Datainspektionen

Datum	Diarienr
2013-05-03	634-2012

Söderberg & Partners Insurance Consulting KB
Att: N N
Box 7785
103 96 STOCKHOLM

Tillsyn enligt personuppgiftslagen (1998:204)

Datainspektionens beslut§

Datainspektionen konstaterar att Söderberg & Partners Insurance Consulting KB (org. nr 969700-4266) inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att användare av tjänsten ”Privattjänsten” får åtkomst till integritetskänsliga personuppgifter via webbplatsen www.soderbergpartners.se efter autentisering med enbart användarnamn och lösenord.

Datainspektionen konstaterar att Söderberg & Partners Insurance Consulting KB inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att Söderberg & Partners Insurance Consulting KB:s anställda får åtkomst till integritetskänsliga personuppgifter i Söderberg & Partners Insurance Consulting KB:s Kundsystem över öppet nät efter autentisering med enbart användarnamn och lösenord.

Datainspektionen förelägger Söderberg & Partners Insurance Consulting KB enligt 45 § första stycket personuppgiftslagen

- att vidta åtgärder som innebär att åtkomst till integritetskänsliga personuppgifter via tjänsten Privattjänsten föregås av stark autentisering samt
- att vidta åtgärder som innebär att anställdas åtkomst till integritetskänsliga personuppgifter i Söderberg & Partners Insurance Consulting KB:s Kundsystem över öppet nät föregås av stark autentisering.

Ärendet avslutas, men kan komma att följas upp.

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

Redogörelse för tillsynsärendet

Datainspektionen har genomfört en inspektion hos Söderberg & Partners Insurance Consulting KB (bolaget) den 16 maj 2012. Inspektionen var en del i Datainspektionens projekt för att kartlägga och kontrollera försäkringsförmedlares behandling av kunders personuppgifter. Syftet med inspektionen var att kontrollera vilka personuppgiftsbehandlingar som bolaget utför i samband med förmedling av personförsäkringar och kontrollera IT-säkerheten.

Protokoll har upprättats och översänts till bolaget för synpunkter. Vid inspektionen framkom bl.a. följande.

Allmänt

Bolaget förmedlar tjänstepensioner och vissa försäkringar genom ett antal förmedlarbolag som är kommanditdelägare i bolaget. Försäkringsförmedlarna är anställda av förmedlarbolagen (anställda). Bolaget har idag, inklusive bolagsmännen, ca 920 anställda.

Kundsystemet

Bolaget och bolagsmännen har ett gemensamt Kundsystem som bolaget äger och ansvarar för. Uppgifter om bolagets företagskunder (kundföretag) och kundföretagens anställda (kunder) registreras i bolagets Kundsystem.

Bolaget ingår samarbetsavtal med kundföretag om att ge kunder rådgivning. I samband med det lämnar kundföretaget viss information om kunderna till bolaget. Uppgifter som samlas in på detta sätt är:

- Kontaktuppgifter
- Anställningsuppgifter
- Löneuppgifter
- Personnummer

Dessa uppgifter registreras i Kundsystemet. Bolaget anser sig i denna fas behandla uppgifterna för kundföretagets räkning i egenskap av personuppgiftsbiträde.

Vid ett personligt möte mellan bolaget och kunden samlar den enskilde rådgivaren in uppgifter om kunden som är adekvat och relevant för att ge kunden en fullständig rådgivning enligt 5 kap. 4 § lagen (2005:405) om försäkringsförmedling (förmedlarlagen). Uppgifter samlas in genom att kunden fyller i en s.k. rådgivningsenkät varpå uppgifterna registreras i Kundsystemet med kundens samtycke. Uppgifter som samlas in på detta sätt är:

- Civilstånd
- Familj
- Befintliga försäkringar
- PPM-kod
- Inkomster
- Utgifter
- Tillgångar och sparande
- Fastighet och bostadsrätt
- Skulder
- Hälsodeklaration

I och med att kunden lämnar uppgifter till bolaget och bolagets dokumentationsskyldighet enligt förmedlarlagen inträder anser bolaget att personuppgiftsansvaret för samtliga personuppgifter som registreras om kunden i Kundsystemet fortsättningsvis åvilar bolaget.

