

OMMVA

RLDST

REND

2024



Digitaliseringen alltmer märkbar i regleringen

2 Digitaliseringen alltmer märkbar i regleringen

Digitaliseringen påverkar alla delar av samhället och gör sig alltmer märkbar i regleringen. Det kommer flera EU-rättsakter som bland annat rör datadelning, artificiell intelligens och it-säkerhet. Den digitala utvecklingen innebär fördelar och utmaningar som påverkar många samhällsområden samtidigt, om än på olika sätt och i olika omfattning. Det är mot den bakgrunden som reglering av digitala frågor sällan är försäkrings- och tjänstepensionsspecifik utan kan beröra hela finanssektorn eller till och med aktörer från flera samhällssektorer. Vilka är utmaningarna med horisontella regelverk på det digitala området och hur kan vi möta dem?

2.1 Digitaliseringen förflyttar gränser även i regleringen

Reglering – ett verktyg för samhällsutveckling

Samhällsutveckling innebär ofta att det sker en utveckling som påverkar många samhällsområden samtidigt, men på olika sätt och i olika omfattning. Reglering är ett verktyg för att forma och styra samhällsutvecklingen. Två områden med en tydlig och omfattande påverkan på stora delar av samhället är hållbarhet och digital utveckling. Det är därför naturligt att EU-lagstiftaren, med EU-kommissionen i spetsen, har tagit beslut om och fortsätter att presentera en mängd förslag på dessa för samhällsutvecklingen centrala områden. Vi kommer i detta avsnitt att fokusera på regelutvecklingen på det digitala området.³⁹ Men först ska vi kortfattat belysa några särdrag i regleringen av försäkring och tjänstepensioner.

Försäkringsföretag och tjänstepensionsföretag är föremål för omfattande reglering. I stort sett all den regleringen är EU-rättsligt grundad, antingen genom direktverkande rättsakter eller genom direktiv som genomförts i svensk rätt. Syftet med regleringen är att upprätthålla ett högt konsumentskydd.

För försäkringsföretags rörelse gäller till exempel solvens II-regelverket, för tjänstepensionsföretag gäller andra tjänstepensionsdirektivet (IORP II) och för försäljning och annan distribution av försäkringar gäller direktivet om försäkringsdistribution. Utöver försäkringsspecifik reglering berörs försäkringsföretag av flera regelverk som är gemensamma för hela eller delar av finanssektorn som till exempel EU-direktivet om distansförsäljning av finansiella tjänster till konsumenter och förordningen om paketerade och försäkringsbaserade investeringsprodukter för icke-professionella investerare. Därutöver finns det många regelverk som har ett ännu bredare tillämpningsområde, till exempel penningtvättsregelverket, den allmänna dataskyddsförordningen (GDPR) och reglering på skatteområdet.

För försäkringsbranschen är EU:s regelgivning således central och regleringstakten fortsätter att vara hög. Ett återkommande inslag i ökande omfattning är översyner av befintliga regelverk. Som exempel kan nämnas att de allra flesta regelverk som nämns ovan antingen är föremål för översyn eller har nyligen varit det.

³⁹ Hållbarhetsreglering behandlas i avsnitt 5.

Digitaliseringen gör sig alltmer märkbar i regleringen

Under senare tid har digitaliseringen gjort sig alltmer märkbar i EU-regleringen, bland annat i form av flera nya horisontellt verkande förslag och färdiga rättsakter. Med horisontella förslag och rättsakter avses här sådana som inte endast berör försäkrings- och tjänstepensionsföretag utan karakteriseras av att tillämpningsområdet är brett, antingen hela finanssektorn eller till och med aktörer från flera olika samhällssektorer.

Att regleringstakten är hög på digitaliseringsområdet är knappast förvånande. Digitaliseringen påverkar i stort sett alla delar av samhället. Det handlar bland annat om att produkter kopplas samman eller integreras med digitala tjänster, om att data har blivit en drivkraft för tillväxt och innovation, om utökade analysmöjligheter med artificiell intelligens (AI) samt om ökad sårbarhet när det gäller cyberangrepp och andra it-relaterade störningar. EU-kommissionen har lagt fram flera förslag till reglering som tar sikte på dessa och andra förändringar med anledning av digitaliseringen. I flera fall handlar det om reglering som har betydelse för försäkringsbranschen.

”Det handlar bland annat om att produkter kopplas samman eller integreras med digitala tjänster, om att data har blivit en drivkraft för tillväxt och innovation, om utökade analysmöjligheter med AI samt om ökad sårbarhet när det gäller cyberangrepp och andra it-relaterade störningar.”

Sammankopplingen mellan produkter och digitala tjänster har bland annat betydelse i ansvarsfrågor och är en anledning till att EU:s regelverk om produktansvar nu ses över. Det handlar bland annat om att klargöra hur produktansvaret ska tillämpas när digitala inslag förekommer som en del i produkter, till exempel digitala tjänster. EU-kommissionen har också lagt fram ett förslag om bevisning som ska underlätta för skadelidande i situationer när AI-system orsakar skador.

Att tillgång till data har blivit allt viktigare har bidragit till att EU-kommissionen eftersträvar en gemensam marknad även för data. Den ambitionen har resulterat i flera förslag i syfte att underlätta möjligheterna att dela sina data med tredje part. På finansområdet handlar det till ett exempel om kommissionens förslag till förordning om en ram för åtkomst till finansdata. Det väntas få stor betydelse för sektorn. Förslaget behandlas närmare i avsnitt 2.1.

Digitaliseringen har gett utökade möjligheterna till analys och beslutsstöd med verktyg som AI. I detta ligger stora möjligheter. Fel eller missbruk vid AI-användning kan emellertid medföra risker för bland annat säkerhet och grundläggande rättigheter. Ur ett regleringsperspektiv uppkommer frågor om hur riskerna ska hanteras och hur skyldigheter ska fördelas mellan olika aktörer. Inom EU förhandlas sedan en tid tillbaka en horisontell rättsakt om utveckling och användning av AI i skilda verksamheter, inklusive försäkringsverksamhet. Förslaget behandlas närmare i avsnitt 2.2.

