If Skadeförsäkring AB

Diarienummer:
DI-2021-4355

Datum:
2023-01-19

Beslut efter tillsyn enligt dataskyddsförordningen – If Skadeförsäkring

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att If Skadeförsäkring AB, den 6 november 2020, har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1]. Det har skett genom att If Skadeförsäkring AB till den klagande har skickat känsliga personuppgifter om denne i ett e-postmeddelande utan att använda en tillräckligt säker krypteringslösning. If Skadeförsäkring AB har därmed inte vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen.

Integritetsskyddsmyndigheten ger If Skadeförsäkring AB en reprimand enligt artikel 58.2 b dataskyddsförordningen för den konstaterade överträdelsen.

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn beträffande If Skadeförsäkring AB (If eller bolaget) med anledning av ett klagomål.

Den klagande har angett att personuppgifter rörande hälsa har överförts via e-post utan att ha skyddats av kryptering hela vägen från avsändaren till mottagaren, dvs. genom en s.k. end-to-end-kryptering. IMY har med anledning av klagomålet inlett tillsyn i syfte att utreda om If har säkerställt en lämplig säkerhetsnivå i enlighet med artikel 32 i dataskyddsförordningen för den aktuella behandlingen.

Handläggningen har skett genom skriftväxling. Mot bakgrund av att det gäller gränsöverskridande behandling har IMY använt sig av de mekanismer för samarbete och enhetlighet som finns i kapitel VII i dataskyddsförordningen. Berörda tillsynsmyndigheter har varit dataskyddsmyndigheterna i Danmark, Finland, Norge och Estland.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

[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).

Uppgifter från If

If har i huvudsak uppgett följande.

Överföring av känsliga personuppgifter via e-post den 6 november 2020
If har uppgett att bolaget är personuppgiftsansvarig för den personuppgiftsbehandling som klagomålet avser. Vidare har If angett att det inom ramen för dess skadereglering i en av den klagandes anmäld personskada skickat ett e-postmeddelande till den klagande. E-postmeddelandet skickades den 6 november 2020 till den e-postadress som den klagande angett. Det innehöll If:s beslut samt en bifogad fil innehållande den medicinska bedömning som låg till grund för beslutet. Den medicinska bedömningen omfattade bakgrund, händelseförlopp, diagnos, bedömning, gradering av eventuell invaliditet samt födelsedatum (ej personnummer).

E-postmeddelandet skickades krypterat med s.k. tvingande Transport Layer Security-kryptering (Enforced TLS-kryptering). Det innebar att meddelandet överfördes krypterat från If:s servrar till mottagarens e-postserver, som i det aktuella fallet fanns hos Tele2 (operatören). För det fall att den mottagande servern inte kunde ta emot ett TLS-krypterat meddelande, skickades det inte. På detta sätt säkerställdes det att meddelandet alltid överfördes krypterat. De riktlinjer som gällde vid den aktuella tidpunkten föreskrev att när känsliga personuppgifter skickades via e-post skulle e-postmeddelandet alltid krypteras.

Lösningen med tvingande TLS-kryptering implementerades med anledning av ett avgörande[2] från Datatilsynet i Danmark där If fick kritik för att använda s.k. opportunistisk TLS vid kryptering av e-postmeddelande som innehöll känsliga personuppgifter.

If har även hänvisat till ett avgörande[3] från Datatilsynet i Danmark där dataskyddsmyndigheten konstaterade, efter en granskning hos en advokatfirma, att användandet av tvingande TLS 1.2 innebär en kryptering med tillräcklig säkerhet för e-post som innehåller konfidentiell och känslig personlig information vid överföringen. If har uppgett att det var denna krypteringslösning som också användes när e-postmeddelandet med den medicinska bedömningen skickades till den klagande den 6 november 2020.

