Datainspektionen

Datum	Diarienr
2013-05-03	654-2012

Cerberus AB
Att: N N
Engelbrektsgatan 7
114 32 STOCKHOLM

Tillsyn enligt personuppgiftslagen (1998:204)

Datainspektionens beslut

Gallring
Datainspektionen konstaterar att Cerberus AB (org. nr 556677-0391) inte lever upp till kraven på gallring i 9 § punkt i) personuppgiftslagen genom att inte gallra uppgifter som behandlas för direktreklamändamål.

Datainspektionen förelägger Cerberus AB enligt 45 § första stycket personuppgiftslagen att gallra uppgifter som behandlas för direktreklamändamål senast tre månader från det datum då uppgifterna samlades in.

IT-säkerhet
Datainspektionen konstaterar att Cerberus AB inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att användare av tjänsten ”Closetalk” får åtkomst till integritetskänsliga personuppgifter i Closetalk på webbplatsen www.cerberusradgivning.se efter autentisering med enbart användarnamn och lösenord.

Datainspektionen konstaterar att Cerberus AB inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att anställda får åtkomst till integritetskänsliga personuppgifter i ”Foldersystemet” över öppet nät efter autentisering med enbart användarnamn och lösenord.

Datainspektionen konstaterar att Cerberus AB inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att i systemen Closetalk och Foldersystemet inte ha en behandlingshistorik som löpande registrerar användaridentitet, tidpunkt och vilka personuppgifter användaren har haft åtkomst till och vilka åtgärder som vidtagits med personuppgifterna.

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

Datainspektionen förelägger Cerberus AB enligt 45 § första stycket personuppgiftslagen

- att vidta åtgärder som innebär att åtkomst till integritetskänsliga personuppgifter via Cerberus AB:s webbplats föregås av stark autentisering samt
- att vidta åtgärder som innebär att anställdas åtkomst till integritetskänsliga personuppgifter i Cerberus AB:s system Foldersystemet över öppet nät föregås av stark autentisering.
- att säkerställa spårbarhet av åtkomst genom att i systemen Closetalk och Foldersystemet införa en behandlingshistorik som löpande registrerar användaridentitet, tidpunkt och vilka personuppgifter användaren har haft åtkomst till och vilka åtgärder som vidtagits med personuppgifterna.

Ärendet avslutas, men kan komma att följas upp.

Redogörelse för tillsynsärendet

Datainspektionen har genomfört en inspektion hos Cerberus AB (bolaget) den 2 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. Bolaget hjälper såväl privatpersoner som företag med rådgivning kring försäkringar och förmedling av försäkringar. Bolaget har mer än 100 anställda, varav ca 40 är försäkringsförmedlare/-rådgivare.

IT-miljö

Bolaget använder fyra system där personuppgifter behandlas, Closetalk, Foldersystemet, ”Filemaker” och ”Dexter”.

De anställda arbetar i en webbapplikation kallad ”Fjärrskrivbord” mot systemen Foldersystemet, Filemaker och Dexter. All data lagras i systemen via Fjärrskrivbordet.

Terminalservrarna loggar vilka användarkonton som loggar in och ut ur i systemen Closetalk och Foldersystemet. Dessa loggar sparas i dag ca fyra veckor. Loggarna är terminalservrarnas säkerhetsloggar och visar bara in- och utloggning.

Closetalk

Bolaget samlar med stöd av kundens fullmakt in uppgifter om kundens nuvarande försäkringsengagemang hos de aktuella försäkringsbolagen. Det kan handla om kapital-, pensions-, sjuk-, och olycksfallsförsäkringar och kollektivt avtalade försäkringar, vald försäkringsgivare avseende ITP-K eller därmed jämställd försäkring samt individuellt pensionssparande (IPS). Uppgifter som samlas in är:

- Namnuppgifter
- Kontaktuppgifter
- Försäkringsnummer
- Försäkringsbolag
- Försäkringens värde
- Uppgifter om fonder inklusive uppgift om hur mycket som har betalats in.

Kunder och anställda hos bolaget kan logga in i Closetalk via webbplatsen www.cerberusradgivning.se. Kunden får därmed åtkomst till alla uppgifter om sig själv som registrerats i Closetalk. Den enskilde anställde har åtkomst till uppgifter i Closetalk beroende av vilken behörighet som bolaget har gett den anställde.

Inloggningen sker med hjälp av användarnamn och lösenord.

Foldersystemet

I Foldersystemet sparas uppgifter om kunder i mappar i Windows. Mapparna namnges med kundens personnummer och namn. Alla handlingar som upprättas av eller om kunden skannas in och sparas i kundens mapp i form av pdf-filer. Handlingar som sparas är t.ex

- Identitetshandling
- Fullmakt
- Försäkringsansökan
- Hälsodeklaration

Bolagets anställda har extern åtkomst till uppgifter i bl.a. Foldersystemet via en Terminal Server Gatewaylösning. Vilka uppgifter den enskilde anställde har åtkomst till är beroende av vilken behörighet som bolaget har gett den an-

ställde. Åtkomsten kan gälla alla typer av uppgifter inklusive hälsodeklarationer.

Inloggningen sker med hjälp av användarnamn och lösenord.

