Rekommendation om behandling av personuppgifter inom försäkringsföretagens utredningsverksamhet

Denna rekommendation har utarbetats gemensamt av Svensk Försäkring och Trafikförsäkringsföreningen (TFF) och beslutats av båda organisationernas styrelser.

1. Syfte och omfattning

I försäkringsverksamhet behandlas personuppgifter i samband med utredning av oklara försäkringsfall. Vid sådana utredningar förekommer det att även uppgifter om lagöverträdelser som innefattar brott och domar i brottmål behandlas. Uppgifter av detta slag är alltid att betrakta som integritetskänsliga.

Denna rekommendation lägger fast allmänna principer för försäkringsföretags behandling av personuppgifter vid utredning av oklara försäkringsfall. I dokumentet beskrivs kortfattat vissa grundläggande bestämmelser i dataskyddsförordningen och kompletterande rekommendationer lämnas beträffande tillämpningen av bestämmelserna. Dessa avsnitt markeras i texten med ramar. Rekommendationen är avsedd att komplettera de generella riktlinjer för försäkringsföretagens utredningsverksamhet som har fastställts av Svensk Försäkrings styrelse. [1]

Denna rekommendation är ett uttryck för vad som utgör god sed inom försäkringsbranschen vid behandling av personuppgifter i samband med utredning av oklara försäkringsfall.

Rekommendationens syfte är

- att fastställa höga krav på integritetsskydd vid försäkringsföretags behandling av personuppgifter i samband med utredning av oklara försäkringsfall
- att öka tydligheten beträffande förutsättningarna för försäkringsföretags behandling av personuppgifter vid sådana utredningar

Rekommendationen omfattar behandling av personuppgifter i samband med utredning av oklara försäkringsfall som utförs av försäkringsföretag/återförsäkringsgivare som är medlem i Svensk Försäkring och/eller TFF samt av Larmtjänst AB. Nedan används ”försäkringsföretag” som samlingsbegrepp för alla dessa. Rekommendationen gäller endast sådan behandling

[1] Se även Svensk Försäkrings rekommendationer om behandling av personuppgifter om hälsa inom försäkringsbranschen.

som omfattas av dataskyddsförordningen. Alla hänvisningar i texten avser dataskyddsförordningen om inte något annat anges.

2. Rättsliga förutsättningar

2.1 Generella förutsättningar

En av de grundläggande principerna för behandling av personuppgifter i dataskyddsförordningen är enligt artikel 5 att personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt. En behandling är laglig i den mån den är nödvändig för att uppfylla vissa angivna intressen i artikel 6, en s.k. legal grund. Vid utredning av oklara försäkringsfall kan följande legala grunder vara relevanta.

- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås (punkten b).
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (punkten c).
- Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts intressen, om inte den registrerades intressen eller grundläggande rättigheter eller friheter väger tyngre och kräver skydd av personuppgifter (punkten f).

Beträffande punkten b (fullgörande av avtal) så kan denna endast tillämpas vid utredning av skador där försäkringstagaren själv (d v s avtalsparten) begär ersättning. Försäkringsföretaget måste i dessa fall förvissa sig om att förutsättningarna för rätt till ersättning enligt försäkringsavtalet är uppfyllda. Denna grund är däremot inte tillämplig då ersättningsanspråket framställs av någon annan än försäkringstagaren, till exempel en förmånstagare eller en skadad tredje man vid trafikolycka.

Punkten c (rättslig förpliktelse) kan vara tillämplig för utredning. En förutsättning är dock att det finns en lagstadgad skyldighet för försäkringsföretaget att behandla uppgifterna. Försäkringsföretag är enligt försäkringsavtalslagen skyldiga att reglera en skada och måste således behandla personuppgifter som krävs för att utreda och ersätta skadan. Försäkringsföretag har även skyldighet att utreda misstänkt penningtvätt enligt lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