Ny lösning för hantering av e-postmeddelanden
If har angett att bolaget, i tiden efter klagomålet, har höjt säkerheten bland annat genom att bolaget har utvecklat och lanserat en ny kommunikationslösning för e-postmeddelanden till bolagets kunder. Inom ramen för denna lösning får If:s kunder tillgång till e-postmeddelanden via ”Mina sidor” på bolagets webbplats. Lösningen fungerar på så sätt att en avisering skickas till kunden per e-post eller sms med information om att kunden har fått ett meddelande från If som kan läsas på ”Mina sidor”. För att logga in på ”Mina sidor” behöver kunden autentisera sig med BankID.

[2] Se Datatilsynets (Danmark) avgörande av den 18 juni 2020 i ärende J.nr. 2019-31-2175.
[3] Se Datatilsynets (Danmark) avgörande av den 5 november 2019 i ärende J.nr. 2019-41-0026.

Motivering av beslutet

Tillämpliga bestämmelser

Uppgifter om hälsa utgör s.k. känsliga personuppgifter. Det är förbjudet att behandla sådana särskilda kategorier av personuppgifter enligt artikel 9.1 i dataskyddsförordningen, såvida behandlingen inte omfattas av något av undantagen i artikel 9.2. Dessa uppgifter anses extra skyddsvärda eftersom behandlingen av dessa uppgifter kan innebära betydande risker för enskildas grundläggande rättigheter och friheter.

Den personuppgiftsansvarige ska vidare, enligt artikel 32.1 i dataskyddsförordningen, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå till skydd för de uppgifter som behandlas. 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 bland annat:

- Pseudonymisering och kryptering av personuppgifter.
- 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.

IMY:s bedömning

E-postmeddelande sänt till den klagande den 6 november 2020
Eftersom den som är personuppgiftsansvarig enligt artikel 32 i dataskyddsförordningen är ansvarig för säkerheten vid behandlingen, behöver den personuppgiftsansvarige bedöma de risker som är förknippade med den behandling av personuppgifter som ska ske och vidta lämpliga tekniska och organisatoriska åtgärder för att hantera de risker som identifieras. Vad som är lämpliga åtgärder ska inte uppfattas som att det är frågan om en godtycklig bedömning utan en bedömning som är adekvat utifrån behandlingens art, omfattning, sammanhang och ändamål samt riskerna för den enskildes fri- och rättigheter. I detta fall är det frågan om överföring av känsliga personuppgifter över öppet nät (internet). Att det rör sig om behandling av känsliga personuppgifter innebär att det ställs högre krav på de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige ska vidta.

När ett e-postmeddelande skickas över öppet nät har avsändaren eller mottagaren i allmänhet ingen kontroll över vilka datorer (t.ex. servrar) det specifika e-

postmeddelandet passerar längs vägen. En konsekvens av detta är att alla som förfogar över utrustning som oskyddade e-postmeddelanden passerar, kan ta del av, sprida vidare eller förvanska dem.

Genom att vidta lämpliga tekniska och organisatoriska åtgärder ska personuppgifter som överförs över ett öppet nät inte kunna läsas av obehöriga. Det kan uppnås genom att e-postmeddelandet som innehåller personuppgifter krypteras och/eller att överföringen av e-postmeddelandet skyddas genom kryptering. Tvingande TLS är ett exempel på en krypteringslösning som kan användas för att skydda ett e-postmeddelande. I det aktuella fallet skedde överföringen av e-postmeddelandet med tvingande TLS.

IMY konstaterar att den lösning som If använde för att översända e-postmeddelandet till den klagande endast krypterade e-postmeddelandet under transporten från If:s e-postserver till den e-postserver som tillhandahölls av den klagandes operatör. Det innebar att krypteringen upphörde innan meddelandet hade nått den slutliga mottagaren och utgjorde således inte någon s.k. end-to-end-kryptering. På så sätt fanns det risk för att obehöriga kunde ta del av e-postmeddelandet i klartext efter att den krypterade överföringen hade upphört.

