FNO
Finansnæringens Fellesorganisasjon

Justisdepartementet
Lovavdelingen
Postboks 8005 Dep
0030 Oslo

Også sendt elektronisk til:
lovavdelingen@jd.dep.no

Dato: 14.06.2012
Vår ref.: 12-370 BKA TS/CT
Deres ref.: 2012001634 ES LLE/AHI/mk

Høringsuttalelse - EU-kommisjonens forslag til nye personvernregler

Finansnæringens Fellesorganisasjon (FNO) viser til Justisdepartementets høringsbrev av 19. april 2012 vedrørende EU-kommisjonens forslag til nye personvernregler, som har svarfrist 15. juni 2012.

FNOs hovedsynspunkter kan sammenfattes i følgende punkter:

- Flere bestemmelser bærer preg av å være utformet for å dekke sosiale medier og skylagring. FNO ser positivt på at det utformes personvernregelverk som vil gjelde for denne type tjenester. Vi er imidlertid av det syn at Kommisjonen i for liten grad har vurdert om bestemmelsene er tilpasset gjennomregulerte næringer som bank- og forsikring, som også er underlagt finanstilsyn. Etter vår mening kunne Kommisjonens formål vært oppnådd ved å supplere personverndirektivet med nye bestemmelser for sosiale medier og andre nye tjenester.
- FNO mener det bør inntas en bestemmelse i forordningen hvor det presiseres at spesialregulering vil få forrang ved motstrid mellom de generelle reglene i forordningen og spesialregulering i annet EU-regelverk.
- Det foreslåtte sanksjonsnivået er etter FNOs vurdering uforholdsmessig høyt.
- FNO mener det er uklart hvilke rom som gjenstår for nasjonal regulering på områder som ikke reguleres i forordningen eller på områder som kun delvis er regulert i forordningen. Konkrete eksempler gis nedenfor i punkt 3.

1. Generelle kommentarer

FNO observerer at det foreligger svært mange delegasjonshjemler for Kommisjonen i forordningen. Dette har bl.a. den konsekvens at det blir noe vanskelig å overskue

rekkevidden av forslaget. I og med at forordningen skal gjelde for alle bransjer, ser vi likevel at det foreligger et behov for at Kommisjonen kan utarbeide særregulering og implementeringsakter.

FNO vil likevel stille spørsmål ved om Kommisjonen vil rekke å lage nødvendig sekundærlovgivning før forordningen trer i kraft. Sen utarbeidelse av sekundærlovgivning kan, med mindre det gis utsatt ikrafttredelse for enkelte bestemmelser, få den konsekvens at behandlingsansvarlige først må legge om rutinene slik at de etterlever reglene i den generelle forordningen, før de igjen må endre rutinene for å følge regler som Kommisjonen utarbeider med hjemmel i delegert myndighet. I store organisasjoner med omfattende datasystemer som bank og forsikring er dette ressurskrevende og kostbare prosesser.

FNO vil også bemerke at flere av bestemmelsene henviser til eller forutsetter nasjonallovgivning, og vi mener det er uklart i hvilket omfang nasjonal lovgivning kan opprettholdes.

Enkelte bestemmelser, så som for eksempel artikkel *17 Ret til at blive glemt og ret til sletning* og artikkel 18 *Ret til dataportabilitet*, bærer preg av å være utformet for å regulere sosiale medier og skylagring. Dette viser også eksemplene Kommisjonen trekker frem ved presentasjon av bestemmelsene i sin meddelelse til Parlamentet og Rådet. FNO ser positivt på at det utformes personvernregelverk som vil gjelde for denne type tjenester. Vi er likevel av det syn at Kommisjonen i for liten grad har vurdert om bestemmelsene er tilpasset næringer som bank- og forsikring, som i stor grad er regulert av annet EU-regelverk. FNO vil videre presisere at finansnæringen også er underlagt finanstilsyn som gjør at næringen til en viss grad stiller i en annen kategori enn andre næringsdrivende som behandler personopplysninger. Etter vår oppfatning kunne Kommisjonens formål om å regulere de nye tjenestene nås ved å utarbeide et tillegg til eksisterende regelverk som begrenset seg til å dekke disse "nye" mediene/tjenestene.

Kommisjonen gis i noen bestemmelser delegert myndighet til å fastsette format for meddelelser fra den behandlingsansvarlige til den registrerte, som eksempler kan nevnes artikkel 12 *Procedurer og ordninger for udøvelse av den registreredes rettigheder* og artikkel 32 *Meddelelse af brud på persondatasikkerheden til den registrerede*. FNO synes det er svært uheldig dersom finansinstitusjoner skal bli diktert hvordan kontakten med egne kunder skal foregå. Finansinstitusjoner har jevnt over store og kostnadskrevende systemer, for eksempel nettbankløsninger, som brukes til kundekommunikasjon. Eventuelle krav fra Kommisjonen kan føre til at det blir nødvendig å utarbeide nye systemer og/eller foreta dyre tilpassinger av kommunikasjonsløsningene som benyttes i dag. Etter vårt syn er det et paradoks at Kommisjonen i meddelelsen til Rådet og Parlamentet signaliserer at det er et mål at reglene i forordningen skal gjelde for ulike teknologier og tjenester på ulike tekniske plattformer, samtidig som det fremmes forslag om formatkrav i enkeltbestemmelser.