Enligt punkten f (intresseavvägning) ska den personuppgiftsansvariges eller en tredje parts berättigade intressen vägas mot den registrerades intressen eller grundläggande rättigheter och friheter. Försäkringsföretagen har ett berättigat intresse att utreda oklara försäkringsfall avseende den enskilda kunden (försäkringstagaren) men även när ersättningsanspråket framställs av någon annan än försäkringstagaren, till exempel en förmånstagare, en medförsäkrad eller en skadad tredje man vid trafikolycka. Utredningen utgör ett led i den skadereglering som genomförs för att fastställa, försvara och göra gällande rättsliga anspråk. Enligt skälen till dataskyddsförordningen utgör behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier ett berättigat intresse.[2] Beträffande försäkringsrörelse så utgör förhindrande av bedrägerier också ett tungt vägande intresse för kollektivet av försäkringstagare, dvs. tredje man, som inte skall belastas (via sina premier) av kostnader för oberättigade försäkringsanspråk. Det ligger självfallet också i andra tredje mäns (samhället i stort) intresse att försäkringsbedrägerier och andra brott motverkas och att stöldgods kan återfinnas.

[2] Skäl 47 i dataskyddsförordningen.

2.2 Behandling av känsliga personuppgifter

Inom ramen för en utredning av ett oklart försäkringsfall kan det även, beroende på försäkringsfallets natur, vara nödvändigt att behandla uppgifter om hälsa och andra känsliga personuppgifter. Enligt artikel 9 punkten f får känsliga personuppgifter behandlas om det är nödvändigt för att fastställa, göra gällande eller försvara rättsligt anspråk. Denna punkt är regelmässigt tillämplig för försäkringsföretagens utredningsverksamhet under förutsättning att uppgifterna är nödvändiga för att inom ramen för utredningen fastställa, göra gällande eller försvara rättsliga anspråk som riktas eller kan riktas mot försäkringsföretaget.

2.3 Behandling av uppgifter om brott

Enligt artikel 10 får behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder endast utföras under kontroll av en myndighet eller om det särskilt tillåtet enligt nationell rätt. Enligt 5 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning får personuppgifter som avses i artikel 10 behandlas av andra än myndigheter om behandlingen är nödvändig för att 1) rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller 2) en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras. Behandling av personuppgifter som rör fällande domar som är nödvändig för att utreda oklara försäkringsfall är tillåten enligt punkten 1 eftersom det är fråga om att fastställa ett rättsligt anspråk, begäran om försäkringsersättning.

Rekommendation

Försäkringsföretag kan behandla personuppgifter vid utredning av oklara försäkringsfall med stöd av artikel 6 punkterna b (fullgörande av avtal), c (rättslig förpliktelse)och f (intresseavvägning). Punkten b kan dock bara åberopas när ersättningsanspråket framställs av försäkringstagaren själv.

Försäkringsföretag kan även behandla känsliga personuppgifter vid utredning av oklara försäkringsfall med stöd av artikel 9 punkten f om det är nödvändigt för att fastställa, göra gällande eller försvara rättsligt anspråk.

I utredningsverksamhet kan även personuppgifter om lagöverträdelser som innefattar brott och brottmålsdomar behandlas med stöd av 5 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning.
Se även avsnitt 4 nedan när det gäller förutsättningarna för varnande tips till annat/andra försäkringsföretag.

3. Informationsskyldighet

Dataskyddsförordningen innehåller regler om skyldighet att dels självmant lämna viss information till den registrerade, dels lämna ytterligare information på begäran bland annat genom ett registerutdrag.

3.1 Information som ska lämnas självmant

Enligt artiklarna 13 och 14 är den personuppgiftsansvarige skyldig att självmant lämna viss information om behandlingen av uppgifter till den registrerade. Information ska till exempel lämnas om den personuppgiftsansvariges identitet,

ändamålet/n med behandlingen, till vilka kategorier av mottagare informationen kan lämnas ut m.m.

När personuppgifterna samlas in från någon annan än den registrerade själv, är huvudregeln att informationen ska lämnas till den registrerade

- inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,
- om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller
- om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut första gången.

Det finns vissa undantag från informationsplikten i artikel 14.5 b, bland annat om uppfyllandet av informationsplikten skulle göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen. I sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen.

Det finns dessutom undantag från informationsplikten för personuppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400), se 5 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddslag.

