Svensk Försäkring

Rekommendation om hantering av personuppgifter om hälsa och andra känsliga personuppgifter inom försäkringsbranschen

Svensk Försäkring är en branschorganisation för svenska försäkringsföretag. De försäkringsföretag som har rätt att meddela trafikförsäkring i Sverige är skyldiga att vara medlemmar i Trafikförsäkringsföreningen (TFF). Inom båda organisationerna administreras även ett flertal skadereglerings- och försäkringsnämnder.

1. Syfte och omfattning

I försäkringsverksamhet behandlas frekvent uppgifter om enskilda personers hälsa. Sådana personuppgifter är alltid att anse som känsliga[1]. Försäkringsföretagen behandlar även andra känsliga personuppgifter till exempel om medlemskap i en fackförening.

Vidare kan det förekomma att försäkringsföretag behandlar integritetskänsliga uppgifter som till exempel uppgifter om fällande domar i brottmål eller överträdelser som innefattar brott.

Denna rekommendation lägger fast allmänna principer och utgör god sed inom försäkringsbranschen för försäkringsgivares behandling av känsliga personuppgifter samt uppgifter om fällande domar i brottmål eller överträdelser som innefattar brott. Rekommendationen tydliggör också hur försäkringsföretagen behandlar sådana personuppgifter.

Rekommendationen utgör endast en komplettering av de grundläggande bestämmelser som finns i försäkringsrörelselagen (FRL), försäkringsavtalslagen (FAL), övrig lagstiftning för försäkringsföretag samt Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (nedan benämnd dataskyddsförordningen), lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och därtill anknytande förordning samt riktlinjer från Datainspektionen och Europeiska dataskyddsstyrelsen.

Rekommendationen omfattar sådan behandling av känsliga personuppgifter som utförs av:

[1] I dataskyddsförordningen används i huvudsak benämningen särskilda kategorier av personuppgifter i stället för känsliga personuppgifter. I lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning används i stället benämningen känsliga uppgifter.

- TFF
- försäkringsföretag/återförsäkringsföretag som är medlem i Svensk Försäkring och/eller TFF och
- försäkrings-/skaderegleringsnämnd som administreras av Svensk Försäkring eller TFF.

Även Svensk Försäkring har att i tillämpliga delar beakta hanteringsreglerna i rekommendationen.

Försäkringsföretag används som övergripande term för alla tre kategorier i nedanstående rekommendation.

2. Rättslig grund för behandling av personuppgifter

2.1 Bakgrund

Enligt dataskyddsförordningen måste all behandling av personuppgifter vila på en rättslig grund. En grundläggande förutsättning för behandling är således att någon av de rättsliga grunder som anges i artikel 6 är tillämpliga.

För behandlingarna måste ändamålen med behandlingen fastställas, liksom den rättsliga grund på vilken denna sker. Den rättsliga grunden för en behandling av en viss typ av personuppgift kan vara olika, beroende på för vilket ändamål behandlingen sker. Försäkringsföretaget är skyldigt att informera den registrerade om vilken grund som åberopas för respektive behandling.

Enligt artikel 9.1 i dataskyddsförordningen är det förbjudet att behandla vissa känsliga personuppgifter. Det finns dock undantag från detta förbud, vilka också framgår av artikel 9.

2.2 Rättslig grund enligt artikel 6 i dataskyddsförordningen

För försäkringsverksamhet kan flera rättsliga grunder bli tillämpliga för de olika ändamål som försäkringsföretag behandlar personuppgifter för. De som kan bli aktuella är 6.1.a (samtycke), 6.1. b (fullgörande av avtal), 6.1.c (rättslig förpliktelse) eller 6.1.f (berättigat intresse). Här redogörs för några av dessa grunder.

2.2.1 Fullgörande av avtal

Den rättsliga grunden fullgörande av avtal är tillämplig i de fall behandlingen avser uppgifter rörande parten i avtalet, det vill säga försäkringstagaren. I de fall det är fråga om uppgifter om någon annan person kopplad till en försäkring, såsom till exempel en försäkrad eller en förmånstagare, är det dock tveksamt om denna grund kan åberopas då dessa inte är avtalsparter. I kommentaren till PuL anges att det är en förutsättning för att kunna tillämpa grunden fullgörande av avtal att den registrerade själv är avtalspart och det finns inget som tyder på att detta har

förändrats.[2] Om behandlingen avser uppgifter om någon annan än försäkringstagaren kan i stället framför allt punkten c, rättslig förpliktelse, vara tillämplig.