Kunden kan vid detta möte även efterfråga rådgivning utöver vad som omfattas av samarbetsavtalet med kundföretaget. Rådgivningen kan således resultera i att kunden kompletterar sitt försäkringsinnehav med sådana försäkringar som ägs i första hand av kunden själv. Bolaget kommer därmed att betrakta kunden även som ”privatkund”.

Bolagets egna anställda har, beroende på individuell behörighet, tillgång till Kundsystemet. Kundsystemet har ca 1 600 användare uppdelade på ca 400 behörighetsgrupper (inklusive mejlgrupper).

Företagstjänsten
Kundföretaget har via webbplatsen www.soderbergpartners.se och tjänsten ”Företagstjänsten” åtkomst till alla sina anställdas anställningsuppgifter, löneuppgifter, och vilken pensionsutfästelse anställda är kopplade till. När det gäller de försäkringar som företaget äger och betalar för har kundföretaget åtkomst till bl.a. försäkringsnummer, försäkringsbolag, aktuell premie och premiehistorik. Kundföretaget har inte åtkomst till några av de uppgifter som den anställde lämnar i rådgivningsenkäten. Kundföretaget har inte heller åtkomst till lika många uppgifter om de försäkringar som kundföretaget äger som den anställde har genom tjänsten ”Privattjänsten”.

Inloggningen sker med hjälp av användarnamn och lösenord.

Privattjänsten
Via webbplatsen www.soderbergpartners.se och den s.k. Privattjänsten har den enskilde kunden åtkomst till de uppgifter som denne har lämnat inom ramen för rådgivningsenkäten, t.ex. uppgift om familj, inkomster, utgifter,

tillgångar, sparande och skulder. Den hälsodeklaration som kunden eventuellt har lämnat kan dock inte kommas åt via Privattjänsten. Kunden har vidare åtkomst till sitt försäkringsinnehav, i form av villkor och belopp, samt vilken ev. förvaltning som han eller hon har valt. Kunden kan också ändra sina kontaktuppgifter via Privattjänsten.

Inloggningen sker med hjälp av användarnamn och lösenord.

Extern åtkomst till Kundsystemet via Terminal Server Gatewaylösning
Cirka 200-300 av bolagets anställda har extern åtkomst till uppgifter i Kundsystemet över öppet nät via en Terminal Server Gatewaylösning. Vilka uppgifter den enskilde anställde har åtkomst till är beroende av vilken behörighet som bolaget har gett den anställde. Åtkomsten kan gälla alla typer av uppgifter utom hälsodeklarationer.

Inloggningen sker med användarnamn och lösenord.

Skäl för beslutet

Personuppgiftsansvaret
Datainspektionen konstaterar att bolaget är personuppgiftsansvarigt för all den personuppgiftsbehandling som sker från och med det att bolaget registrerar uppgifter som kunden själv lämnar till bolaget vid det personliga mötet och bolagets dokumentationsskyldighet enligt förmedlarlagen uppstår.

IT-säkerheten
Tillämpliga bestämmelser
Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna och
- hur pass känsliga de behandlade personuppgifterna är.

För det fall personuppgifter behandlas på ett olagligt sätt ska Datainspektionen enligt 45 § första stycket personuppgiftslagen genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse.

Privattjänsten

Datainspektionen konstaterar att användare av Privattjänsten har åtkomst till integritetskänsliga personuppgifter om enskildas ekonomi, bl.a. uppgift om tillgångar, sparande och skulder samt försäkringsinnehav, över öppet nät. För inloggning till Privattjänsten krävs användarnamn och lösenord.