Digitaliseringen har också inneburit att samhällslivet blivit alltmer beroende av digital teknologi. Med detta följer en ökad sårbarhet för cyberangrepp och andra it-

relaterade risker och ett behov av att hantera dessa risker. Detta gäller inte minst i finanssektorn. Mot den bakgrunden har en EU-förordning, förordningen om digital operativ motståndskraft för finanssektorn (DORA-förordningen), nyligen antagits.⁴⁰ Den omfattar bland annat försäkringsverksamhet. Förordningen behandlas närmare i avsnitt 2.3.

Horisontell reglering innebär utmaningar för lagstiftaren och tillämparna

Den digitala tekniken är gränsöverskridande på så sätt att den sällan är knuten till någon viss bransch eller marknad. I digitala frågor är regleringen därför i regel inte specifik för försäkrings- och tjänstepensionsverksamhet utan sektorövergripande som rättsakten om AI, eller sektorgemensam för finansiella tjänster, som förslaget till förordning om en ram för åtkomst till finansdata och DORA-förordningen. Det finns flera utmaningar med sådan horisontell reglering.

En grundläggande utmaning är att horisontell reglering sällan anpassas efter de specifika förhållanden som gäller för försäkrings- och tjänstepensionsverksamhet. I sektorgemensam reglering finns risk för att reglering utformas med till exempel bankverksamhet som utgångspunkt och inte fullt ut tar hänsyn till viktiga särdrag i till exempel försäkringsverksamhet. När det till exempel gäller datadelning finns redan viss tvingande reglering för banker, men inte för försäkringsgivare. Samtidigt finns det avgörande skillnader mellan den data som den aktuella bankregleringen avser (betalkontoinformation) och den bredd av data som försäkrings- och tjänstepensionsföretag hanterar i sin verksamhet.

I sektorövergripande reglering kan det vara svårt för lagstiftaren – och för all del även för branschen – att tidigt identifiera de aspekter som rör försäkrings- och tjänstepensionsverksamhet i olika regleringsprocesser. Om det sker i ett sent skede av dessa processer minskar utsikterna för att sådana aspekter kommer att beaktas.

Även om försäkrings- och tjänstepensionsfrågor identifieras i tid kan det vara en utmaning att få gehör för dessa perspektiv. Ansvar för att ta fram lagförslag om digitala frågor kan mycket väl ligga hos en del i lagstiftarens organisation som annars inte hanterar försäkringsfrågor och som inte har någon erfarenhet av att hantera dessa. I EU-kommissionen har generaldirektoratet för Kommunikationsnät, innehåll och teknik ("DG Connect") ansvaret för digitaliseringspolitiken, inklusive rättsakten om AI. I Regeringskansliet har det dåvarande Infrastrukturdepartementet tidigare haft ansvar för EU-förhandlingarna om AI-rättsakten. I sektorövergripande reglering kan följderna i värsta fall bli att försäkrings- och tjänstepensionsperspektiv förloras helt.

Ansvar för att även branschens perspektiv uppmärksammas och beaktas i regleringsprocesserna vilar på såväl lagstiftaren som branschen. För att uppnå ett slutresultat i form av välavvägd ny lagstiftning är det viktigt att regleringsförslag arbetas fram genom samråd mellan samtliga berörda ansvarsområden inom EU-kommissionen och/eller Regeringskansliet. Och det är inte minst viktigt när det gäller horisontell reglering att lagstiftaren redovisar fullgoda konsekvensbeskrivningar av sina förslag, i syfte att försäkra sig om att en åtgärd som övervägs verkligen behövs för samtliga berörda aktörer, att den löser det aktuella problemet

⁴⁰ Europaparlamentets och rådets förordning (EU) 2022/2554.

samt att ge ett allsidigt underlag för bedömningen av de konsekvenser som åtgärden kan medföra. Hela regleringsprocessen måste också kännetecknas av öppenhet så att försäkringsbranschen och andra intressenter har reell möjlighet att vara delaktiga genom synpunkter och andra inspel.

Liknande svårigheter kan uppkomma även i tillsynsmyndigheternas arbete. Enligt förslaget till AI-rättsakt ska till exempel en nationell tillsynsmyndighet utses i medlemsstaterna och ett nytt organ för efterlevnad och samarbete inrättas på EU-nivå, den Europeiska nämnden för AI. Det är knappast troligt att detta organ kommer att ha någon större erfarenhet av försäkringsfrågor. Sådana aktörer kan på grund av sitt uppdrag också ha svårt att fullt ut beakta intressen som de inte har till uppgift att vaka över. EU:s finanstillsynsmyndigheter har olika verksamhetsområden och deras perspektiv kan därför skilja sig åt. Dessa myndigheter bemyndigas ofta att komplettera sektorregleringen på lägre nivå. Viktiga bemyndiganden av detta slag finns till exempel i DORA-förordningen. I sådana sammanhang är det angeläget att den Europeiska försäkrings- och tjänstepensionsmyndigheten (EIOPA) deltar och kan bidra med försäkringserfarenhet.

En annan grundläggande utmaning är att horisontell reglering kan ge upphov till överlappningar med andra regelverk. Det handlar inte enbart om duplicering av krav utan också om att regelverk skärs på flera led. Rörelseregelverket solvens II respektive DORA-förordningen innehåller till exempel regler båda om hantering av it-relaterade risker och om utkontraktering, även om deras respektive tillämpningsområden inte helt sammanfaller. I både den allmänna dataskyddsförordningen (GDPR), som avser behandling av personuppgifter, och förslaget till förordning om en ram för åtkomst till finansdata, som gäller delning av kunddata, finns en rätt för den berörde att få ut sina data och använda dem på annat håll. Tillämpningsområdet och rättighetens utformning är dock inte identiska. Att flera regelverk kan gälla i samma situation komplicerar tillämpningen och anpassningen.

I det följande behandlas tre rättsakter av betydelse för försäkringsbranschen som belyser utmaningarna med horisontell reglering, nämligen förordningsförslaget om en ram för åtkomst till finansdata (FIDA), förordningsförslaget om harmoniserade regler för AI samt DORA-förordningen.

2.2 Regelverk om datadelning

Tillgång till data har blivit en allt viktigare resurs

Mängden data ökar samtidigt som förutsättningarna för att samla in och analysera stora mängder data har utvecklats. Data genereras inte bara i samband med mänskliga aktiviteter som till exempel vid telefonsamtal och betalningar utan också av saker och sensorer, till exempel i trafiken eller i industriella processer. Med hjälp av algoritmer och andra verktyg för dataanalys kan bättre förutsägelser göras och nya mönster hittas. Data kan också användas för att träna algoritmer och behövs alltså för att fullt ut utnyttja potentialen med AI. Tillgång till data har mot den bakgrunden blivit en allt viktigare resurs i de flesta verksamheter, inklusive försäkringsbranschen.