2.2.2 Rättslig förpliktelse

Den rättsliga grunden rättslig förpliktelse torde i första hand avse offentligrättsliga förpliktelser. Men det finns även i civilrättsliga författningar bestämmelser som utgör eller kan medföra rättsliga förpliktelser, såsom inom arbetsrätten. Även förpliktelser som följer av vissa lagreglerade avtal, exempelvis försäkringsavtal av betydelse för andra än parterna eller gynnande tredjemansavtal, skulle kunna omfattas av denna grund.[3] I sådana avtal finns ofta förpliktelser som kan härledas från krav i exempelvis lag eller kollektivavtal och som inte bara gäller mellan avtalsparterna utan även mot tredje part och som förutsätter behandling av personuppgifter.

Den rättsliga grunden rättslig förpliktelse skulle också kunna tillämpas avseende behandling av uppgifter rörande avtalsparten, det vill säga försäkringstagaren, i de fall behandlingen har sin grund i fullgörande av försäkringsavtal och fullgörande av en skyldighet som framgår av tvingande regler i FAL och inte primärt vilar på obligationsrättslig grund.

2.3 Behandling av känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen

2.3.1 Inledning

För att kunna behandla känsliga personuppgifter räcker det inte att finna en rättslig grund i artikel 6 utan ett undantag i artikel 9.2 måste också vara tillämpligt.

Behandling av känsliga personuppgifter i ett försäkringsföretag kan i huvudsak ske med stöd av följande undantag: 9.2.f (rättsligt anspråk), 9.2.b (social trygghet), 9.2.j (statiska ändamål) eller 9.2.a (samtycke).

2.3.2 Behandling av personuppgifter om hälsa

För riskprövning av en personförsäkring behöver försäkringsföretag i regel behandla känsliga personuppgifter i form av hälsouppgifter på individuell nivå[4], men också på kollektiv nivå[5].

---

[2] Öman och Lindblom: Personuppgiftslagen – En kommentar, 2007, sid 184-185. Se även SOU 1997:39 s. 362 f.

[3] Prop. 2017/18:105 s. 53 ff och 188-189.

[4] Se bland annat SOU 2016:37 s. 22, Att försäkringsbolagens riskprövning ska göras på individuell grund innebär enligt utredningen att försäkringsbolaget har ett utredningsansvar när det gäller den försäkringssökandes hälsotillstånd, om bolaget överväger att neka försäkring. Det innebär att försäkringsbolaget i de fallen har en skyldighet att klargöra eventuella otydliga hälsouppgifter som lämnas av den försäkringssökande. I de tveksamma fallen måste försäkringsbolaget även aktivt ta reda på de uppgifter om en enskild försäkringssökandes hälsotillstånd som kan ha betydelse för den personens möjlighet att teckna en försäkring.

[5] Av SOU 2016:37 s. 203 f. framgår också att försäkringsföretaget måste använda sin professionella erfarenhet, exempelvis bolagets egen dokumenterade sjukdoms- och skadestatistik.

Svensk Försäkring

Försäkringsföretag behandlar känsliga personuppgifter på individuell nivå exempelvis för handläggning av ansökan om försäkring, handläggning av ansökan om ändring av försäkring och vid försäkringsfall.

Vid handläggning av en ansökan måste försäkringsföretaget exempelvis kunna göra en bedömning av den risk bolaget tar genom att bevilja eller ändra en försäkring och den försäkrades hälsa är då en viktig parameter.

Det har många gånger konstaterats att socialförsäkringar och kollektiva försäkringar i de flesta fall ger ett otillräckligt skydd och att privata försäkringar fyller en viktig samhällelig funktion.[6] Detta är ett av skälen bakom kontraheringsplikten[7] som, såvitt avser personförsäkring, innebär att ett försäkringsföretag inte får neka att teckna en försäkring det annars erbjuder när det fått in de uppgifter som behövs om det inte finns särskilda skäl att vägra med hänsyn till risken för framtida försäkringsfall, den avsedda försäkringens art eller någon annan omständighet.

Kontraheringsplikten innebär således inte en absolut skyldighet att tillhandahålla försäkring, utan ger försäkringsföretaget rätten att göra en riskprövning. Denna ska vara individuell. Om försäkringsföretaget överväger att neka försäkring har det ett utredningsansvar och en skyldighet att klargöra eventuella otydliga hälsouppgifter som lämnats av den sökande, vilket även innefattar att aktivt ta reda på de uppgifter som kan ha betydelse för personens möjligheter att teckna försäkring.