För att motverka intrång i de registrerades personliga integritet ska den personuppgiftsansvarige vidta lämpliga säkerhetsåtgärder för att förhindra otillbörlig spridning av uppgifter. Datainspektionen anser att integritetskänsliga personuppgifter får lämnas ut via öppet nät, till exempel Internet, endast till identifierade användare vars identitet är säkerställd med stark autentisering. Stark autentisering, också kallat multifaktors autentisering, kan realiseras på olika sätt. Det kan ske exempelvis med e-legitimation, men även andra tekniska funktioner för asymmetrisk kryptering samt vissa lösningar för engångslösenord och liknande kan användas. Det finns standardlösningar för stark autentisering på marknaden som kan förvärvas för en i sammanhanget låg kostnad.

Datainspektionen konstaterar att bolagets rutin för inloggning på Privattjänsten inte innebär att användarens identitet är säkerställd med stark autentisering eftersom bolaget enbart använder en faktor för autentisering. Detta innebär i sin tur att integritetskänsliga uppgifter om kunders ekonomiska förhållanden inte är tillräckligt skyddad mot obehörig åtkomst.

Datainspektionen finner vid en samlad bedömning att bolaget inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att användare kommer åt integritetskänsliga personuppgifter via tjänsten Privattjänsten över Internet på webbplatsen www.soderbergpartners.se efter autentisering med enbart användarnamn och lösenord.

Datainspektionen förelägger därför bolaget, enligt 45 § första stycket personuppgiftslagen, att vidta åtgärder i webbtjänsten Privattjänsten som innebär att åtkomst till integritetskänsliga personuppgifter i tjänsten Privattjänsten via webbplatsen www.soderbergpartners.se föregås av stark autentisering.

Extern åtkomst till Kundsystemet via Terminal Server Gatewaylösning

Datainspektionen konstaterar att bolagets anställda, via en Terminal Server Gatewaylösning, har åtkomst till integritetskänsliga personuppgifter om enskildas ekonomi som har registrerats i bolagets Kundsystem över öppet nät. För denna inloggning till Kundsystemet krävs användarnamn och lösenord.

Datainspektionen konstaterar att inte heller denna rutin innebär att användarens identitet är säkerställd med stark autentisering eftersom bolaget enbart

använder en faktor för autentisering. Detta innebär i sin tur att integritetskänsliga uppgifter om kunders ekonomiska förhållanden som behandlas i Kundsystemet inte är tillräckligt skyddade mot obehörig åtkomst.

Datainspektionen finner vid en samlad bedömning att bolaget inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att användare kommer åt integritetskänsliga personuppgifter i Kundsystemet över öppet nät via en Terminal Server Gatewaylösning efter autentisering med enbart användarnamn och lösenord.

Datainspektionen förelägger därför bolaget, enligt 45 § första stycket personuppgiftslagen, att vidta åtgärder som innebär att åtkomst till integritetskänsliga personuppgifter i bolagets Kundsystem över öppet nät via en Terminal Server Gatewaylösning föregås av stark autentisering.

Företagstjänsten

Datainspektionen konstaterar att kundföretaget har åtkomst till viss ekonomisk information på webbplatsen www.soderbergpartners.se via tjänsten Företagstjänsten. Den ekonomiska information som användaren får åtkomst till via tjänsten Företagstjänst är dock betydligt mindre omfattande och integritetskänslig än den information som användaren får åtkomst till via tjänsten Privattjänsten respektive Terminal Server Gatewaylösningen. Datainspektionen anser därför att autentisering genom användarnamn och lösenord vid inloggning till webbplatsen www.soderbergpartners.se via tjänsten Företagstjänsten utgör en sådan lämplig säkerhetsnivå som sägs i 31 § personuppgiftslagen.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick ta del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av tf. generaldirektören Hans-Olof Lindblom i närvaro av tillsynschefen Catharina Fernquist, juristen Malin Fredholm, IT-säkerhetsspecialisten Adolf Slama samt avdelningsdirektören Hans Kärnlöf, föredragande.

Hans-Olof Lindblom

Hans Kärnlöf