I det følgende vil vi gi innspill på hvordan regelverket vil kunne få betydning for relevant sektorlovgivning for finansnæringen, herunder EU-lovgivning (punkt 2), nasjonal lovgivning (punkt 3) og amerikansk skatterapporteringslovverk (FATCA) (punkt 4). Vi vil også komme med noen kommentarer til enkelte bestemmelser i forordningen (punkt 5). Underveis vil vi også komme med synspunkter om hvilke byrder forslaget vil kunne medføre for næringen. I punkt 6 vil vi komme med noen avsluttende bemerkninger.

2. Forordningens betydning for andre EU-regler

Finansinstitusjoner og deres virksomhet er i dag regulert av et stort antall EU-direktiver som i noen grad også inneholder regler om behandling av personopplysninger.

Tredje hvitvaskingsdirektiv stiller for eksempel krav om at finansinstitusjoner skal kjenne sin kunde, noe som nødvendiggjør legitimasjonskontroll og derigjennom behandling av personopplysninger. FNO er kjent med at det er påbegynt et arbeid med revisjon av tredje hvitvaskingsdirektiv, og det må antas at de plikter som eventuelt fastsettes i henhold til et eventuelt fjerde hvitvaskingsdirektiv, vil harmoneres med de plikter/krav som fastsettes i personvernforordningen. Også i andre direktiver er det bestemmelser som gir anvisning på finansinstitusjoners behandling av personopplysninger, og vi kjenner ikke til at disse er foreslått tilpasset.

Betalingstjenestedirektivet artikkel 79 forutsetter for eksempel at finansinstitusjoner som utfører betalingstjenester skal ha anledning til å bearbeide og utveksle betalingsinformasjon for å motvirke betalingsbedragerier. Denne bestemmelsen er gjennomført i norsk rett i finansieringsvirksomhetsloven § 4b-4. Forbrukerkredittdirektivets artikkel 8 gir videre uttrykk for en plikt for kredittgivere til å vurdere kunders kredittverdighet, og den forutsetter blant annet at medlemsstater har nasjonal lovgivning om kredittinformasjon og databaser for slike formål. Regler om kredittopplysningsvirksomhet finnes som kjent i gjeldende personopplysningslov § 3 og personopplysningsforskriften kapittel 4. Det fremgår ikke konkret av ordlyden i personvernforordningen at medlemsstatene kan ha regler om kredittverdighet og kredittopplysningsvirksomhet, og FNO har vanskelig for å finne unntak i forordningen som gjør det mulig å beholde denne typen regler.

Det kan også stilles spørsmål ved om Kommisjonen har vurdert forholdet mellom de generelle reglene i forordningen og bankers behov for å behandle personopplysninger ved bruk av interne målemetoder for klassifisering og kvantifisering av kunder og kredittrisiko som ledd i å oppfylle gjeldende kapitalkravsregler som bl.a. følger av det konsoliderte bankdirektivet (2000/12/EC) og CAD-direktivet (93/6/EC), og som er gjennomført i finansieringsvirksomhetsloven § 2-9 og §§ 2-9a til 2-9d. Det følger også av den nåværende bankkonsesjonen for behandling av personopplysninger at personopplysninger for dette formålet kan innhentes fra kredittopplysningsforetak. Reglene om kapital- og likviditetskrav

vil bli ytterligere strammet inn gjennom CRD IV, som følger opp den internasjonale kapitalkravsreformen, Basel III, og det er lite trolig at dette vil redusere behovet for å behandle personopplysninger.

FNO mener det er helt nødvendig at Kommisjonen klargjør hvordan de ulike regelverkene forholder seg til hverandre. For å unngå tolkningsspørsmål bør det inntas en tolkningsbestemmelse i forordningen hvor det fremkommer at eventuell spesialregulering vil få forrang ved motstrid mellom en regel i spesialregulering og regel i personvernforordningen.

3. **Forordningens betydning for norsk regelverk**

Forordningen er som nevnt av svært vid karakter, og FNO synes det er uklart hvilke norske regler som vil kunne opprettholdes og hvilke som eventuelt må falle bort som følge av en eventuell ikrafttredelse av forordningen. Problemstillingen blir ikke enklere ettersom enkelte av bestemmelsene i forordningen henviser til at medlemsstatene kan ha nasjonale regler på noen områder eller, som i en del tilfeller, forutsetter nasjonal lovgivning.