I samband med ett försäkringsfall kan behandling av personuppgifter avseende hälsa vara nödvändigt i syfte att fastställa eventuell rätt till ersättning och nivå på denna samt för att kunna utesluta förekomsten av oriktiga uppgifter.

På kollektiv nivå kan behandling av känsliga personuppgifter vara nödvändig för att försäkringsföretaget ska kunna göra beräkningar av de totala riskerna försäkringsföretaget tar och för att ständigt kunna uppdatera sina riskantaganden samt för att kunna bestämma premier.[8]

Rättsligt anspråk (artikel 9, punkt f)

Behandling av hälsouppgifter får ske om denna är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras. Det bekräftas av förarbetena till personuppgiftslagen att viss behandling av känsliga uppgifter kan vara nödvändig för att fastställa om någon har rätt till en förmån eller en rättslig skyldighet gentemot någon annan.[9] Som exempel nämns behandling av hälsouppgifter i vissa försäkringssammanhang där inhämtande av hälsouppgifter är en förutsättning för att få teckna en viss försäkring.[10]

Behandling av hälsouppgifter får också ske om ett försäkringsföretag har nekat att tillhandahålla eller ändra en försäkring. Den sökande kan påkalla domstolsprövning

---

[6] Se bl.a. SOU 2016:37 s. 58 och prop. 2017/18:105 s. 80.

[7] 3 kap. 1 § och 11 kap. 1 § FAL.

[8] Se även avsnitt 8.

[9] SOU 1997:39 s. 375 ff.

[10] I prop. 2017/18:105 s. 76 framgår det att, i den utsträckning det inte framkommer något annat i förordningen eller genom EU-domstolens praxis, framstår det naturligt att undantagen från förbudet att behandla känsliga uppgifter tolkas i linje med den praxis som har utvecklats enligt motsvarande bestämmelser i dataskyddsdirektivet och personuppgiftslagen.

av frågan enligt 16 kap. 7 § FAL och godtas inte försäkringsföretagets ståndpunkt kan domstolen förklara att den sökande har rätt att teckna eller ändra försäkringen.

När ett försäkringsavtal meddelats är viss behandling av hälsouppgifter nödvändig för att fastställa parternas rättsliga anspråk till följd av avtalet, exempelvis för att kunna bedöma rätt till ersättning vid försäkringsfall. Det gäller också vid prövning vid exempelvis nämnder och domstolar. Sådan behandling är således tillåten enligt art 9.2 f i dataskyddsförordningen.

Även viss behandling av känsliga uppgifter som sker för kollektiva ändamål, bland annat för beräkning av risktagande är tillåten enligt samma rättsliga grund.

Social trygghet (artikel 9.1, punkt b)

Behandling av hälsouppgifter får ske om det är nödvändigt för att fullgöra skyldigheter och utöva rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd.

I propositionen 2017/18:105 s. 80 anges att många gruppförsäkringar och kanske särskilt flera av de som har anknytning till arbetslivet eller som följer av kollektivavtal kan fylla en viktig funktion inom området social trygghet och socialt skydd. Det framgår vidare att denna grund därför kan vara tillämplig för försäkringsföretag som administrerar sådana försäkringar.

Även andra typer av försäkringsavtal kan med fog hävdas fylla en lika viktig funktion inom området social trygghet och socialt skydd. Denna grund skulle därför även kunna vara tillämplig för andra typer av försäkringsavtal än de som nämns i propositionen.

Samtycke (artikel 9, punkt a)

En enskild kan i samband med ansökan om försäkring lämna sitt samtycke till att försäkringsföretaget behandlar uppgifter om hälsa[11]. Denna grund lär i regel enbart användas för den behandling som sker för att handlägga en sökandes ansökan om försäkring eller ansökan om ändring av försäkring. Annan nödvändig behandling av hälsouppgifter torde huvudsakligen grunda sig på annan rättslig grund än samtycke. Av försäkringsföretagets begäran om samtycke bör det tydligt framgå vilken behandling samtycket avser.

2.3 Behandling av andra känsliga personuppgifter än hälsa

Försäkringsföretagen behöver behandla också andra känsliga personuppgifter än om hälsa. Ett exempel är vid gruppförsäkringsavtal där det kan vara nödvändigt för att fastställa vilken grupp en enskild tillhör. En registrering av medlemmar i den försäkrade gruppen kan då innebära en indirekt registrering av känsliga personuppgifter, exempelvis om försäkringsavtalet avser medlemmar i en fackförening, ett politiskt parti eller en annan ideell förening.[12]

[11] För information om vilka krav som ställs på ett sådant samtycke, se dataskyddsförordningen.