3.2 Information som ska lämnas på begäran

Enligt artikel 15 har en registrerad också rätt att begära ett registerutdrag med alla de personuppgifter som behandlas om honom eller henne.

En förutsättning för att uppgifterna ska ingå i registerutdraget är dock att de omfattas av dataskyddsförordningens tillämpningsområde enligt artikel 2.1 som stadgar att förordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Information behöver inte lämnas om personuppgifter *i löpande text* i följande fall[3]:

- Den löpande texten har inte fått sin slutliga utformning när ansökan görs och uppgifterna har inte lämnats ut till tredje man. Som exempel kan nämnas koncept och utkast till en text. Undantaget gäller dock inte om uppgifterna har behandlats under längre tid än ett år.

- Den löpande texten utgör minnesanteckning eller liknande och uppgifterna har inte lämnats ut till tredje man. Undantaget avser promemorior och liknande som har kommit till bara för att förbereda ett ärende. Som exempel kan nämnas en föredragningspromemoria som används för att förbereda ett ärende för avgörande.

[3] 5 kap. 2 § lagen om kompletterande bestämmelser till EU:s dataskyddsförordning.

Det finns även ett undantag från informationsplikten för personuppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400), se 5 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddslag.

Rekommendation

Försäkringsföretag har regelmässigt rutiner för att självmant lämna obligatorisk information till försäkringstagare och skadelidande. Av informationen bör det bland annat framgå att uppgifter kan lämnas till annat försäkringsföretag och Larmtjänst AB. Vid utredning av oklara försäkringsfall förekommer det att personuppgifter registreras eller behandlas på annat sätt även beträffande andra personer, till exempel vittnen. Rutiner måste finnas för att lämna information även till sådana personer. Information behöver dock inte lämnas om den registrerade redan förfogar över informationen eller om annat undantag från informationsskyldigheten är tillämpligt enligt artikel 14.5.

Skyldigheten att på begäran lämna registerutdrag gäller även utredningsärenden förutsatt att personuppgifterna omfattas av dataskyddsförordningens tillämpningsområde enligt artikel 2.1. Rutiner bör därför finnas för att fullgöra även denna informationsplikt. Förutom de undantag som anges ovan beträffande vissa uppgifter i löpande text, bör försäkringsföretag kunna göra undantag beträffande uppgifter av följande slag:

- Personanknuten information som samlats in inför en domstolsprocess, om det kan antas att ett utlämnande av informationen skulle försämra företagets ställning som part i rättegången.
- Uppgifter om att en person misstänks för försäkringsbedrägeri eller annan brottslig verksamhet, medan utredning pågår.
- Uppgifter om identitet på vittnen.

Stöd för dessa undantag finns i 5 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, samt i prop. 2017/18:105 s. 107 och 202 med hänvisning till att tidigare praxis enligt 27 § PuL bör kunna vara vägledande (se prop. 1997/98:44 s 84).

4. Utlämnande av uppgift till annat försäkringsföretag eller myndighet

I samband med utredningsverksamhet förekommer det ibland anledning att misstänka att ett eller flera andra försäkringsföretag har utsatts för eller kan komma att utsättas för brott eller försök till brott. Frågan är om det då är tillåtet att lämna sådan information till berört/berörda företag.

Begreppet *behandling* av personuppgift omfattar även ”utlämnande genom överföring, spridning eller tillhandahålla på annat sätt”. En förutsättning för att det ska vara tillåtet för ett försäkringsföretag att lämna ett ”varningstips” till annat företag är därmed att den registrerade först samtycker till detta eller att någon annan grund för behandling är tillämplig.

Att begära samtycke av en misstänkt gärningsman är inte realistiskt. Däremot får en uppgift behandlas (till exempel lämnas ut) om detta är nödvändigt för ”ett ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade

intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter”.[4]

I skälen till dataskyddsförordningen anges att sådan behandling som är absolut nödvändig för att förhindra bedrägerier utgör ett berättigat intresse för berörd personuppgiftsansvarig.