När man talar om datadriven innovation på finansområdet, det vill säga att företag använder data och dataanalys för att utveckla nya produkter och tjänster, är det främst kunddata och öppna finansiella tjänster som har stått i fokus. Öppna finansiella tjänster handlar om att dela och återanvända kundinformation och innebär att kunder ger tredjepartsleverantörer tillgång till kunddata för att olika typer av finansiella tjänster ska kunna erbjudas.⁴¹

Utökad datadelning kan medföra nya möjligheter för konsumenter. Finansinspektionen nämner i en rapport bland annat mer individanpassade tjänster och produkter och att konsumenter får större möjligheter att jämföra produkter med varandra.⁴² Med utökade möjligheter till en samlad bild av konsumentens finansiella situation skapas enligt rapporten också bättre försättningar för rådgivning. I detta ligger möjligheter också för försäkringsbranschen, som vill ha trygga och nöjda kunder.

Diskussionen om öppna finansiella tjänster har ursprungligen haft fokus på bankerna. EU:s andra betaltjänstdirektiv (PSD2) innebär att banker är skyldiga att tillgängliggöra delar av den information de har om sina kunder till leverantörer av betalningsinitieringstjänster och kontoinformationstjänster.⁴³ Till skillnad från bankområdet har det på försäkringsområdet hittills inte funnits några särskilda regler om datadelning.⁴⁴ På försäkringsområdet har datadelning alltså skett genom oreglerade metoder, till exempel på frivillig grund.

Faktaruta: Hur ser datadelningen ut i branschen i dag?

Finansinspektionen har i en rapport kartlagt användningen av öppna finansiella tjänster i bland annat försäkringsbranschen.⁴⁵ Enligt rapporten ökar användningen i branschen, men från låga nivåer. Vidare görs bedömningen att tjänsterna används brett inom försäkring. Av en genomförd enkät framgår bland annat följande:

- 42 procent av försäkringsföretagen uppger att olika aktörer hämtat data från dem via oreglerade metoder
- 14 procent, av försäkringsföretagen uppger att de själva nyttjar öppna finansiella tjänster för datainhämtning.
- 61 procent av försäkringsföretagen uppger att användningen av öppna finansiella tjänster ökar.

Svaren får läsas mot bakgrund av att det i rapporten konstateras att det för närvarande inte finns några reglerade inhämtningsmetoder i branschen utan att tredjepartsleverantörerna använder oreglerade metoder.⁴⁶

⁴¹ Finansinspektionen, *Användningen av öppna finansiella tjänster i Sverige*, Dnr 23-3846.

⁴² Ibid.

⁴³ Europaparlamentets och rådets direktiv (EU) 2015/2366.

⁴⁴ I den allmänna dataskyddsförordningen (GDPR), som är generellt tillämplig, finns en rätt till dataportabilitet som innebär att den som har lämnat sina personuppgifter i vissa fall rätt har rätt att få ut och använda uppgifterna på annat håll.

⁴⁵ Finansinspektionen, *Användningen av öppna finansiella tjänster i Sverige*, Dnr 23-3846.

⁴⁶ I rapporten nämns skärmskrapning eller så kallad reverse engineering som exempel på oreglerade metoder, ibid.

Nya regler för delning av finansdata

Förutsättningar för datadelning på försäkringsområdet står i begrepp att förändras i viktiga delar. I juni 2023 lade EU-kommissionen fram ett förslag till förordning om en ram för åtkomst till finansdata ("FIDA", regulation on a framework for Financial Data Access).⁴⁷ I likhet med PSD2 handlar förslaget om delning av kunddata. Förslaget gäller dock hela finansområdet, inklusive försäkring och tjänstepension, och har även i övrigt ett mycket bredare tillämpningsområde än PSD2.

Det är viktigt att en sektorgemensam reglering tar hänsyn till de skillnader som finns mellan till exempel banker och försäkringsgivare. Vid jämförelse dem emellan har det påpekats att det finns ett stort antal olika försäkrings- och pensionsprodukter, att försäkringsgivare ofta har stora mängder data och data som har bearbetas, att det är fråga om data av vitt skilda slag samt att försäkringsdata kan innefatta mycket integritetskänsliga uppgifter om till exempel hälsa.⁴⁸ Det har också framhållits att kunder interagerar mindre ofta med försäkringsgivare än med till exempel banker. Det bör också understrykas att försäkringsgivare har ett stort intresse av andra data än kunddata.

Datadelning aktualiserar i sig också en rad komplexa frågor. Det är talande att meningarna går isär bland de intressenter som har yttrat sig under den konsultationsprocess som föregått förslaget.⁴⁹ Ur kundens perspektiv handlar det till exempel om kontroll över hanteringen av data samt frågor om integritet och säkerhet. För de aktörer som direkt deltar i datadelningen är det grundläggande om det ska finnas en skyldighet att tillgängliggöra data eller om den ska ske på frivillig basis. En annan central fråga är vilka data som ska omfattas. Det kan till exempel handla om att göra skillnad på data med olika integritetskänslighet eller mellan rådata och data som datainnehavaren har bearbetat. Av betydelse är också hur kostnader för delningen ska fördelas. Vem som ska få tillgång till data och på vilka villkor är inte enbart grundläggande förutsättningar för datadelning utan kan också ha betydelse för konkurrensen på en marknad. Ur ett praktiskt perspektiv hör också interoperabilitet till de centrala frågorna. Interoperabilitet är förmågan hos olika system att fungera och kommunicera med varandra. Man behöver använda gemensamma standarder, till exempel för data och tekniska gränssnitt.

Datadelning kan ha positiva konsekvenser för såväl försäkrings- och tjänstepensionsföretag som deras kunder. Om det blir så beror i slutändan i stor uträkning på hur reglerna utformas. Branschen har därför anledning att noga följa de förhandlingar på EU-nivå som påbörjats.

⁴⁷ COM(2023) final 360 av den 28 juni 2023.