[12] Av artikel 9 i dataskyddsförordningen framgår att personuppgifter som avslöjar bland annat politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening är känsliga personuppgifter.

Behandling av sådana känsliga personuppgifter i ett försäkringsföretag kan i huvudsak ske med stöd av följande undantag: 9.2.f (rättsligt anspråk), 9.2.b (social trygghet), 9.2.j (statistiska ändamål) eller 9.2.a (samtycke).

Rättsligt anspråk (artikel 9.2 punkten f)

Behandling av känsliga personuppgifterna kan vara nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras (artikel 9.1 punkt f). Som angetts ovan kan viss behandling av känsliga uppgifter vara nödvändig för att fastställa om någon har rätt till en förmån eller en rättslig skyldighet gentemot någon annan. Det kan gälla till exempel för att bestämma om en enskild har rätt att teckna en viss gruppförsäkring.

Denna grund kan exempelvis vara tillämplig när behandlingen är nödvändig till följd av avtal med fackliga organisationer om gruppförsäkring för deras medlemmar (jfr prop. 1997/98:44 s. 124 och prop. 2017/18:105 s. 80). Personuppgifter om medlemskap i en fackförening behöver då behandlas.

Social trygghet (artikel 9.2 punkten b)

I propositionen 2017/18:105 s. 80 anges att många gruppförsäkringar och kanske särskilt flera av de som har anknytning till arbetslivet eller som följer av kollektivavtal kan fylla en viktig funktion inom området social trygghet och socialt skydd (artikel 9.1 punkt b). Det anges vidare att undantaget om socialt skydd därför kan vara tillämpligt för de som tillhandahåller eller administrerar sådana försäkringar.

3. Möjlighet att behandla uppgifter om fällande domar om brott och lagöverträdelser som innefattar brott

Enligt artikel 10 i dataskyddsförordningen får behandling av uppgifter om domar och överträdelser som innefattar brott endast utföras under kontroll av myndighet eller om det är tillåtet enligt nationell rätt. I 5 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning finns sådana nationella bestämmelser. De tillåter att personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel behandlas av andra än myndigheter om

1) behandlingen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller

2) behandlingen är nödvändig för att en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.

Försäkringsföretag kan behöva behandla uppgifter om domar om brott och lagöverträdelser som innefattar brott, exempelvis för att pröva rätten till ersättning eller för att efter skadereglering återkräva ersättning från den som vållat skadan.

I de fall en uppgift om fällande dom eller lagöverträdelse som innefattar brott är nödvändig för att pröva rätten till ersättning eller för att efter skadereglering återkräva ersättning från den som vållat skadan är behandlingen nödvändig för att fastställa ett rättsligt anspråk, det vill säga en begäran om försäkringsersättning (första

punkten i ovan nämnd förordning).[13] Detsamma gäller när uppgifterna är nödvändiga för riskbedömning.

Livförsäkringsföretag har vidare skyldigheter enligt till exempel penningtvättsregleringen som kan innebära behov av att behandla sådana uppgifter. Uppgifter som behandlas för att motverka penningtvätt kan därför vara nödvändiga för att uppfylla en rättslig förpliktelse (andra punkten i ovan nämnd förordning).

4. Fullmakt för att inhämta personuppgifter om hälsa enligt FAL

Försäkringsföretags möjligheter att begära en fullmakt för att inhämta hälsouppgifter från andra än den sökande är reglerade i FAL. Enbart om det är nödvändigt för att pröva en försäkringsansökan får ett försäkringsföretag begära en fullmakt för att inhämta uppgifter om en persons hälsotillstånd från andra än den sökande, till exempel olika vårdgivare.[14] Detsamma gäller om det behövs för att reglera ett försäkringsfall.[15] Fullmakten ska lämnas på en särskild handling. En fullmakt som lämnats enligt bestämmelserna i FAL är, om det inte uttryckligen framgår av fullmaktsblanketten, inte att betrakta som ett samtycke till behandling av personuppgifter enligt dataskyddsförordningen.

Det finns ytterligare rekommendationer om fullmakter i Svensk Försäkrings rekommendationer angående försäkringsbolagens bruk av fullmakter.