Med anledning av ovanstående kan If inte anses ha skyddat uppgifterna på ett sådant sätt att endast den avsedda mottagaren kunnat ta del av dem efter att e-postmeddelandet hade levererats till operatörens e-postserver. Vid denna tidpunkt upphörde krypteringen och därmed saknade uppgifterna tillräckligt skydd mot obehörigt röjande av eller obehörig åtkomst till personuppgifterna. Eftersom det rörde sig om känsliga personuppgifter utgjorde det en beaktansvärd risk för integritetsintrång gentemot den klagande.

If har hänvisat till ett avgörande från det danska Datatilsynet, som rör en advokatfirma, för att visa att Datatilsynet har bedömt tvingande TLS som en tillräckligt säker lösning för att överföra känsliga personuppgifter. IMY kan konstatera att beslutet inte avser en specifik behandling utan att det var frågan om en planlagd tillsyn gällande säkerheten vid behandling av personuppgifter, särskilt vid användning av krypterade e-postmeddelanden. Advokatfirman har angett olika metoder som de använder för att säkerställa en säker kommunikation. Vilken metod som används bedöms i det enskilda fallet och en av metoderna är att kryptera överföringen av e-postmeddelande genom att använda tvingande TLS. Datatilsynet har bedömt att advokatfirmans agerande var i enlighet med dataskyddsförordningen. IMY:s granskning i detta fall skiljer sig från det åberopade avgörandet då denna granskning avser om en specifik försändelse har omfattats av tillräckligt skydd hela vägen från avsändaren till mottagaren.

Sammanfattningsvis finner IMY att If, vid det aktuella tillfället, inte hade vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig i förhållande till risken med behandlingen, eftersom If skickat e-postmeddelandet innehållande känsliga personuppgifter utan att se till att den krypteringslösning som valts skyddade meddelandet hela vägen fram till mottagaren. If behandlade därmed personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

If:s nya lösning för hantering av e-postmeddelanden
If har uppgett att bolaget, i tiden efter klagomålet, bland annat har utvecklat och lanserat en ny kommunikationslösning för e-postmeddelanden till bolagets kunder. Det noteras att den personuppgiftsbehandling som sker inom ramen för denna lösning inte är föremål för klagomålet och är därför inte del av IMY:s granskning.

Val av ingripande

Av artikel 58.2 i och artikel 83.2 i dataskyddsförordningen framgår att IMY 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. Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om en administrativ sanktionsavgift ska påföras och vid bestämmande av avgiftens storlek. 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.

IMY har konstaterat att If har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen. En överträdelse av den bestämmelsen kan föranleda en sanktionsavgift. If:s överträdelse har skett genom att bolaget den 6 november 2020 skickat ett e-postmeddelande innehållande känsliga personuppgifter till den klagande utan att använda en tillräckligt säker krypteringslösning som skyddat meddelandet hela vägen från avsändaren till den avsedda mottagaren (s.k. end-to-end-kryptering).

IMY:s tillsyn rör ett e-postmeddelande som If sänt utan användning av tillräckliga säkerhetsåtgärder – det som klagomålet avser. If har arbetat med att förbättra säkerheten dels genom att efter Datatilsynets beslut mot If ha ändrat från opportunistisk till tvingade TLS, dels att efter det att den klagande påtalat säkerhetsbrister vidtagit säkerhetsåtgärder genom att bland annat ha utvecklat och lanserat en ny kommunikationslösning för e-postmeddelanden till bolagets kunder. Sammantaget anser därför IMY att det är frågan om en mindre överträdelse varför If, med stöd av 58.2 b i dataskyddsförordningen, ges en reprimand.

Övrigt

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av it- och informationssäkerhetsspecialisten Mats Juhlén.

Vid den slutliga handläggningen av ärendet har även juristen Per Nydén medverkat.

Katarina Tullstedt, 2023-01-19 (Det här är en elektronisk signatur)

Kopia till
DPO@if.se

Hur man överklagar

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

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