⁴⁸ Standaert, W och Muylle, S, (2022) *Framework for open insurance strategy: insights from a European study*, Geneva Papers on Risk and Insurance – Issues and Practise; EIOPA (2023), *Discussion Paper on Open Insurance: an explanatory use case in the insurance sector*, EIOPA-Bos-23-211.

⁴⁹ COM(2023) final 360 av den 28 juni 2023.

Finanssektorns regler en del i en gemensam marknad för data

I ett bredare perspektiv har förordningsförslaget FIDA sin bakgrund i EU-kommissionens datastrategi från 2020.⁵⁰ Strategin syftar till att skapa en gemensam marknad för data. Flera rättsakter har tagits fram inom ramen för strategin. En av dessa är *dataakten*.⁵¹ Förordningen innehåller harmoniserade regler om tillgång till och användning av data från bland annat uppkopplade produkter, så kallade sakernas internet. Förordningen ger användare större kontroll över data från deras användning av sådana produkter. På användarens begäran ska datainnehavaren till exempel göra sådana data tillgängliga för tredje man. Det finns också regler som tar sikte på förhållandet mellan datainnehavaren och tredje man i sådana fall. Det handlar till exempel om att säkerställa att oskäligen avtalsvillkor inte används och om rimlig ersättningsnivå. Försäkringsbranschen har stort intresse av tillgång till data från sakernas internet, till exempel från uppkopplade produkter i bilar. EU-förhandlingarna om förordningen är i praktiken avslutade och ett formellt antagande väntas inom kort.

Datarättsförordningen är sektorövergripande. Den är en del av den rättsliga ramen för att utveckla *gemensamma dataområden* inom vissa strategiska sektorer. I sin strategi för digitalisering av finanssektorn i EU utvecklar EU-kommissionen datastrategins tankar på att skapa ett gemensamt dataområde på finansområdet.⁵² Förslaget till förordning om en ram för åtkomst till finansdata är en del i detta arbete.

Vad innebär FIDA?

Förslaget till förordning om en ram för åtkomst till finansdata innehåller regler om tillgång till, delning och användning av kunddata hos finansiella företag. Avsikten är bland annat att kunderna ska ges större kontroll över sina data och bereda tredjepartsanvändare tillgång till data så att kunderna till exempel kan dra nytta av innovativa produkter. Ett led i detta är också att underlätta standardisering i samband med datadelning.

Förordningen är tillämplig på en rad finansiella företag som bedriver tillståndspliktig verksamhet. Dit hör till exempel banker, försäkrings- och tjänstepensionsföretag samt försäkringsförmedlare.

Förslaget innebär – enkelt uttryckt – att kunden får en rätt att få ut sina data och använda dem på annat håll. De finansiella företagen är enligt förslaget alltså skyldiga att tillgängliggöra data för kunden eller att dela data med användare, om kunden begär det. Ur användarens synvinkel handlar det om en praktiskt betydelsefull möjlighet att – med kundens medgivande – få del av dennes data. I förslaget finns också bestämmelser som ska ge kunden kontroll över användningen. Användare får till exempel bara använda data för ändamål som kunden har samtyckt till, och ett lämnat samtycke kan dras tillbaka.⁵³ Kunderna ska också få tillgång till

⁵⁰ COM(2020) final 66 av den 19 februari 2020.

⁵¹ COM(2022) final 68 av den 23 februari 2022.

⁵² COM(2020) 591 final av den 26 oktober 2020.

⁵³ COM(2023) 360 final av den 28 juni 2023.

”manöverpaneler” i användargränssnittet. De ska ge överblick över lämnade samtycken och göra det praktiskt möjligt att hantera dessa.⁵⁴

Finansiella företag har dubbla roller enligt förslaget. De kan i egenskap av data-innehavare vara skyldiga att tillhandahålla data men de kan också ta emot data i egenskap av användare. Även andra företag än finansiella företag kan bli användare enligt förslaget. De måste då ansöka om tillstånd och uppfylla vissa verksamhetskrav. Det handlar till exempel om att uppfylla vissa it-säkerhetskrav som gäller även för finansiella företag.⁵⁵ Till skillnad från finansiella företag har dessa företag emellertid inte någon skyldighet att dela data med andra.

Förordningen omfattar en rad olika kategorier av kunddata hos de finansiella företagen. På försäkrings- och tjänstepensionsområdet omfattas bland annat vissa kunddata som rör pension och annat försäkringssparande samt sakförsäkring.⁵⁶ Med hänvisning till risken för finansiellt utanförskap har en del försäkringsdata undantagits. Dit hör bland annat andra livförsäkringsprodukter än försäkringsbaserade investeringsprodukter samt sjukförsäkring (sickness and health insurance). Detta motiveras bland annat av risker i samband med prissättning och riskbedömning.⁵⁷ Med kunddata avses inte enbart data som kunden själv har tillhandahållit. Även data som genereras i samband med kundens interaktion med företaget kan omfattas.

All datadelning enligt förslaget ska, som utgångspunkt, ske inom ramen för datadelningssystem. Att bilda dessa är en viktig del av förslaget. Användare och data-innehavare ska enligt förslaget ansluta sig till ett eller flera datadelningssystem.⁵⁸ Där ska ett antal svåra och praktiskt viktiga frågor lösas.⁵⁹ Det handlar till exempel om gemensamma standarder som behövs vid datadelningen, ersättning till data-innehavare vid delning med användare, ansvar till exempel då data är felaktiga eller bristfälliga samt tvistelösning. Datainnehavare kan få ersättning för datadelning endast om delningen har skett inom ramen för ett datadelningssystem.⁶⁰ I det ligger alltså ett starkt incitament att ansluta sig. Om datadelningssystem inte bildas på något eller några områden kan EU-kommissionen i stället anta reglering i aktuella delar.⁶¹

Konkurrens på lika villkor viktigt för branschen...

Data har – som nämnts ovan – blivit en alltmer strategisk resurs. En grundläggande utgångspunkt för tvingande regler om datadelning bör vara att de säkerställer *konkurrens på lika villkor*. Försäkringsbranschen har uppmärksammat frågan bland annat när det gäller tillgången till data, kostnadsfördelningen och skyddet av affärskänslig information.

⁵⁴ Ibid.

⁵⁵ Ibid.

⁵⁶ Ibid

⁵⁷ Ibid

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ Ibid.

⁶¹ Ibid.

