



Intern åtkomst till känsliga personuppgifter hos försäkringsbolag


Datainspektionens rapport 2010:2

Intern åtkomst till känsliga personuppgifter hos försäkringsbolag

Datainspektionens rapport 2010:2.

Pris 53 kr, inklusive moms.

Tryckt hos Intellecta infolog i Solna, oktober 2010 på Arctic Volume White papper

 Miljömärkt trycksak 341077.

Innehåll

Inledning	4
Tillämplig lagstiftning	4
Tekniska begränsningar av behörigheter	4
Rutiner för tilldelning, ändring, borttagning och uppföljning av behörigheter	5
Åtkomst till historiskt material	5
Åtkomst till skyddade personuppgifter	6
Behandlingshistorik (loggar) och åtkomstkontroll (logguppföljning) ..	6
Information och utbildning	7
Mer information	7

Inledning

Försäkringsbolag behandlar en mängd olika personuppgifter i sin verksamhet. Många av uppgifterna är känsliga, till exempel uppgifter om hälsa eller medlemskap i fackförening. Det är därför viktigt att försäkringsbolagen har en fullgod IT-säkerhet och att åtkomsten till uppgifterna är begränsad till de personer som behöver uppgifterna för att utföra sina arbetsuppgifter.

Det är bakgrunden till att Datainspektionen under året har genomfört ett projekt om intern åtkomst¹ till känsliga personuppgifter hos försäkringsbolag. Vi har granskat ett antal försäkringsbolags rutiner för behörighetsstyrning och åtkomstkontroll vid behandling av känsliga personuppgifter. I projektet ingick också att granska hanteringen av så kallade skyddade personuppgifter. I den här rapporten redovisar vi våra slutsatser.

Tillämplig lagstiftning

I personuppgiftslagen (1998:204) finns bestämmelser om hur personuppgifter får behandlas. I den mån det inte finns avvikande bestämmelser i annan lag eller förordning är ett försäkringsbolag skyldigt att följa bestämmelserna i denna lag.

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.

Tekniska begränsningar av behörigheter

Försäkringsbolags IT-system innehåller stora mängder personrelaterad information. En grundläggande princip är att anställda inom bolaget endast bör ha tillgång till personuppgifter som de behöver för sitt arbete. Behovet av åtkomst varierar naturligtvis beroende på bolagets verksam-

¹ Med intern åtkomst menar vi den tillgång en anställd på ett försäkringsbolag har till bolagets ärendehanteringssystem och/eller andra register som innehåller personuppgifter om enskilda försäkringstagare, skadelidande, med flera.

hetsområde och den anställdes arbetsuppgifter. För att begränsa den elektroniska tillgången ska bolaget ha ett system för behörighetsstyrning. Med hjälp av detta ska åtkomstmöjligheterna tekniskt begränsas så mycket som det är faktiskt och praktiskt möjligt med hänsyn till den aktuella verksamheten och känsligheten hos personuppgifterna.

Rutiner för tilldelning, ändring, borttagning och uppföljning av behörigheter

Som Datainspektionen anger i sina allmänna råd om säkerhet för personuppgifter bör det finnas rutiner för tilldelning och kontroll av behörigheter.

Hos försäkringsbolag, som behandlar känsliga personuppgifter, kräver Datainspektionen att det finns rutiner för tilldelning, ändring och borttagning av behörigheter. Vidare krävs rutiner för systematiska och återkommande uppföljningar av tilldelade behörigheter och att uppföljningar faktiskt sker.

Åtkomst till historiskt material

Ett av de grundläggande kraven i personuppgiftslagen är att den personuppgiftsansvarige ska se till att personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs ska de gallras. Det finns två olika sätt att gallra personuppgifter. Man kan antingen avidentifiera eller förstöra dem. Att avidentifiera personuppgifterna innebär att man avlägsnar alla identifieringsmöjligheter så att de inte längre går att koppla samman med en fysisk person. Att förstöra personuppgifterna innebär att se till att de inte går att återskapa.