FileMaker
FileMaker är ett Customer Relationship management system (CRM-system) som innehåller uppgifter om potentiella kunder. Bolaget hämtar uppgifter om personer i en viss ålder och med inkomst över ett visst belopp från PAR AB. Uppgifter som inhämtas på detta sätt är:

- Förnamn
- Tilltalsnamn
- Efternamn
- Adress
- Telefonnummer

Bolaget hämtar även in uppgifter från den registrerade själv. Uppgifter som inhämtas på detta sätt är t.ex.:

- Uppgift om att den registrerade aldrig mer vill bli uppringd
- Uppgift om att den registrerade vill bli uppring vid ett visst senare tillfälle
- Uppgift om att den registrerade vill få ett informationsbrev hemskickat
- Uppgift om att den registrerade inte är intresserad av bolagets tjänster just nu

Bolaget gallrar inte uppgifterna i Filemaker eftersom uppgifterna behövs för att bolaget ska kunna bedriva verksamheten på ett effektivt och ändamålsenligt sätt.

Skäl för beslutet

Gallring
Datainspektionen bedömer att bolagets behandling av personuppgifter i FileMaker ingår i en strukturerad samling av personuppgifter. Det innebär att personuppgiftslagens hanteringsregler ska tillämpas på behandlingen.

Personuppgifter får enligt 9 § punkt i) personuppgiftslagen inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Personuppgifter måste enligt 9 § punkt g) personuppgiftslagen, om det är nödvändigt, vara aktuella.

Bolaget gallrar inte uppgifter i systemet Filemaker.

Datainspektionen konstaterar att ändamålet med behandling av personuppgifter i systemet Filemaker är marknadsföring mot personer som bolaget inte har någon kundrelation till.

Datainspektionen anser att uppgifter i ett sådant direktreklamregister är nödvändiga för sitt ändamål fram till dess att de använts för den avsedda direktreklamkampanjen.

Datainspektionen anser vidare att det är nödvändigt att uppgifter i ett direktreklamregister är aktuella för att integritetskränkande marknadsföringsåtgärder ska kunna undvikas. Med hänsyn till att adressuppgifter ofta ändras kan uppgifter i ett direktreklamregister anses aktuella endast under en kortare tid. Datainspektionens anser att uppgifter i ett direktreklamregister inte ska bevaras under längre tid än tre månader från det datum då uppgifterna samlades in.

Datainspektionen anser att bolaget inte lever upp till kraven på gallring i 9 § punkt i) personuppgiftslagen genom att inte gallra uppgifter som behandlas för direktreklamändamål.

Datainspektionen förelägger därför bolaget, enligt 45 § första stycket personuppgiftslagen, att gallra uppgifter som behandlas för direktreklamändamål senast tre månader från det datum då de samlades in.

Övrigt
Det bör framhållas att för det fall en direktreklamkampanj leder till att det uppstår ett kundförhållande mellan bolaget och den registrerade får uppgifter om kunden bevaras för kundadministrativt ändamål så länge kundförhållandet varar och användas för marknadsföringsändamål under högst ett års tid efter det att kundförhållandet har upphört.

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.

Åtkomst till Closetalk

Datainspektionen konstaterar att användare av tjänsten Closetalk har åtkomst till integritetskänsliga personuppgifter om enskildas ekonomi över öppet nät. Användaren har bl.a. åtkomst till sammanställning av försäkringar med sparmoment, ppm, fonder, värdepapper och övriga tillgångar. Det går således att kontinuerligt följa utvecklingen på den enskildes finansiella innehav. För inloggning till Closetalk 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 till Closetalk 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 Closetalk över Internet på webbplatsen www.cerberusradgivning.se 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 via bolagets webbplats föregås av stark autentisering.

Åtkomst till Foldersystemet

Datainspektionen konstaterar att bolagets anställda, via en Terminal Server Gatewaylösning, har åtkomst till integritetskänsliga personuppgifter om enskildas hälsa och ekonomi som har registrerats i bolagets system Foldersystemet över öppet nät. För denna inloggning till Foldersystemet 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 hälsa och ekonomiska förhållanden som behandlas i Foldersystemet 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 Foldersystemet 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 Foldersystem över öppet nät föregås av stark autentisering.

Spårbarhet av åtkomst

Datainspektionen konstaterar att systemen Closetalk och Foldersystemet innehåller känsliga personuppgifter. Bolaget loggar endast in- och utloggning till systemen Closetalk och Foldersystemet.

Datainspektionen anser att när känsliga personuppgifter behandlas ska det finnas en behandlingshistorik, t.ex. i form av en logg, som löpande registrerar användaridentitet, tidpunkt och vilka personuppgifter användaren har haft åtkomst till och vilka åtgärder som vidtagits med personuppgifterna. Det ska vara möjligt att utreda felaktig eller obehörig användning av personuppgifter. Bolaget har ingen sådan detaljerad behandlingshistorik för åtkomst till känsliga personuppgifter. Datainspektionen förelägger därför bolaget att säkerställa spårbarhet av åtkomst genom att införa behandlingshistorik, t.ex. loggar, över åtkomst till systemen Closetalk och Foldersystemet.

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