Förslaget till förordning om en ram för åtkomst till finansdata är ett gemensamt regelverk för finanssektorn. När det gäller datadelning bygger förslaget i denna del på ömsesidighet. De finansiella företagen är skyldiga att dela data, men har också möjlighet att få del av data. Som framgått ovan innebär förslaget att även aktörer utanför finanssektorn kan delta i datadelningen. I denna del gäller dock inte någon ömsesidighet. Aktörerna utanför finanssektorn har möjlighet att ta del av data, men är inte skyldiga att dela enligt förslaget. Även mycket stora företag med stort marknadsinflytande kan dra ensidig fördel av förslagets regler. Några begränsningar finns inte dessa avseenden.

Kostnadsfördelningen mellan dataanvändare och datainnehavare är en annan fråga av betydelse för konkurrens på lika villkor. Datainnehavaren står för den större delen av kostnaden för datadelning och bör ha en möjlighet att kompensera sig i rimlig omfattning.⁶² Att dela data är förenat med kostnader. Det kan handla om kostnader för att producera data, till exempel att samla in, standardisera och kvalitetssäkra data, samt kostnader för delningen, till exempel att tillhandahålla nödvändig infrastruktur.⁶³ I förslaget ställs krav på datainnehavarens infrastruktur till exempel när det gäller säkerhet, standarder och information till kunden.⁶⁴ Om datainnehavaren inte kan få rimlig kostnadstäckning finns det risk att regleringen genererar kostnader utan tillräcklig efterfrågan och kundnytta.

Kostnadsfördelningen har också betydelse för fortsatt innovation. Att dela data kan å ena sidan bidra till innovation och ett bättre utbud av produkter och tjänster. Om all data görs fritt tillgänglig för alla finns å andra sidan inte längre tillräckliga incitament för att producera och förädla data. I förlängningen kan det påverka innovation negativt. Av samma skäl bör datainnehavare inte tvingas dela affärskänslig information.

När det gäller affärskänslig information handlar det om att säkerställa ett fortsatt skydd för företagshemligheter, men också om vilka data som ska delas. Försäkringsbranschen är en dataintensiv bransch där data samlas in och bearbetas som en del i verksamheten. Bearbetad data har en annan affärskänslighet än rådata. Denna skillnad bör återspeglas i förslaget, som inte är entydigt i detta avseende.⁶⁵ Ibland görs åtskillnad mellan data som tillhandahållits av kunden, såsom en adressuppgift, observationsdata, såsom kundens sökhistorik på en webbsida, och data som är resultat av bearbetning, till exempel en riskprofil.⁶⁶ Att data som direkt eller indirekt har en tydlig koppling till kunden ska kunna bli föremål för delning är lättare att förstå än att data ska omfattas som har omvandlats genom bearbetning, ibland tillsammans med annan data.

...liksom tillgång till data utanför finanssektorn

Avslutningsvis bör också betydelsen av sektorövergripande datadelning understrykas. Förordningsförslaget fokuserar på delning av finansdata. Det är dock inte

⁶² Bestämmelser om ersättning finns i *ibid*.

⁶³ Expert Group on European Financial Data Space (2022), *Report on Open Finance*.

⁶⁴ COM(2023) 360 final av den 28 juni 2023.

⁶⁵ Förslaget omfattar bland annat data som genereras i samband med kundens interaktion med företaget.

⁶⁶ OECD(2018), *Personalised Pricing in the Digital Era*.

enbart delning av data inom detta område som kan bidra till innovation och konsumentnytta. Det gör även sektorövergripande datadelning. Försäkringsbranschen, som hanterar risker i nästan alla delar av samhället, har ett särskilt intresse av tillgång till data från olika sektorer. Dataakten öppnar möjligheter till exempel när det gäller tillgång till data från användningen av uppkopplade produkter. I ett längre perspektiv är det också viktigt för branschen att säkerställa tillgång till data från andra samhällsområden, som till exempel hållbarhetsdata.

2.3 Regelverk om AI

AI innebär möjligheter för försäkringsbranschen

Dataanalys har alltid varit central i försäkringsbranschen. Den används till exempel för att bedöma och prissätta risker. Rent praktiskt kan det handla om att aktuarier tillämpar olika slags matematiska modeller på försäkringsdata. Med ny teknik följer andra möjligheter att bearbeta data än tidigare. Inom försäkringsområdet används redan i dag avancerade tillämpningar av teknik för dataanalys och AI i tjänster för bland annat kunddialoger, riskberäkningar, skadeförebyggande åtgärder och bedrägeriprevention. För försäkringsbranschen innebär AI – liksom på många andra områden – möjligheter att utveckla och förbättra verksamheten.

Faktaruta: Vad kan bättre analysmöjligheter vid riskbedömning innebära?

Tillgång till data från olika källor och analysverktyg som AI kan ge bättre analysmöjligheter än tidigare vid riskbedömning. Till de möjliga fördelar som har uppmärksamats hör att de faktiska riskerna bättre kan återspeglas i premierna.⁶⁷ Detta kan ge incitament för att begränsa risker och att vidta skadeförebyggande åtgärder när så är möjligt. Vidare kan en högre grad av automatisering av riskbedömningen bidra till sänkta kostnader. En bättre riskbedömning kan även leda till att försäkringsskydd kan erbjudas i situationer där detta inte tidigare varit möjligt på grund av stor osäkerhet eller höga risker.

Riskbedömningen ska givetvis vara korrekt och saklig även när den sker med hjälp av till exempel AI-verktyg. I detta ligger att data och analysverktyg inte får ge upphov till diskriminering eller på annat sätt snedvrیدا resultatet. En mera förfinad riskbedömning kan ge förutsättningar för större premiedifferentiering. Att individer med olika risk behandlas olika vid premiesättning är dock inte detsamma som diskriminering. Privat försäkring bygger på att den premie som en kund betalar ska täcka den risk som individen tillför kollektivet. En ökad individualisering kan dock vara negativt för den enskilde om den leder till svårigheter att få försäkringsskydd till rimlig kostnad. Hantering av stora mängder data ger också upphov till integritetsfrågor. Tillgång till data om försäkringstagarens beteende genom

⁶⁷ I det följande jfr bland annat Geneva Association(2018), Big Data and Insurance: Implications for Innovation, Competition and Privacy och Geneva Association (2022), Responsible Use of Data in the Digital Age, 2022 och Geneva Association (2023), Regulation of Artificial Intelligence in Insurance: Balancing consumer protection and innovation.

sensorer kan till exempel ge nya möjlighet att begränsa risker och arbeta förebyggande, men behöver också vägas mot integritetsintresset.