Hanteringsregler[16]

- Fullmakt enligt FAL ska endast omfatta en försäkringsansökan, ett skadereglerингsärende eller annat specifikt ärende.[17] Fullmakt som utfärdats vid försäkringsansökan får dock utformas så att den även innefattar sådan skadereglering som sker efter dödsfall.
- Fullmakter ska helst ligga i separata dokument.[18]
- Fullmakter ska innehålla tydlig information om syfte, omfattning och vad fullmakten innebär.
- Det ska tydligt framgå av fullmakten att den gäller till dess den återkallas eller ärendet avslutas. I samband med att fullmakten lämnas bör även informeras om de konsekvenser som kan följa av att fullmakt återkallas innan ett ärende avslutas.

5. Skyldighet att lämna information till de registrerade

Enligt artiklarna 13-14 i dataskyddsförordningen har den personuppgiftsansvarige en skyldighet att lämna viss information till de registrerade när personuppgifter samlas in om dem. När ett försäkringsföretag är personuppgiftsansvarigt behöver

---

[13] Se även Svensk Försäkrings rekommendationer om behandling av personuppgifter inom försäkringsföretagens utredningsverksamhet.
[14] 11 kap. 1 a § FAL som dock benämner det samtycke i stället för fullmakt.
[15] 7 kap. 1 a § och 16 kap. 1 a § FAL som dock benämner det samtycket i stället för fullmakt.
[16] Se även punkt 12 Ikraftträdande.
[17] En försäkringsansökan eller skadeanmälan kan omfatta flera försäkringsprodukter.
[18] Med dokument avses såväl dokument i pappersform som motsvarande elektroniska lösningar.

det därför lämna denna information. Reglerna gäller även då hälsouppgifter och andra känsliga personuppgifter samlas in.

Försäkringsföretaget ska till den registrerade bland annat lämna sina kontaktuppgifter, ge information om den avsedda personuppgiftsbehandlingen och om de registrerades rättigheter.

Den information som lämnas ska vara klar och tydlig. Den kan tillhandahållas genom en fysisk skriftlig handling, eller elektroniskt när så är lämpligt. Den kan även ges muntligt om den registrerade begär det.

Informationen behöver inte lämnas om och i den mån den registrerade redan förfogar över informationen.

Om försäkringsföretaget behandlar uppgifter som skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen hos en myndighet gäller inte den registrerades rätt till information.[19] Detta innebär att försäkringsföretag kan tillämpa sekretess i förhållande till den försäkrade vid dennes utnyttjande av registrerades rättigheter i vissa angivna situationer.

Informationen kan ges i ett eller flera steg.[20] I det första steget behöver inte all information ges, förutsatt att den registrerade tydligt får upplysning om vart fullständig information kan erhållas. I den följande informationen ska all information ges.

6. Hantering av känsliga personuppgifter i registerutdrag

Om försäkringsföretaget behandlar uppgifter som skulle ha varit sekretessbelagda hos en myndighet gäller inte den registrerades rätt till information.[21] Detta innebär att försäkringsföretag kan tillämpa sekretess i förhållande till den försäkrade själv vid dennes utnyttjande av registrerades rättigheter i vissa angivna situationer, exempelvis rätten till registerutdrag. Det kan exempelvis gälla i viss utredningsverksamhet.[22]

När det gäller uppgifter om hälsa som den registrerade själv tillhandahållit försäkringsföretaget bör dessa normalt ingå i ett registerutdrag. När det är fråga om hälsouppgifter som försäkringsföretag själva eller med stöd av fullmakt inhämtat från annan än den registrerade, exempelvis uppgifter som förekommer i journaler, läkarintyg och läkarutlåtande, är det inte självklart att dessa uppgifter ska ingå i registerutdraget eftersom försäkringsföretaget på grund av begränsad insikt i hälsotillståndet hos den registrerade eller brist på den typ av medicinska kvalifikationer som krävs, inte kan pröva frågan om sekretess i förhållande till den registrerade. I stället kan försäkringsföretaget redovisa vilka handlingar som inhämtats och

[19] 5 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[20] I art 29-gruppens riktlinjer om öppenhet (WP260 rev. 01) beskrivs hur information kan ges i flera steg och vad som bör ingå i de olika stegen.
[21] 5 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[22] Se Svensk Försäkrings rekommendation om behandling av personuppgifter inom försäkringsföretagens utredningsverksamhet.

varifrån och hänvisa den registrerade till den vårdgivare som upprättat handlingarna, så att denne kan göra sekretessbedömningen.

