska säkerhetsåtgärder har vidtagits såsom översyn av samtliga behörigheter och behörighetsnivåer för medarbetare med tillgång till webbaserade verktyg. Skärpta behörighetskrav har införts, exempelvis kräver samtliga kodförändringar rörande spårning på webbplatsen godkännande av två behöriga medarbetare. Berörda medarbetare har också erhållit ytterligare utbildning för att öka medarbetarnas kunskap om lagstiftning kring mätning och spårning i digitala kanaler.

För att ytterligare minska risken för otillåten utgående trafik genomförs regelbundet även manuella kontroller av inställningar och dataflöden i de verktyg som används som en del i marknadsprocessen. En utredning pågår även internt för att se över förutsättningarna för att automatiskt kunna genomföra kontroller av dataflöden från webbplatser till tredje part.

Den aktuella Meta-pixeln är avstängd och det finns inte någon plan på att aktivera den igen. Länsförsäkringar AB har vidtagit tekniska säkerhetsåtgärder som omöjliggör tjänsten Avancerad matchning även om Meta-pixeln i framtiden skulle återinföras. Länsförsäkringar AB har även utvecklat ett filter för att hindra överföring av personuppgifter från fritextfält.

Motivering av beslutet

Tillämpliga bestämmelser m.m.

Av artikel 95 i dataskyddsförordningen följer att dataskyddsförordningen inte ska innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter, för sådana områden som redan omfattas av skyldigheter enligt det så kallade eDataskyddsdirektivet[3]. eDataskyddsdirektivet har genomförts i svensk rätt genom lagen (2022:482) om elektronisk kommunikation (LEK), där bland annat insamling av uppgifter genom webbkakor regleras.

Enligt 9 kap. 28 § LEK, som genomför artikel 5.3 i eDataskyddsdirektivet, får uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Vidare framgår att detta inte hindrar sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt. LEK trädde i kraft den 3 juni 2022. Under den i ärendet aktuella tiden gällde dock samma krav enligt 6 kap. 18 § lagen om (2003:389) om elektronisk kommunikation. Det är Post- och telestyrelsen som är tillsynsmyndighet enligt LEK (1 kap 5 § förordningen (2022:511) om elektronisk kommunikation).

[3] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

Europeiska dataskyddsstyrelsen (EDPB) har yttrat sig över samspelet mellan eDataskyddsdirektivet och dataskyddsförordningen. Av yttrandet följer bl.a. att den nationella tillsynsmyndighet som utsetts enligt eDataskyddsdirektivet ensamt är behörig att övervaka efterlevnaden av direktivet. Däremot är tillsynsmyndigheten enligt dataskyddsförordningen behörig tillsynsmyndighet för den behandling som inte regleras särskilt i eDataskyddsdirektivet.[4]

EDPB har den 7 oktober 2024 antagit riktlinjer gällande den tekniska omfattningen av artikel 5.3 i eDataskyddsdirektivet. I riktlinjerna anges bland annat att ett vanligt tillvägagångssätt för företag är användningen av unika identifierare eller beständiga identifierare. Sådana identifierare kan härledas från beständiga personuppgifter (namn, efternamn, mejladress, telefonnummer etc.) vilka hashas på användarens enhet, samlas in och delas mellan flera personuppgiftsansvariga för att unikt identifiera en person genom olika datamängder (användardata som samlats in genom användandet av en webbsida eller applikation, kundrelationshantering som avser online- eller offlineköp eller prenumerationer etc.). I riktlinjerna klargörs att omständigheten att informationen matas in av användaren inte utesluter tillämpligheten av artikel 5.3 i eDataskyddsdirektivet eftersom informationen tillfälligt lagras på terminalen innan den samlas in. När det gäller insamling genom unika identifierare på webbsidor eller mobilapplikationer ger den insamlande parten instruktioner till webbläsaren (genom kod som distribueras till terminalen/klienten) som skickar informationen. Därmed sker en hämtning av uppgifter och artikel 5.3 är tillämplig.[5] Den omständigheten att den insamlande parten som instruerar terminalen att skicka tillbaka informationen inte är densamma som den som tar emot informationen utesluter inte tillämpligheten av artikel 5.3 i eDataskyddsdirektivet.[6]

Personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Den personuppgiftsansvarige ska enligt artikel 5.2 i datasskyddförordningen ansvara för och kunna visa att de grundläggande principerna i artikel 5.1 i dataskyddsförordningen följs (principen om ansvarsskyldighet).