Det finns risker med AI, men regleringsbehovet ser olika ut

Att AI innebär möjligheter för enskilda, näringslivet och samhället i stort är något som har uppmärksammats i många sammanhang. Samtidigt finns det risker med användning av AI. Till de risker som uppmärksammats hör säkerhetsrisker vid användning av AI-system och negativ påverkan på grundläggande rättigheter.

Ur ett rättighetsperspektiv kan till exempel frågor om diskriminering, insyn och transparens samt ansvarsfördelning uppkomma. Detta har bland annat sin bakgrund i att resultaten som AI producerar är beroende av AI-systemets utformning och vilka data som används. Fel i data och algoritmer kan snedvrیدا resultaten. Snedvrیدna resultat kan vara svåra att upptäcka. För en utomstående kan det till exempel vara svårt att förstå vad en algoritm tar hänsyn till eller vilka data som används ("black box AI"). AI och speciellt maskininläring kan användas för att fatta beslut som är viktiga för den enskilde. Om det förekommer snedvrیدning i data och algoritmer kan detta leda till så kallad algoritmisk diskriminering. Vid maskininläring kan till exempel brister i träningsdata leda till ojämlika beslut.

Det är tveklöst så att användning av AI föranleder angelägna överväganden och regleringsbehov i olika avseenden. På vissa områden finns dock redan reglering som hanterar AI-relaterade risker. Den allmänna dataskyddsförordningen (GDPR), som rör hantering av personuppgifter, innehåller till exempel en rätt att i vissa fall motsätta sig automatiserat beslutsfattande.⁶⁸ Det kan, som för försäkringsbranschens del, också finnas sektorreglering att ta hänsyn till.

Vad innebär förslaget om ett gemensamt regelverk för AI?

EU-kommissionen lade i april 2021 fram ett förslag till förordning med EU-gemensamma regler om AI.⁶⁹ Förslaget avser bland annat att säkerställa att AI-system är säkra och att de utvecklas och används i enlighet med grundläggande rättigheter. Förordningsförslaget är horisontellt och gäller AI-system i vitt skilda verksamheter, inklusive försäkrings- och tjänstepensionsverksamhet. Förslaget ålägger leverantörer och användare av AI-system skyldigheter utifrån ett riskbaserat förhållningssätt. Leverantörer (som kan inkludera utveckling för egen användning) har längre gående skyldigheter än användare.

Användning av AI delas in i olika kategorier av risk. I vissa fall anses risken oacceptabel och användningen förbjuds. Det handlar om olika typer av manipulation, social poängsättning samt ansiktsigenkänning och annan biometrisk identifiering.

Om risken är hög får AI-systemet användas endast om det genomgått en granskningsprocess som har likheter med EU:s produktsäkerhetslagstiftning. Det ställs till exempel krav på transparens, spårbarhet och kvaliteten på de data som

⁶⁸ Europaparlamentets och rådets förordning (EU) 2016/679.

⁶⁹ COM(2021) 206 final av den 21 april 2021.

används. Kravet på datakvalitet avser bland annat att undvika diskriminering vid maskininlärning.⁷⁰

Vad är då hög risk? Ett antal AI-system definieras som högrisksystem i en bilaga till förordningsförslaget. Till de aktuella användningsområdena hör tillgång till grundläggande privata och offentliga tjänster, som till exempel kreditvärdering. I EU-kommissionens förslag fanns inte några försäkringstjänster med. Under förhandlingarna i ministerrådet och Europaparlamentet har emellertid liv- och sjukförsäkring (life and health insurance) lagts till. I rådtexten tar skrivningarna sikte på AI-system för riskbedömning och prissättning för sådana försäkringar. Avsikten är att bilagan ska kunna uppdateras även efter det att förordningen har antagits.

EU-kommissionens förslag har förhandlats i ministerrådet och i Europaparlamentet som båda har antagit sina förhandlingspositioner. Triloger påbörjades under sommaren 2023 och väntas pågå i vart fall fram till årsskiftet.

Försäkringsregleringen tar hand om AI-relaterade risker

Försäkringsbranschen har framhållit att försäkring inte bör klassificeras som hög risk av flera skäl. Till att börja med omfattas försäkringsgivarna redan av en robust sektorspecifik reglering som innefattar tillsyn. Denna ordning har till syfte att – tillsammans med reglering som den allmänna dataskyddsförordningen (GDPR) – ta hand om riskerna i förekommande fall. Relevant försäkringsreglering finns till exempel i rörelseregelverket solvens II, som innehåller bestämmelser om styrning, riskhantering och intern kontroll, och försäkringsdistributionsregelverket, som innehåller uppföranderegler om till exempel interna processer för produktgodkännande och transparens. Finanstillsynsmyndigheterna är också särskilt lämpade att förstå och följa upp riskerna i sektorn. De har en annan förståelse för särdragen på området än en myndighet som har ett allmänt tillsynsuppdrag. I försäkringsverksamhet deltar till exempel en särskild yrkesgrupp – aktuarier – i riskbedömning och prissättning.

För försäkringsverksamhet gäller också vissa grundläggande förutsättningar. För att kunna erbjuda försäkringsskydd till rimliga kostnader måste till exempel risker kunna bedömas och prissättas korrekt. Det är inte säkert att den Europeiska nämnden för AI, det EU-organ som enligt förslaget ska skapas för efterlevnad och samarbete, kommer att ha sådana perspektiv. När det gäller tillsynen ska som utgångspunkt *en* nationell tillsynsmyndighet utses men en eller flera nationella myndigheter kan få tillsynsuppgifter enligt förslaget.⁷¹ På det finansiella området är utgångspunkten att den myndighet som har hand om den finansiella tillsynen ska få sådana uppgifter på sitt område.⁷²

EIOPA har i ett brev till ministerrådet och Europaparlamentet gett uttryck för att försäkring inte bör anses vara hög risk för närvarande.⁷³ I anslutning till detta har

⁷⁰ Ibid.

⁷¹ Ibid.

⁷² Ibid.

⁷³ EIOPA (2022) *Letter to co-legislators on the Artificial Intelligence Act*, EIOPA-BoS-22/632.

myndigheten understrukt vikten av att undvika överlappande reglering och utmaningarna ur ett tillsynsperspektiv.