7. Sekretess

Inom försäkringsbranschen har det sedan lång tid tillbaka tillämpats en frivilligt påtagen sekretess. När det gäller uppgifter om genetisk undersökning eller genetisk information finns det en lagstadgad sekretess enligt gällande försäkringsrörelselagstiftning.[23] Det finns även en lagstadgad sekretess i förhållande till förmånstagare.[24]

En av de grundläggande principerna i artikel 5[25] i dataskyddsförordningen är att personuppgifter ska behandlas på ett sätt som säkerställer att personuppgifternas integritet och konfidentialitet upprätthålls. Särskilt sträng sekretess bör tillämpas vid behandling av känsliga personuppgifter vilket exempelvis innebär krav på interna behörighetsbegränsningar till personuppgifterna samt i övrigt vidtagande av adekvata säkerhetsåtgärder i samband med behandling för att säkerställa att uppgifterna inte blir tillgängliga för en vidare krets än nödvändigt.[26]

Att lämna ut känsliga personuppgifter till tredje part kräver stöd av en rättslig grund, se ovan.

Hanteringsregler

- Försäkringsföretag ska se till att en tydlig sekretessförbindelse avseende uppgifter om enskilda personers hälsa undertecknas av anställda samt övriga som på försäkringsföretagets uppdrag kan komma att hantera sådana uppgifter.
- Försäkringsföretag ska upprätta interna rutiner som syftar till att säkerställa att uppgifter som omfattas av sekretess inte lämnas ut till obehöriga.

8. Säkerhet

Dataskyddsförordningen ställer krav på att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Uppgifterna måste till exempel skyddas både mot obehörigt intrång och mot förlust av information.

Vid fastställande av säkerhetsnivån måste det beaktas vilka tekniska möjligheter som finns och vad det skulle kosta att genomföra åtgärderna.

En viktig utgångspunkt vid bedömning av vilka säkerhetsåtgärder som krävs är vidare

---

[23] 4 kap. 16 § FRL. Uppgift om genetisk undersökning eller genetisk information som avser en enskild person får inte obehörigen röjas.

[24] 4 kap. 14 § FRL. En personuppgift som anger att en försäkringstagare har vidtagit dispositioner beträffande försäkringsbelopp som utfaller i framtiden till förmån för någon annan och som behandlas enligt personuppgiftslagen (1998:204) får inte lämnas ut till förmånstagaren.

25 Dataskyddsförordningen artikel 5 f; De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

[26] Även ytterligare artiklar i Dataskyddsförordningen ställer krav på att personuppgifter behandlas med adekvat säkerhet så att personuppgifterna inte blir tillgängliga för fler personer än nödvändigt.

- vilken typ av uppgifter som behandlas, det vill säga hur känsliga uppgifterna är, och
- vilken typ av behandling som utförs, det vill säga vilka risker som är förenade med behandlingen.

De kategorier av uppgifter som avses i art 9 dataskyddsförordningen, såsom uppgifter om en enskild persons hälsa, är alltid att anse som känsliga. Enligt Datainspektionen är även andra uppgifter om enskilds personliga och ekonomiska förhållanden inom försäkringsväsendet normalt att anse som integritetskänsliga.[27]

Detta förhållande ställer krav på en hög säkerhetsnivå hos försäkringsföretag vid all behandling av sådana uppgifter.

Om en ny typ av behandling sannolikt leder till en hög risk för personers rättigheter och skyldigheter ska försäkringsföretag enligt dataskyddsförordningen göra en konsekvensbedömning av skyddet av personuppgifter. En sådan bedömning krävs särskilt om det rör sig om behandling i stor omfattning av personuppgifter om hälsa.

Om försäkringsföretag anlitar utomstående för behandling av personuppgifter på ett sådant sätt att ett biträdesförhållande uppstår, 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.

Utöver regleringen i dataskyddsförordningen, kräver Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (nedan benämnd Solvens II-förordningen) att ett företag som outsourcar verksamhet eller funktioner som är av väsentlig betydelse vid sitt val av uppdragstagare ska försäkra sig om att outsourcingen följer kraven i Solvens 2-förordningen samt vid var tid gällande dataskyddsregler. Försäkringsföretaget ska också försäkra sig om att uppdragstagaren omfattas av samma krav på säkerhet och konfidentialitet som försäkringsföretaget för information både när det gäller företaget och dess kunder. Avtalet med uppdragstagaren måste tydligt ange att leverantören måste skydda konfidentiell information både när det gäller företaget och dess kunder. [28]

