Datainspektionen

Datum	Diarienr
2013-05-03	653-2012

Max Matthiessen AB
Att: N N
Box 5908
114 89 STOCKHOLM

Tillsyn enligt personuppgiftslagen (1998:204)

Datainspektionens beslut

Datainspektionen konstaterar att Max Matthiessen AB (org. nr 556421-0911) inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom

- att användare av tjänsten ”Privattjänsten” får åtkomst till integritetskänsliga personuppgifter via webbplatsen www.maxm.se efter autentisering med enbart användarnamn och lösenord samt
- att Max Matthiessen AB:s anställda får åtkomst till integritetskänsliga personuppgifter över öppet nät efter autentisering med enbart användarnamn och lösenord.

Datainspektionen förutsätter att Max Matthiessen AB fortsätter det påbörjade arbetet med att införa stark autentisering vid inloggning till Max Matthiessen AB:s affärssystem över öppet nät.

Ärendet avslutas, men kan komma att följas upp.

Redogörelse för tillsynsärendet

Datainspektionen har genomfört en inspektion hos Max Matthiessen AB (bolaget) den 15 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 bedriver försäkringsförmedling. 90 % av bolagets uppdragsgivare är företag. Bolaget har 420 anställda och 12 000 kundföretag och 150 000 aktiva individkunder.

PML

Bolaget har ett affärssystem för försäkringsförmedling som heter Pro Max Liv (PML).

Kundföretag tillhandahåller bolaget grunduppgifter om kundföretagets anställda. Uppgifterna läggs in i PML. Bolaget bokar sedan in ett möte med den anställde. Vid mötet lämnar den anställde uppgifter till bolaget och blir därmed individkund (kund) hos bolaget.

Bolaget samlar sedan med stöd av fullmakt från arbetsgivare och kunden in ytterligare uppgifter om kunden från bl.a. arbetsgivare, försäkringsgivare, försäkringsadministratörer, fondförvaltare, banker och myndigheter såsom Försäkringskassan och Premiepensionsmyndigheten för att få en komplett bild av kundens pensioner och finansiella sparande.

Uppgifter som samlas in om kunden är:

- ID i databasen
- Ändringsdatum
- Förnamn
- Efternamn
- Personnummer
- Adress
- Postnummer
- Ort
- Telefonnummer
- Civilstånd
- Företag
- Make/maka
- Barn
- Mobilnummer
- Faxnummer
- Typ av kund
- Kapital likvida medel
- Kapital aktier
- Kapital fonder
- Kapital övrigt
- Boendelån
- Övriga lån
- Värde av fastighet
- Värde av fritidsboende
- Värde av borätt
- Taxeringsvärde villa
- Taxeringsvärde fritidsboende
- Hyra
- Räntor
- Driftskostnader
- Partners Inkomst
- Partners Kapital
- Förmånsplan
- Gruppförsäkring
- Olyckfallsförsäkring
- Gruppsjukförsäkring
- Pension
- Premieplan
- Förmånsplan
- Pensionssystem
- Barn
- ITPK belopp

- Sjukvårdsförsäkring
- Försäkringsbrev
- Firmatecknare
- Senaste sjukpremie
- Pensionsplan
- ATP poäng
- Datum för ändring av civilstånd
- E-mail
- Skötselfullmakt
- Försäkringsbesked
- Privata försäkringar
- Fullmaktsdokument
- Äktenskapsförord
- Avdelning
- Kostnadsställe
- Kundstatus
- Landskod
- Grad av arbetsförmåga
- Hälsodeklaration

Bolaget skannar in alla handlingar, med undantag för hälsodeklarationer. Bolaget lagrar inte individkunders hälsodeklarationer på något sätt, utan vidarebefordrar den som en pappershandling till försäkringsbolaget i fråga.

Autentisering

Bolagets kunder kan logga in i PML via den s.k. ”Privattjänsten” på bolagets webbplats www.maxm.se. Kunden får då åtkomst till uppgifter om sitt försäkringsskydd, sitt sparande, sina pensions- och försäkringspremier samt sitt totala innehav i fonder, aktier och andra tillgångar. Inloggningen sker för närvarande med hjälp av användarnamn och lösenord.

Förutom loggning via bolagets intranät kan bolagets anställda logga in i PML via en VPN-tunnel knuten till bolagets inloggningsserver. Den enskilde anställde har åtkomst till uppgifter i PML beroende av vilken behörighet som bolaget har gett den anställde. Inloggningen sker för närvarande med hjälp av användarnamn och lösenord.

Bolaget har på senare tid inlett arbetet med att införa stark autentisering vid inloggning via såväl webbplatsen som via VPN-tunneln. Inloggning ska ske med engångslösenord och/eller E-legitimation (BankID). Bolaget har köpt en programvara som ska installeras under april 2013. Testning och implementeringsprojektet kommer att påbörjas innan sommaren 2013. De nya inloggningsrutinerna kommer att börja tillämpas av kunder och anställda någon gång under hösten 2013.

Skäl för beslutet

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 i form av försäkringsskydd, sparande, pensions- och försäkringspremier samt totalt innehav i fonder, aktier och andra tillgångar 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.maxm.se efter autentisering med enbart användarnamn och lösenord.

Extern åtkomst till PML över en VPN-koppling

Datainspektionen konstaterar att bolagets anställda, via en VPN-tunnel, har åtkomst till integritetskänsliga personuppgifter om enskildas ekonomi som

har registrerats i bolagets PML över öppet nät. För denna inloggning till PML 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 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 anställda kommer åt integritetskänsliga personuppgifter i PML över öppet nät via en VPN-tunnel efter autentisering med enbart användarnamn och lösenord.

Nya inloggningsrutiner

Datainspektionen konstaterar att bolaget har inlett arbetet med att införa nya rutiner för inloggning till PML via både webbplatsen och VPN-tunneln. Autentiseringen ska ske med engångslösenord och/eller E-legitimation (BankID). De nya inloggningsrutinerna kommer att börja tillämpas av kunder och anställda under hösten 2013.

Datainspektionen konstaterar att bolagets nya rutin för inloggning till PML via Privattjänsten och VPN-tunneln innebär att användarens identitet är säkerställd med stark autentisering eftersom rutinen innebär att användaren identifieras med två faktorer. När förändringen är genomförd kan bolaget anses leva upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen.

Slutsats

Datainspektionen förutsätter att bolaget inför den nya inloggningsrutinen i enlighet med vad som ovan beskrivits. Ärendet kan därmed avslutas, men kan komma att följas upp.

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