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. Vid bedömningen av vilka tekniska och organisatoriska åtgärder som är lämpliga ska den personuppgiftsansvarige beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.

Enligt artikel 32.1 omfattar lämpliga skyddsåtgärder, när det är lämpligt,

- Pseudonymisering och kryptering av personuppgifter.

[4] Yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter, antaget den 12 mars 2019, punkt 68 och 69.
[5] EDPB:s riktlinjer Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, punkt 61–63.
[6] Ibid, punkt 34.

- Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna.
- Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.
- Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Enligt artikel 32.2 i dataskyddsförordningen ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för 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.

I skäl 75 till dataskyddsförordningen anges faktorer som ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter. Bland annat nämns förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt samt om behandlingen avser uppgifter om hälsa eller sexualliv. Vidare ska beaktas om behandlingen gäller personuppgifter om sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

I skäl 76 till dataskyddsförordningen anges att hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller hög risk**.**

Integritetsskyddsmyndighetens bedömning

IMY ska inledningsvis ta ställning till om dataskyddsförordningen är tillämplig och om IMY är behörig tillsynsmyndighet. Om så är fallet ska IMY pröva frågan om Länsförsäkringar AB är personuppgiftsansvarig och om bolaget i så fall har vidtagit lämpliga säkerhetsåtgärder enligt artikel 32 i dataskyddsförordningen för att skydda de personuppgifter som behandlats vid användning av Meta-pixeln med funktionen Avancerad matchning aktiverad under perioden den 10 mars till och med den 21 juni 2021.

IMY är behörig tillsynsmyndighet
IMY:s granskning tar sikte på Länsförsäkringar AB:s användning av Meta-pixeln, ett scriptbaserat verktyg i form av ett kodstycke, på Länsförsäkringar AB:s webbplats, där funktionen Avancerad matchning senare kom att aktiveras. Funktionen Avancerad matchning har medfört att Meta-pixeln instruerat användarnas webbläsare att samla in och hasha information i form av de personuppgifter som användarna angett på sidan. Utifrån dessa uppgifter har en unik identifierare skapats som tillfälligt lagrats i användarens terminal och sedan förts över till, och därmed hämtats av, Meta för matchning. Den aktuella behandlingen har därmed omfattat både sådan lagring i och hämtning från användares terminalutrustning som avses i 9 kap. 28 § i LEK, och motsvarande bestämmelse i 6 kap. 18 § lagen om (2003:389) om elektronisk kommunikation.

Post- och telestyrelsen är ensamt behörig att utöva tillsyn över tillämpningen av LEK. IMY:s granskning avser dock om Länsförsäkringar AB vidtagit tillräckliga

säkerhetsåtgärder, vilket inte är något som regleras särskilt i LEK. IMY är därmed behörig att utreda den fråga som tillsynsärendet gäller.

Länsförsäkringar AB är personuppgiftsansvarig
Länsförsäkringar AB har uppgett att Länsförsäkringar AB är personuppgiftsansvarig för den personuppgiftsbehandling som granskats i ärendet. Av utredningen framgår att syftet med att implementera och använda Meta-pixeln varit att optimera Länsförsäkringar AB:s marknadsföring. Genom att behandla uppgifter om besökares beteende på webbplatsen har Länsförsäkringar AB:s marknadsföring på Metas tjänst Facebook således kunnat optimeras.