Försäkringsbolag menar att det av olika skäl finns anledning att bevara personuppgifter, däribland känsliga uppgifter, som avser icke beviljade försäkringar och avslutade försäkringar.²

Personuppgifter som avser icke beviljade försäkringar eller avslutade försäkringar ska avskiljas från personuppgifter som behövs för att hantera beviljade och alltjämt pågående försäkringar. Avskiljande betyder att personuppgifterna lagras på ett sådant sätt att de inte längre hålls tillgängliga i den dagliga hanteringen och är, i personuppgiftslagens mening, en säkerhetsåtgärd.

Försäkringsbolag är alltså skyldiga att ha rutiner för att avskilja eller gallra personuppgifter som avser icke beviljade och avslutade

² Se Datainspektionens rapport 2006:2 Så bör försäkringsbolag behandla känsliga personuppgifter.

försäkringar. Rutinerna bör bland annat innehålla tidsfrister för när uppgifterna ska avskiljas eller gallras.

Åtkomst till skyddade personuppgifter

Hos försäkringsbolag, som hanterar uppgifter avseende personer med skyddade personuppgifter i sina IT-system, är det viktigt att det finns spärrmarkeringar som syns tydligt vid sökning i registren. Vidare är det viktigt att all personal som hanterar dessa personuppgifter ges grundlig information och att kretsen av personer som har tillgång till uppgifterna begränsas så mycket som möjligt.

Vid inspektionerna hos försäkringsbolagen visade det sig att det ofta gick att få fram en lista över de personer som har skyddade personuppgifter genom sökning via till exempel namnfältet eller försäkringsbolagets adress. En sådan möjlighet att sammanställa dessa uppgifter för var och en av de anställda som har tillgång till systemen är inte förenlig med personuppgiftslagens krav. Det gäller oavsett om de skyddade personuppgifterna går att läsa i systemet eller inte. Redan själva sökmöjligheten innebär en säkerhetsrisk.

Behandlingshistorik (loggar) och åtkomstkontroll (logguppföljning)

Av Datainspektionens allmänna råd om säkerhet för personuppgifter framgår det att det, beroende på känsligheten hos personuppgifterna, bör finnas en behandlingshistorik som sparas en viss tid. Detta för att åtkomsten ska kunna kontrolleras. En behandlingshistorik bör följas upp och skyddas mot otillåtna ändringar.

En behandlingshistorik bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Behandlingshistoriken bör, beroende på känsligheten hos personuppgifterna, ange till exempel läsning, ändring, utplåning eller kopiering av personuppgifter.

I försäkringsbolags IT-system, i vilka det behandlas känsliga personuppgifter och uppgifter om personer med skyddade personuppgifter, ska det finnas en behandlingshistorik. Behandlingshistoriken ska kunna användas till att utreda vem som har läst, kopierat eller ändrat informationen. Det är också viktigt att försäkringsbolagen regelbundet och systematiskt följer upp vem som har haft åtkomst till vilka uppgifter.

Information och utbildning

Hos ett försäkringsbolag, som behandlar känsliga personuppgifter, måste det finnas instruktioner som anger under vilka förutsättningar bolagets anställda får ta del av personuppgifter.

I Försäkringsförbundets rekommendation om behandling av personuppgifter om hälsa inom försäkringsbranschen, antagen den 7 oktober 2009, anges bland annat att en försäkringsgivare ska ha utarbetade interna regler för behandling av personuppgifter om hälsa och att dessa regler ska fastställas genom beslut av styrelsen, VD eller företagsledningen.

Mot denna bakgrund bedömer Datainspektionen att instruktioner som anger under vilka förutsättningar bolagets anställda får ta del av personuppgifter ska vara skriftliga. Instruktionerna bör finnas allmänt tillgängliga för anställda, till exempel på ett intranät.

Försäkringsbolag bör också se till att alla som har tillgång till personuppgifter får relevant utbildning. Genom att ge anställda en klar uppfattning om vad som är tillåtet, vilka konsekvenserna blir om man bryter mot instruktionerna och andra bestämmelser samt hur efterlevnaden av instruktionerna följs upp minskas risken för otillåten åtkomst.

Mer information

Mer information hittar du i Datainspektionens allmänna råd Säkerhet för personuppgifter samt Datainspektionens rapport 2006:2 Så bör försäkringsbolag behandla känsliga personuppgifter.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