Som exempel på en situation som kan vara avsedd med formuleringen om utlämnande till tredje man, nämns i den juridiska litteraturen att ”en personuppgiftsansvarig behandlar personuppgifter som kan tyda på att en viss person planerar att utföra ett bedrägeri mot en annan personuppgiftsansvarig, till vilken personuppgifterna lämnas ut”.[5] Detta exempel ger stöd för att försäkringsföretag kan varna ett annat företag vid misstanke om att det andra företaget har utsatts för eller kan komma att utsättas för brott eller försök till brott.

Om informationen rör en lagöverträdelse som innefattar brott, ställs det särskilda krav, se ovan.

Ett varnande tips till annat försäkringsföretag om brottsmisstanke kan naturligtvis vara nödvändigt för att detta företag ska kunna försvara sig mot ett felaktigt ersättningsanspråk.

Det förekommer även att myndigheter begär uppgift från försäkringsföretag om viss person. Myndigheterna har oftast lagstöd för begäran men det kan vara svårt för försäkringsföretaget att bedöma om det finns sådant stöd.

Rekommendation Försäkringsföretag kan lämna varnande tips till annat/andra försäkringsföretag om det uppkommer misstanke om att detta/dessa företag har utsatts för eller kommer att utsättas för brott eller försök till brott. En förutsättning för detta är dock att det finns konkret anledning till misstanke och att informationen bara gäller ett enskilt fall. Se även avsnitt 5 nedan angående gallring.
Då myndighet begär att uppgifter om viss person ska lämnas ut, bör försäkringsföretaget begära att myndigheten anger vilket lagstöd som finns för begäran.

5. Gallring

Ett grundläggande krav i dataskyddsförordningen är att personuppgifter inte sparas i en form som möjliggör identifiering av den registrerade längre än *nödvändigt* med hänsyn till ändamålet med behandlingen.[6] Därefter måste uppgifterna gallras. Det är alltså inte tillåtet att spara personuppgifter bara för att ”de kan vara bra att ha”. *Gallring* innebär att personuppgifterna förstörs (raderas) permanent eller avidentifieras.

I detta sammanhang måste det å ena sidan beaktas att det i utredningsärenden kan finnas information som är både omfattande och dessutom av mycket integritetskänslig natur. Å andra sidan måste det också beaktas att försäkringsföretag i sådana ärenden kan ha starkt behov av att bevara uppgifter under lång tid, bland annat på grund av gällande preskriptionsregler och skadelidandes rätt till omprövning. En avvägning mellan dessa intressen och behov måste ske.

[4] Artikel 6.1.f i GDPR.

[5] Se S Öman och H-O Lindblom, Personuppgiftslagen, en kommentar, 4 uppl s 241.

[6] Artikel 5.1.e GDPR.

Rekommendation

Försäkringsföretag ska ha systematiska rutiner för att gallra personuppgifter som man behandlar för ändamålet att utreda oklara försäkringsfall ur ärendehanteringssystem och andra register för utredarstöd. Detta hindrar inte att uppgifterna fortfarande kan bevaras i ett system eller en akt för försäkrings- eller skadeärende om de har insamlats och fortfarande behövs för sådant ändamål.

Gallringsrutinerna bör anknyta både till utredningens status och till gällande preskriptionsfrister enligt följande.

- I utredningsärende som resulterar i att utredare återlämnar skadan till verksamheten för ordinarie skadereglering och ersättning, kan uppgifter som är *nödvändiga* för att hantera redan framställda och eventuella framtida ersättningsanspråk sparas. Detsamma gäller om den skadelidande återkallar ett framställt ersättningsanspråk men framtida ersättningsanspråk kan aktualiseras i ärendet. Uppgifter som sparas får bevaras under samma period som skadeakten sparas. Övriga personuppgifter, som inte är nödvändiga för redan framställda eller framtida ersättningsanspråk, bör gallras senast sex månader efter det att utredningen avslutats, om det inte föreligger särskilda skäl i ett enskilt fall.
- I utredningsärende som resulterar i att anspråket på ersättning för skada avböjs, kan uppgifter som är *nödvändiga* för att motivera avböjandebeslutet sparas. Uppgifter som sparas får bevaras under samma period som skadeakten sparas. Övriga personuppgifter ska gallras senast sex månader efter det att utredningen avslutats, om det inte föreligger särskilda skäl i ett enskilt fall.
- För det fall utredningsärende avser egendom som frånhänts någon genom brott, kan ovan angivna frister för gallring alternativt knytas till relevanta frister enligt lagen om godtrosförvärv.
- Varnande tips om misstanke om brott eller försök till brott, ska gallras om tipset inte föranlett utredning om oklart försäkringsärende inom högst tre år från den dag då tipset inkom.[7] Om det föreligger särskilda skäl i ett enskilt fall kan uppgifterna sparas under längre tid.