IMY konstaterar att Länsförsäkringar AB har bestämt hur behandlingen ska gå till och för vilket ändamål personuppgifterna ska behandlas. IMY bedömer därför att det är Länsförsäkringar AB som enligt artikel 4.7 i dataskyddsförordningen är personuppgiftsansvarig för den personuppgiftsbehandling som tillsynen omfattar.

Har Länsförsäkringar AB säkerställt en lämplig säkerhetsnivå för personuppgifterna?

Behandlingen har innefattat en risk

Den personuppgiftsansvarige ska vidta åtgärder för att säkerhetsställa en skyddsnivå 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. På grundval av en objektiv bedömning ska fastställas huruvida behandlingen innebär en risk eller hög risk.

Av utredningen i ärendet framgår att Länsförsäkringar AB genom att införa Meta-pixeln och funktionen Avancerad matchning oavsiktligt fört över uppgifter till Meta om namn- och kontaktuppgifter avseende webbplastbesökare som lämnat ifrån sig sådana uppgifter i formulär på Länsförsäkringar AB:s webbplats.

IMY gör följande bedömning av riskerna med behandlingen av de registrerades personuppgifter.

De registrerade har lämnat ifrån sig bland annat namn- och kontaktuppgifter till ett företag som bedriver försäkringsverksamhet och uppgifterna har därmed förekommit i ett sammanhang där de registrerade måste ha kunnat förvänta sig en hög grad av konfidentialitet. Länsförsäkringar AB har haft rutiner på plats som följts vid införandet av Meta-pixeln. Meta-pixeln har därmed varit införd på ett sådant sätt att när funktionen Avancerad matchning slogs på möjliggjordes endast överföring av ett begränsat antal uppgifter om en registrerad och som inte avslöjade om den registrerade var kund hos Länsförsäkringar AB eller som rörde uppgifter i en registrerads eventuella kundförhållande med Länsförsäkringar AB. Hur många registrerade som har påverkats av incidenten har inte kunnat identifieras.

Sammanfattningsvis bedömer IMY att behandlingen, med hänsyn till sin art, omfattning och sammanhanget, har inneburit en risk som medfört ett krav på Länsförsäkringar AB att säkerställa en skyddsnivå som är lämplig i förhållande till den aktuella risken. Åtgärderna skulle bland annat säkerställa att personuppgifterna skyddades mot förlust av kontroll.

Länsförsäkringar AB har inte vidtagit tillräckliga skyddsåtgärder

IMY ska därefter bedöma om Länsförsäkringar AB har säkerställt den skyddsnivå som krävts för att skydda de registrerades personuppgifter.

Av Länsförsäkringar AB:s uppgifter framgår att de har formaliserade rutiner för att säkerställa en korrekt behandling av personuppgifter inför, i samband med och efter införandet av nya funktioner på webbplatsen och att dessa rutiner finns dokumenterade i Länsförsäkringar AB:s styrdokument.

IMY konstaterar att Länsförsäkringar AB således haft organisatoriska åtgärder på plats i form av rutiner som dokumenterats i Länsförsäkringar AB:s styrdokument. Länsförsäkringar AB har dock i det aktuella fallet inte följt sina rutiner. Länsförsäkringar AB har haft Meta-pixeln införd på Länsförsäkringar AB:s webbplats och funktionen Avancerad matchning i Meta-pixeln har därefter aktiverats utan att Länsförsäkringar AB varit medvetet om det. Som en konsekvens av att Länsförsäkringar AB vid införandet av denna funktion inte följt sina rutiner och dokumenterat vad som skett har det inte varit möjligt för Länsförsäkringar AB att upptäcka och i efterhand verifiera hur eller av vem denna funktion aktiverades.

Som en följd av att funktionen Avancerad matchning aktiverats utan Länsförsäkringar AB:s vetskap har Länsförsäkringar AB fört över uppgifter till Meta om webbplatsbesökare som inte var avsedda att överföras.