Hanteringsregler

- Försäkringsföretag ska tillse att personuppgifter och särskilt känsliga sådana behandlas på ett sätt som säkerställer att integritet och konfidentialitet upprätthålls genom att vidta adekvata säkerhetsåtgärder innefattande men inte begränsat till upprättande av behörighetsregelverk som säkerställer att uppgifterna endast behandlas av behöriga personer.
- Försäkringsföretag skall säkerställa att tillgängligheten till uppgifterna anpassas utifrån behovet. Detta kan ske exempelvis genom uppsättande av restriktiva interna behörighetsbegränsningar eller ett överförande av framför allt känsliga

[27] Datainspektionen, Allmänna råd angående säkerhet för personuppgifter, 1999, s. 17.
[28] Artikel 274 i Solvens II-förordningen, (EU) 2015/35.

personuppgifterna till särskilt system så att uppgifterna inte längre hålls tillgängliga i den dagliga hanteringen.
- Försäkringsföretag som behandlar uppgifter om enskilds hälsa eller andra känsliga personuppgifter måste observera att distansarbete är förenat med säkerhetsrisker. I den mån distansarbete tillåts måste det säkerställas att arbetet kan utföras med en godtagbar säkerhetsnivå. Detta gäller även vid outsourcad verksamhet och arbete som utförs av exempelvis rådgivande läkare.
- En personakt i pappersform är oftast mycket svår att återskapa om den förstörs eller förloras på annat sätt. Pappershandlingar med uppgifter om enskilds hälsa bör därför förvaras på brandsäkert sätt.
- Vid elektronisk kommunikation måste säkerhetsåtgärder vidtas för att hindra obehörig åtkomst. Som exempel kan nämnas att om känsliga personuppgifter förmedlas genom e-post bör denna vara krypterad eller skyddas på annat sätt.

9. Gallring

Principen om lagringsminimering i artikel 5 i Dataskyddsförordningen innebär att den tidsperiod under vilken personuppgifter får behandlas begränsas till ett strikt minimum. Om fortsatt behandling inte längre är nödvändig med hänsyn till ändamålen med behandlingen så måste behandlingen upphöra och uppgifterna raderas. Av skäl 39 i Dataskyddsförordningen[29] framgår att en personuppgiftsansvarig ska ta fram tidsfrister för gallring och regelbundet kontrollera att radering sker i enlighet med dessa. Dessa krav på gallring omfattar även ett försäkringsföretags behandling av hälsouppgifter och andra känsliga personuppgifter.

Vid framtagande av gallringsrutiner för hälsouppgifter måste det å ena sidan beaktas att det i till exempel patientjournaler ofta finns information som är både omfattande och dessutom av mycket integritetskänslig natur. Å andra sidan måste det också beaktas att försäkringsföretag ofta har starkt behov av att bevara hälsouppgifter under mycket lång tid, bland annat på grund av gällande lagstiftning om preskription och skadelidandes rätt till omprövning. Försäkringsföretag har behov av att kunna kontrollera att den försäkrade risken överensstämmer med verkliga förhållanden. Försäkringsföretag har även behov av att spara uppgifter om man har nekat en försäkring för att kunna försvara detta beslut i domstol om kontraheringsplikten aktualiseras. Försäkringsföretag har vidare behov av att under avtalstiden behandla uppgifter för att bedöma behoven av försäkringstekniska reserveringar. En avvägning mellan dessa intressen och behov måste ske vid uppställande av de tidsfrister för radering av personuppgifterna som ska gälla.

Hanteringsregler

- Försäkringsföretag ska ha rutiner och sätta upp tidsfrister för gallring av personuppgifter[30]. När personuppgifter avseende hälsa behandlas under en längre tid,

[29] Skäl (39) i Dataskyddsförordningen; *”Personuppgifter bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll.”*

[30] ”Så bör försäkringsbolag behandla känsliga personuppgifter”. Rapport från Datainspektionen efter ett tillsynsprojekt 2006.

ska försäkringsföretaget pröva om uppgifterna behövs för behandling i den dagliga verksamheten, eller om de endast behöver bevaras och lagras för framtida ändamål. Så kan till exempel vara fallet när hälsouppgifter har inhämtats för en riskbedömning i samband med ingående av avtalet och där uppgiften sedan behöver sparas för att vid ett eventuellt framtida skadefall kunna ingå i bedömningsunderlaget vid skaderegleringen.

10. Mängden uppgifter

I dataskyddsförordningen föreskrivs det att den personuppgiftsansvarige inte får behandla fler personuppgifter än som är nödvändigt med hänsyn till ändamålen med behandlingen (uppgiftsminimering). Vidare föreskrivs det att den ansvarige ska se till att de uppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen.