6. Mängden information

Enligt artikel 5 punkten c ska personuppgifter som behandlas vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).

I ett utredningsärende kan det förekomma en mängd uppgifter av olika slag. Det är angeläget att försäkringsföretag inte behandlar fler uppgifter än nödvändigt och att de uppgifter som behandlas är relevanta. Samtidigt kan det ibland vara svårt att i ett tidigt skede bedöma vilka uppgifter som verkligen har betydelse för utredningen.

Rekommendation

Om det i ett pågående utredningsärende kan konstateras att viss eller vissa inkomna personuppgifter saknar betydelse för utredningen, ska dessa uppgifter

[7] Tidfristens längd är anpassad till erfarenheten att det ibland dröjer relativt lång tid från tidpunkten för tipset till dess brott eller försök till brott utförs.

snarast gallras om detta är möjligt och inte medför en uppenbart oproportionerlig arbetsinsats.

7. Säkerhet

Försäkringsföretag och personuppgiftsbiträden (exempelvis en extern utredare som är kontrakterad av försäkringsföretaget) måste enligt artikel 32 vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Vid bedömningen av vad som utgör en lämplig säkerhetsnivå bör det bland annat beaktas vilka tekniska möjligheter som finns och kostnaden för att genomföra åtgärderna. En viktig utgångspunkt vid bedömningen är

- vilken typ av *uppgifter* som behandlas, d v s hur känsliga uppgifterna är
- vilken typ av *behandling* som utförs, d v s vilka risker som är förknippade med behandlingen.

Om ett försäkringsföretag anlitar personuppgiftsbiträde föreligger det enligt dataskyddsförordningen en skyldighet att upprätta ett avtal med uppdragstagaren om behandlingen. Avtalet ska säkerställa att de säkerhetskrav som föreskrivs i dataskyddsförordningen uppfylls.

Rekommendation

Vid utredningar av oklara försäkringsfall förekommer det ofta uppgifter som är känsliga och därför ställer krav på en hög säkerhetsnivå vid behandlingen. All behandling av sådana uppgifter ska ske med beaktande av dataskyddsförordningens bestämmelser och tillsynsmyndighetens vid var tidpunkt gällande råd och rekommendationer om säkerhet för personuppgifter. Följande bör särskilt beaktas:

- Uppgifter i utredningsärenden ska bara vara tillgängliga för därtill behörig personal. Åtkomst till sådana uppgifter bör loggas och systematiskt följas upp.
- Vid elektronisk kommunikation måste säkerhetsåtgärder vidtas för att hindra obehörig åtkomst. Om känsliga uppgifter förmedlas via e-post ska denna krypteras eller skyddas på annat likvärdigt sätt. Vid åtkomst till känsliga uppgifter över öppet nät måste mottagarens identitet säkerställas.

8. Uppföljning och kontroll m.m.

Rekommendation

Det är angeläget att försäkringsföretag säkerställer att alla anställda och uppdragstagare som arbetar med utredning av oklara försäkringsfall, får tillräcklig kunskap om hur personuppgifter ska behandlas i samband med sådana utredningar. Försäkringsföretag ska även ha rutiner för utvärdering och kontroll av hur lagregler och interna instruktioner följs.

9. Ikraftträdande

Denna rekommendation ersätter rekommendationen av den 10 juni 2015 och träder i kraft den 1 november 2018. Den gäller försäkringsfall, skadehändelser och tips som anmäls eller inkommer från och med den 1 november 2018.