Länsförsäkringar AB har således saknat förmåga att upptäcka den pågående överföringen av personuppgifter till Meta. IMY anser att Länsförsäkringar AB borde ha haft ett sådant systematiskt säkerhetsarbete att detta skulle ha upptäckts av Länsförsäkringar AB. Ett sådant säkerhetsarbete innefattar att kontroller görs med viss regelbundenhet. Eftersom Länsförsäkringar AB endast har haft rutiner för att följa upp dokumenterade förändringar som utförts enligt uppsatta rutiner, har Länsförsäkringar AB saknat förmåga att upptäcka och åtgärda förändringar som, liksom i det aktuella fallet, genomförts utan att rutinerna följts. Mot denna bakgrund konstaterar IMY att Länsförsäkringar AB har saknat tekniska och organisatoriska säkerhetsrutiner för att systematiskt följa upp och upptäcka oavsiktliga förändringar i sina system.

Som en följd av att Länsförsäkringar AB dels inte tillämpat sina organisatoriska säkerhetsrutiner när Länsförsäkringar AB införde funktionen Avancerad matchning, dels saknat organisatoriska och tekniska säkerhetsrutiner för att upptäcka överföringar har personuppgifter om ett okänt antal personer obehörigen förts över till Meta.

IMY konstaterar sammanfattningsvis att Länsförsäkringar AB vid användningen av Meta-pixeln inte har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som varit lämplig i förhållande till risken. Detta innebär att Länsförsäkringar AB under perioden den 10 mars 2021 till och med den 4 juni 2021 har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Val av ingripande

Av artikel 58.2 i och artikel 83.2 i dataskyddsförordningen framgår att IMY bland annat har befogenhet att påföra en administrativ sanktionsavgift. Beroende på omständigheterna i det enskilda fallet ska en administrativ sanktionsavgift påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2, som t.ex. förelägganden och förbud. 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. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Den konstaterade överträdelsen har skett genom att Länsförsäkringar AB behandlat personuppgifter med en otillräcklig säkerhetsnivå vilket lett till att Länsförsäkringar AB fört över fler personuppgifter än vad som varit avsett om ett okänt antal registrerade till Meta under knappt tre månaders tid. Länsförsäkringar AB har saknat förmåga att under denna tid på egen hand upptäcka överföringen av personuppgifter till Meta. Överträdelsen har skett i försäkringsverksamhet där de registrerade måste anses ha haft en berättigad förväntan på hög grad av konfidentialitet. Länsförsäkringar AB har dock vidtagit åtgärder som begränsat intrånget i de registrerades personliga integritet. Länsförsäkringar AB har vid införandet av Meta-pixeln placerat den på ett sådant sätt på webbplatsen att uppgifter om att en registrerad var kund hos Länsförsäkringar AB inte kunnat utläsas av de uppgifter som fördes över till Meta när funktionen Avancerad matchning aktiverades. Det har därmed inte varit fråga om uppgifter som omfattats av tystnadsplikt. Det har varit fråga om relativt få personuppgifter avseende varje registrerad som förts över till Meta och det har inte avsett integritetskänsliga uppgifter. Vidare har överföringen skett under ett kortare tidsintervall. Personuppgifterna har förts över i hashat, det vill säga oläsligt, format till en enda mottagare och det rör sig därmed inte om ett okontrollerat röjande där uppgifterna exempelvis delats till många obehöriga eller funnits publikt tillgängliga. Vid en sammantagen bedömning finner IMY att det är fråga om en sådan mindre överträdelse som avses i skäl 148 till dataskyddsförordningen och att Länsförsäkringar AB därför ska ges en reprimand.

Detta beslut har fattats av enhetschefen Catharina Fernquist efter föredragning av seniora juristen Hans Kärnlöf. Vid den slutliga handläggningen av ärendet har även it- och informationssäkerhetsspecialisten Petter Flink medverkat.

Catharina Fernquist

Kopia till
Länsförsäkringar AB:s dataskyddsombud

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.