Försäkringsföretag har ofta anledning att begära in patientjournaler i samband med ansökan om försäkring och/eller vid skadereglering. Som konstaterats ovan kan sådana journaler innehålla både omfattande och mycket integritetskänslig information. Det är angeläget att försäkringsföretag inte behandlar fler uppgifter än nödvändigt. Å andra sidan är det ofta inte möjligt för en handläggare att i förväg bedöma vilka uppgifter i en patientjournal som är relevanta i ett försäkrings-/skaderegleringsärende.

Det är också ofta av stor vikt att få tillgång till en fullständig journal med en sammanhängande kedja av noteringar för att kunna göra en korrekt bedömning av ärendet.[31]

Hanteringsregler

- I de fall där det i förväg är möjligt att konstatera att endast uppgifter av visst slag och/eller beträffande viss tidsperiod är av betydelse för ärendets bedömning ska beställning av patientjournal begränsas i motsvarande mån.
- Om det säkert kan konstateras att vissa uppgifter i en inkommen journal saknar betydelse för ärendets bedömning, ska dessa uppgifter förstöras om detta är möjligt och inte medför en uppenbart oproportionerlig arbetsinsats.

11. Behandling av hälsouppgifter för statistiska ändamål

För att beräkna vilken premie en enskild ska betala gör försäkringsföretag statistiska beräkningar av den risk den enskilde står inför och därför tillför försäkringskollektivet. Beräkningar görs även för att säkerställa att företaget gör tillräckliga

[31] När det gäller värdet av en sammanhängande kedja av noteringar kan det nämnas att Högsta domstolen i rättsfallet NJA 2001 s 657 gjort följande bedömning: ”Generellt sett får journalanteckningar från besök som den olycksdrabbade tidigare har gjort hos läkare anses utgöra ett viktigt underlag för bedömningen av huruvida patientens tidigare svagheter under alla förhållanden skulle ha medfört de symptom som visat sig efter försäkringsfallet. Ett skäl till detta är att uppgifterna lämnats och anteckningarna gjorts utan tanke på det aktuella försäkringsärendet. Samtidigt måste beaktas att journalanteckningar kan vara behäftade med en betydande osäkerhet. Läkaren kan bl a ha missuppfattat eller överbetonat något patienten sagt. Osäkerheten förstärks av att journalanteckningarna kan ha upprättats med ett visst dröjsmål efter patientbesöket. Om det finns flera journalanteckningar med ett likartat innehåll, bör de dock kunna tillmätas ett avsevärt bevisvärde såvitt avser patientens status vid de aktuella läkarbesöken.”

avsättningar så att det kan betala försäkringsersättningar till de enskilda som drabbas av en skada. Sådana beräkningar görs för att uppfylla förpliktelser enligt FRL, Solvens II-förordningen och riktlinjer från EIOPA. Statistiska beräkningar görs även för att på andra sätt följa upp verksamheten och för andra statistiska ändamål.

Sådan vidarebehandling av personuppgifter är normalt inte oförenlig med de ursprungliga ändamålen för vilka personuppgifterna har samlats in. För att få vidarebehandla hälsouppgifter för statistiska ändamål måste dock försäkringsföretaget enligt dataskyddsförordningen säkerställa lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.[32]

12. Ikraftträdande och övergångsbestämmelser[33]

Rekommendationen gäller från och med den 1 november 2018 med de begränsningar som anges nedan.

- För livförsäkringsbolag gäller reglerna i punkt 4, ”Fullmakt för att inhämta personuppgifter om hälsa enligt FAL”, endast fullmakter som eventuellt inhämtas i samband med att försäkringsavtal ingås eller förnyas efter den 31 mars 2010.

- För andra Försäkringsföretag än livförsäkringsbolag gäller reglerna i punkt 4, ”Fullmakt för att inhämta personuppgifter om hälsa enligt FAL” med följande undantag.

- Skaderegleringsärenden som inletts före den 1 april 2010.

- Fullmakter som inhämtats vid försäkringsansökan före denna rekommendations ikraftträdande får, utan hinder av vad som annars gäller enligt punkt 4, användas vid skadereglering eller annat specifikt ärende som handläggs efter dödsfall.

- För nämnder och andra organisationer som inte är försäkringsföretag, omfattas ärenden som inkommer från och med den 1 april 2010

[32] Se prop. 2017/18:105 s. 124 f.
[33] Se även punkt 4 Fullmakt för att inhämta personuppgifter om hälsa enligt FAL.