Även om det i dag inte är möjligt att i alla delar förutse hur användningen av AI kommer att utvecklas är det ändå tydligt att den befintliga regleringen bäst tar hand om de AI-relaterade riskerna på försäkrings- och tjänstepensionsområdet.

En annan fråga av intresse för branschen är vilka AI-system som ska omfattas av förordningen. EU-kommissionens ursprungliga förslag innehåller en bred definition som utöver metoder för maskininlärning också kan inkludera statistiska och logiska metoder.⁷⁴ En farhåga är att definitionen skulle kunna omfatta sådant som enklare datorprogram samt traditionella matematiska modeller. Ett exempel kan vara interna modeller som används i företagsstyrningen och för att beräkna kapitalkrav i försäkringsverksamhet. Dessa modeller är till sin natur knappast något som medför risker när det gäller diskriminering eller grundläggande rättigheter och de granskas dessutom av tillsynsmyndigheterna. Branschen har därför önskat en snävare definition som fokuserar på maskininlärningsaspekter av AI.

2.4 Regelverk om it-säkerhet

Digitalisering och operativ motståndskraft hör ihop

De finansiella företagens förmåga att hantera, förhindra och förebygga cyberangrepp och andra it-relaterade störningar har blivit allt viktigare i reglering och tillsyn. Förordningen om digital operativ motståndskraft för finanssektorn (DORA-förordningen) antogs i december 2022 och ska tillämpas från mitten av januari 2025.⁷⁵ De europeiska finanstillsynsmyndigheterna arbetar för närvarande med att ta fram kompletterande reglering i form av tekniska standarder. Att DORA är en förordning innebär att den blir direkt tillämplig i svensk rätt.

Förordningen har sin bakgrund i behovet av att hantera de risker som uppkommer till följd av en alltmer digitaliserad finanssektor. Att den finansiella sektorns beroende av digital teknologi och teknikföretagens tjänster har tilltagit innebär en ökad sårbarhet för cyberangrepp och andra it-relaterade risker. Samtidigt har riskerna också ökat bland annat till följd av det försämrade säkerhetspolitiska läget.⁷⁶

Vad innebär DORA?

DORA-förordningen avser att stärka den operativa motståndskraften mot cyberangrepp och andra it-relaterade störningar i finanssektorn genom att skapa en harmoniserad och heltäckande reglering på området. Störningarna kan vara både avsiktliga och oavsiktliga. Förordningen tillämpas på ett stort antal finansiella företag däribland försäkringsföretag, tjänstepensionsföretag och försäkringsförmedlare. Förordningen innehåller bestämmelser om styrning och riskhantering, incidentrapportering, testning av it-säkerhet, tredjepartsrisker och informations-

⁷⁴ COM(2021) 206 final av den 21 april 2021.

⁷⁵ Europaparlamentets och rådets förordning (EU) 2022/2554.

⁷⁶ Finansinspektionen (2022) *Förstärkt digital motståndskraft hos företag i den finansiella sektorn*, Dnr 22-10015.

delning. Det betyder att förordningen griper in både i det förebyggande arbetet och när incidenter ska hanteras.

När det gäller styrning och riskhantering finns bestämmelser som tydliggör ledningens ansvar för de aktuella riskerna. Det ställs också krav på att ta fram ett riskramverk. Det handlar bland annat om åtgärder som stärker förmågan att identifiera, förebygga, upptäcka och åtgärda it-risker. När det gäller rapportering ska det finnas processer för att hantera incidenter. Allvarliga incidenter ska rapporteras till tillsynsmyndigheten inom viss tid. Det ställs vidare krav på att alla finansiella företag ska testa den digitala operativa motståndskraften. Vissa företag ska också utföra avancerade penetrationstester, det vill säga tester som simulerar ett cyberangrepp på organisationen. När det gäller tredjepartsrisker ställs det bland annat krav på en strategi för sådana risker och på åtgärder inför ingående av avtal med tredjepartsleverantörer. Det ställs också krav på innehållet i sådana avtal och på att kunna avsluta dem i vissa fall.

Mera detaljerade regler när vi går från solvens II till DORA

Reglering av detta slag är inte något helt nytt för försäkringsbranschen. I rörelse-regelverket solvens II finns till exempel grundläggande regler om hantering av risker samt regler om utkontraktering. I den pågående översynen av solvens II förtydligas att riskhanteringssystemet också ska omfatta cybersäkerhet. Dessa regler kompletteras av riktlinjer från EIOPA.⁷⁷ DORA innehåller emellertid en mycket mera omfattande och detaljerad reglering om digital motståndskraft. En annan skillnad är att DORA är tillämplig på andra företag än finansiella företag, nämligen leverantörer av digitala tjänster och datatjänster till den finansiella sektorn. Det kan till exempel handla om molntjänster, programvara och data-analystjänster.⁷⁸ Bakgrunden är att finansiella företag i allt större utsträckning lägger ut it-relaterad verksamhet. Detta kan ge upphov till risker, inte minst om det är kritisk verksamhet som tillhandahålls av endast ett fåtal leverantörer. Förordningen innebär att de europeiska finanstillsynsmyndigheterna ska utöva tillsyn över tredjepartsleverantörer om de bedöms som kritiska.

Som skäl för att den finansiella sektorn bör ha gemensam reglering på detta område har bland annat anförts att it-relaterade risker kan vara sammanlänkade. Om många finansiella företag använder samma leverantör kan risken öka. Man talar då om koncentrationsrisker. En sådan risk kan vara svår för ett enskilt företag att identifiera eftersom ett enskilt företag normalt inte har någon samlad bild av leverantörens avtal med andra. Gemensamma regler och tillsyn över tredjepartsleverantörer kan vara en fördel även av andra skäl. Tredjepartsleverantörer som till exempel molntjänstleverantörer är inte sällan stora företag med global verksamhet och stor förhandlingsstyrka. Med sådana motparter kan det vara en utmaning att driva igenom krav som rör hanteringen tredjepartsrisker till exempel när det gäller avtalsinnehåll.

⁷⁷ Se EIOPA (2020), *Guidelines on information and communication technology security and governance*, EIOPA-BoS-20/600 och EIOPA(2020), *Guidelines on outsourcing to cloud service providers*, EIOPA-BoS-20-002.

