



# Så bör försäkringsbolag behandla känsliga personuppgifter

## Bakgrund och syfte

Under oktober 2006 genomförde Datainspektionen 18 fältinspektioner hos försäkringsbolag i Sverige. Inspektionerna var en del av ett tillsynsprojekt med titeln "Personuppgiftsbehandling hos försäkringsbolag" för att kontrollera **hur försäkringsbolagen behandlar känsliga personuppgifter för att administrera försäkringar som kräver en hälsoprövning av den försäkrade**. Inspektionerna var en fördjupning och en utvidgning av en samordnad tillsynsinsats som samtliga dataskyddsmyndigheter inom EU genomfört under året. Den tillsynen utfördes genom en enkätinspektion hos försäkringsbolag som tillhandahåller privata sjukvårdförsäkringar. I Sverige granskades åtta försäkringsbolag. Datainspektionen lämnade en nationell rapport och för närvarande sammanställs resultaten gemensamt. EU-rapporten förväntas komma i början av år 2007.

Allmänt kan sägas att de 18 granskade bolagen upprätthöll ett gott integritetsskydd och att alla strävade efter att följa gällande regler. Genomgående fanns dock brister i några hänseenden. Bristerna avsåg information, gallring/avskiljande och loggning. I denna rapport redogörs närmare för bristerna och för personuppgiftslagens regler.

Datainspektionens förhoppning är att denna korta rapport kan komma till nytta hos de försäkringsbolag som inte ingick i tillsynsprojektet genom att de ges möjlighet att rätta eventuella brister i den egna hanteringen. Det bör framhållas att samtliga inspekterade bolag redan har rättat till alternativt förklarat att de inom det närmaste året kommer att rätta till konstaterade brister. Eftersom de inspekterade bolagen kommer att följa Datainspektionens påpekanden avslutades inspektionerna. Ytterligare information om personuppgiftslagen och Datainspektionen finns på [www.datainspektionen.se](http://www.datainspektionen.se).



## Bristerna

### Information till den registrerade

Enligt personuppgiftslagen ska information alltid lämnas om personuppgifterna samlas in direkt från de registrerade. Som regel ska information alltid ges om uppgifterna samlas in från någon annan källa än den registrerade. Om den registrerades samtycke är en förutsättning för behandlingen av personuppgifter måste samtycket alltid föregås av information.

De brister som kom fram vid inspektionerna gällde innehållet i den skriftliga information som bolagen lämnade. I några fall framgick inte vem som var personuppgiftsansvarig. Vidare saknades uppgift om rätten till rättelse av felaktiga eller missvisande uppgifter, rätten till information samt rätten att slippa direktreklam.

Datainspektionen begärde att de inspekterade bolagen skulle kontrollera och åtgärda om något av det följande saknades i bolagets information till den registrerade i samband med ansökan om tecknande av försäkring och skadereglering:

1. Den personuppgiftsansvariges identitet (namn, adress, telefonnummer och i förekommande fall organisationsnummer och e-post adress),
2. Ändamålen med behandlingen av personuppgifter samt
3. All övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen, såsom
  - vilka kategorier av uppgifter som ska behandlas,
  - information om mottagare, eller kategorier av mottagare, av uppgifterna,
  - skyldighet att lämna uppgifter,
  - rätten att gratis en gång årligen efter ansökan erhålla information,
  - rätten att efter anmälan till den personuppgiftsansvarige slippa direktreklam och
  - rätten att få rättelse av felaktiga eller missvisande uppgifter.

Av informationen ska också framgå att personuppgifter kan komma att behandlas under viss tid även om försäkring inte beviljas och sedan försäkring avslutas.

## Gallring/avskiljande

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. Ett annat grundläggande krav är att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen för behandlingen.

Flera av de inspekterade bolagen behöll personuppgifter som avsåg icke beviljade samt avslutade försäkringar efter det att ärendena hos bolagen hade avslutats. Som skäl för att spara uppgifter om avslutade försäkringar åberopades bland annat 12 kap. 4 § försäkringsavtalslagen (2005:104). Uppgifterna fanns således kvar i samma register som uppgifter som avsåg pågående ärenden (gällande försäkringar).

Datainspektionen begärde att bolagen skulle ta fram rutiner för att avskilja eller förstöra personuppgifter enligt följande:

- Personuppgifter som avser icke beviljade alternativt avslutade försäkringar ska avskiljas från personuppgifter som behövs för ändamålet 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. Ett alternativ är att uppgifterna förstörs.

- Rutiner för att avskilja uppgifterna eller för att förstöra uppgifterna ska tas fram. Rutinerna bör omfatta till exempel den överskottsinformation som ibland finns i patientjournaler samt tidsfrister.
- När det gäller icke beviljade försäkringar bör tidsfristen vara relativt kort, förslagsvis längst sex månader, jfr 7 kap. 6 § försäkringsavtalslagen.
- Beträffande avslutade försäkringar hänvisas till Datainspektionens skrift nr 10 *"Hur länge får personuppgifter bevaras?"* s. 13.

## Behandlingshistorik (logg)

För att kunna kontrollera vilka personer som har haft tillgång till personuppgifterna bör det finnas en behandlingshistorik (logg) som sparas en viss tid. Hur loggen ska utformas beror på hur känsliga personuppgifterna är. En logg ska följas upp och skyddas mot otillåtna ändringar. Normalt ska den vara så detaljerad att den kan användas för att utreda om personuppgifter har använts felaktigt eller obehörigt. Om personuppgifterna är känsliga ska loggen visa

användaridentitet, tidpunkt och vilka personuppgifter användaren haft tillgång till – även om han eller hon bara har läst informationen. Loggen ger också ett förebyggande skydd. En förutsättning är då att användarna informeras om att all användning loggas och att loggen följs upp.

Några av de inspekterade bolagen sparade loggen på obestämd tid.

Datainspektionen begärde följande:

En genomgång ska göras så att personuppgiftslagens krav iakttas vad gäller loggning. Därvid ska övervägas under hur lång tid som loggen verkligen behövs för den dagliga verksamheten.

- Om logguppgifterna inte längre behövs men ändå inte anses kunna förstöras ska de avskiljas. Med avskiljas menas att uppgifterna inte längre ingår i den uppgiftssamling som är allmänt tillgänglig för hantering av aktuella försäkringar.
- En avvägning ska göras om hur lång tid som en avställd logg ska sparas. Den personuppgiftsansvarige måste själv göra den avvägningen med hänsyn till känsligheten hos uppgifterna.

## Kontakta Datainspektionen

Postadress: Datainspektionen, Box 8114, 104 20 Stockholm

E-post: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

Webbplats: [www.datainspektionen.se](http://www.datainspektionen.se)

Tfn: 08-657 61 00, Fax: 08-652 86 52



Datainspektionen