⁷⁸ Europaparlamentets och rådets förordning (EU) 2022/2554.

Hur blir det med proportionaliteten i ett gemensamt regelverk?

Att DORA är ett gemensamt regelverk för hela finanssektorn innebär att förordningen är tillämplig på företag av olika storlek och verksamhet och med olika exponering för it-relaterade risker. För försäkrings- och tjänstepensionsföretag kan det förstås vara en nackdel att reglerna inte har utformats specifikt för förhållande på försäkrings- och tjänstepensionsområdet. För branschen är det därför viktigt att det ska vara möjligt att tillämpa regelverket proportionellt. Detta har i viss mån gjorts möjligt. Till att börja med undantar förordningen vissa mindre försäkrings- och tjänstepensionsföretag och försäkringsförmedlare från tillämpningsområdet.⁷⁹ Vidare finns i vissa fall lättnader för mindre aktörer som till exempel små tjänstepensionsföretag.⁸⁰ Förordningen innehåller slutligen en övergripande princip om proportionell tillämpning.⁸¹

Bland dessa åtgärder torde proportionalitetsprincipen ha störst praktisk betydelse. De anpassningsmöjligheter som den erbjuder kan inte betraktas fristående utan måste bedömas i förhållande till regelverket i övrigt. I praktiken är det svårt att tillämpa en allmän princip på regler som ger ett begränsat handlingsutrymme till följd av sin detaljgrad. Som nämns ovan är DORA ett mycket detaljerat regelverk. Hur hög detaljgraden slutligen blir kommer att avgöras av de tekniska standarder som de europeiska finanstillsynsmyndigheterna ska ta fram, till exempel om tidsfristen för rapportering av allvarigare incidenter.

Att reglerna i DORA i delar är föreskrivande begränsar också anpassningsmöjligheterna, bland annat till riskerna på försäkringsområdet. Utrymmet för en riskbaserad tillämpning minskar om regler utan undantag föreskriver vad som ska göras och när det ska ske snarare än vilka mål som ska uppnås. Det kan till exempel handla om krav på att med fasta tidsintervall se över styrdokument eller vidta kontrollåtgärder. Sådana krav förekommer bland annat i DORA:s bestämmelser om riskhantering och testning.⁸²

En annan utmaning med finanssektorgemensam reglering är att tillämparna måste förhålla sig till flera regelverk. På försäkringsområdet kommer de allmänna reglerna i rörelseregelverket solvens II om riskhantering och utkontraktering till exempel att gälla vid sidan av de särskilda reglerna om digital motståndskraft i DORA. I gränssnittet mellan allmänna och specifika regler kan frågor uppkomma om i vilka avseenden reglerna skiljer sig åt och om anpassningar av organisationen. En särskild fråga är vad som ska hända med EIOPA:s riktlinjer på området eftersom dessa riktlinjer i stor utsträckning kommer vara överlappande med delar av DORA. Dessa kompletterar solvens II men är särskilt inriktade på it-relaterade risker.

2.5 Sammanfattande reflektioner

Digitaliseringen erbjuder många möjligheter. På försäkringsområdet kan digitaliseringen exempelvis ge företagen bättre förutsättningar att förstå kundernas behov och preferenser och därmed bidra till ökad kundnytta. Det finns emellertid

⁷⁹ Ibid.

⁸⁰ Ibid.

⁸¹ Ibid.

⁸² Se till exempel ibid.

också risker och utmaningar. Det är därför naturligt att det växer fram reglering även på detta område. För att fullt ut dra fördel av digitaliseringen behövs reglering av hög kvalitet. I annat fall riskerar lagstiftarens många gånger goda ambitioner bakom regleringen att förfelas. Detta gäller självfallet såväl EU-rätten som sådan som den svenska reglering som blir resultatet när EU-rätt i förekommande fall genomförs nationellt.

Svensk Försäkring har återkommande framhållit att goda regleringsprocesser är grundläggande för att åstadkomma reglering av hög kvalitet. Det innebär bland annat att lagstiftaren utifrån rimliga tidsplaner måste arbeta fram nya regler med god framförhållning och efter samråd med berörda aktörer. Det betyder också att nya förslag alltid måste underbyggas av tydliga konsekvensutredningar.

Dessa utgångspunkter står sig även – och är kanske till och med särskilt viktiga – när det gäller den horisontellt verkande regleringen på digitaliseringsområdet. Värdet av konsekvensutredningar är till exempel särskilt stort där den tekniska utvecklingen är snabb och dessutom påverkar olika områden, något som gör det svårt att överblicka följderna. Detsamma gäller på områden som kanske tidigare har varit oreglerade och där vägval kan handla om reglering alls bör införas och vad som i så fall är en lämplig tidpunkt för detta. Det finns naturligtvis också ett intresse av att reglering som beslutas och genomförs står sig och inte behöver ändras alltför snart till exempel till följd av den tekniska utvecklingen.

Likaså är samråd fortsatt centralt. Samråd fyller en särskilt viktig funktion i horisontella frågor där det är en utmaning för lagstiftaren att fånga upp alla relevanta aspekter. Det är då nödvändigt att lagstiftaren förankrar förslag brett, i ett tidigt skede och vid behov även senare under regleringsprocessens gång. Att regler tas fram med god framförhållning innan de börjar tillämpas är också betydelsefullt på detta område, inte minst att det finns rimlig tid för nödvändiga it-anpassningar.

Att lagstiftningen ska hålla hög kvalitet är i grunden lagstiftarens ansvar. Branschen kan emellertid bidra i lagstiftarens arbete. Att fånga upp försäkrings- och tjänstepensionsperspektiv även i breda sammanhang och att kunna belysa konsekvenserna på ett rimligt konkret sätt i till exempel underlag till konsekvensutredningar är dock många gånger en utmaning och särskilt så i horisontella frågor. Det ställer krav på både överblick och detaljkunskap. För att ta ett större grepp om de digitala frågorna har Svensk Försäkring bildat en särskild referensgrupp för digitaliseringsfrågor. Den kan bidra till att samla branschens kunnande och erfarenheter för att på bästa sätt möta regleringsutmaningarna på området.



Svensk Försäkring

Svensk Försäkring Box 24043, Karlavägen 108, 104 50 Stockholm
Tel 08 522 785 00
www.svenskforsakring.se