FNO vil i det følgende identifisere særnorske regler/registre/behandlingsgrunnlag som er relevante for finansinstitusjoner, og som vi er usikre på om kan opprettholdes under det nye personvernregimet. Denne listen, som *ikke* er uttømmende, består av eksempler på regelsett/registre/behandlingsgrunnlag som alle anses å være svært viktig for norsk finansnæring, og som FNO mener det er viktig å kunne opprettholde også under et eventuelt nytt personvernregime i EU.

a) *Reglene i personopplysningsloven/-forskriften som ikke har korresponderende bestemmelser i forordningen*

Personopplysningsloven/- forskriften har regler om henholdsvis bruk av fødselsnummer mv. (personopplysningsloven § 12), kameraovervåkning (personopplysningsloven kapittel VI og personopplysningsforskriften kapittel 8), og om innsyn i ansattes e-postadresse (personopplysningsforskriften kapittel 9).

Når det gjelder bruk av fødselsnummer fremgår det av personopplysningsloven § 12 at bruk fordrer saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering. Bestemmelsens ordlyd legger således til grunn strenge krav før bruk kan aksepteres. Datatilsynet har funnet det nødvendig å åpne for bruk av fødselsnummer i typekonsesjonene for behandling av personopplysninger som er gitt henholdsvis banker og forsikringsselskaper, noe som tydeliggjør at det er viktig for næringen å kunne benytte fødselsnummeret som entydig identifikasjonsmiddel. Fødselsnummeret brukes bl.a. til sikker identifikasjon for å oppfylle krav i hvitvaskingsregelverket, i rapporteringsøyemed for eksempel til skattevesenet, vask mot Brønnøysundregistrene i

direktemarkedsføringsøyemed, jf. markedsføringsloven § 12 og til kundeadministrasjon. Dersom næringen heretter ikke vil kunne benytte fødselsnummer, vil dette medføre betydelige praktiske vanskeligheter i gjennomføringen av de nevnte plikter, endringer av rutiner og kostbare omleggelser av systemer. Dette vil også være tilfellet på den offentliges side som er mottaker av opplysninger fra finansnæringen.

Som nevnt over i punkt 2, er det også forutsatt i forbrukerkredittdirektivet artikkel 8 at medlemslandene skal sørge for at kredittgivere skal vurdere kunders kredittverdighet blant annet ved søk i relevant database. Regler om kredittopplysningsvirksomhet fremgår av personopplysningsloven § 3 og personopplysningsforskriften kapittel 4. FNO vil fremholde at det er svært viktig å kunne opprettholde disse reglene, da de er helt nødvendige bl.a. ved vurdering av både fysiske og juridiske personers lånesøknader og for å gjennomføre risikoklassifisering etter bestemmelsene i finansieringsvirksomhetsloven § 2-9 og §§ 2-9a til 2-9d.

b) Konsesjonssystemet – personopplysningsloven kapittel 6 og forskriften §§ 7-2 og 7-3

Norske finansinstitusjoner må, som kjent, overholde de plikter som oppstilles av Datatilsynet i typekonsesjonene for å behandle personopplysninger gitt henholdsvis banker og forsikringsselskaper. FNO vil stille spørsmål om det er rom for å opprettholde et norsk konsesjonssystem etter personopplysningsloven dersom en personvernforordning trer i kraft. Etter FNOs vurdering har det ingen stor betydning om konsesjonssystemet vil bestå som i dag, eller ikke. FNO vil imidlertid understreke at det er eksempler på at konsesjonene gir finansinstitusjoner utvidede rettigheter til å behandle personopplysninger sammenlignet med det som fremgår av personopplysningslov og forskrift. Eksempelvis følger det av forsikringskonsesjonen at behandling av fagforeningsopplysninger i kollektive forsikringsordninger kan foretas uten skriftlig samtykke fra den registrerte og uten annen hjemmel i lov, i medhold av lov eller av forskrift med hjemmel i lov. Det er videre næringens erfaring at konsesjonsordningen også sikrer en mer enhetlig behandling av personopplysninger i næringen. Dette antas både å sikre forutsigbarheten for kundene og forenkle det offentliges tilsyn med at næringens behandling av personopplysninger er i samsvar med regelverket.

c) Risikovurdering forsikring

Forsikringsvirksomhetsloven (forsvl.) § 12-5 regulerer kravet til og bruken av premietariffer for standardiserte produkter i skadeforsikringsselskaper. Premietariffene dannes i hvert enkelt selskap på bakgrunn av aggregerte historiske skadedata innenfor ulike produktgrupper i vedkommende selskap. Bestemmelsen må suppleres med forsvl. § 12-6 som gjelder den individuelle premieberegning. Tilsvarende hjemler finnes også for livsforsikringsselskapene i forsikringsvirksomhetsloven kapittel 9.

For å fastsette pristariffene har selskapene behov for en del grunnleggende personopplysninger (kontaktinformasjon, fødselsdato/-nummer etc.) som ikke nødvendigvis er sensitive. For personproduktene vil selskapene i mange tilfeller også kreve at forsikringssøkeren avgir helseerklæring. Helseerklæringen vil danne grunnlag for om forsikring blir tegnet uten særskilte vilkår, eller om den tegnes med vilkår/reservasjoner knyttet til bestemte lidelser, eller helt avslås. Slike individuelle helseopplysninger vil være avgjørende viktig for inngåelse av forsikringsavtalen og premieberegningen. FNO legger til grunn at Kommisjonen ikke har til hensikt å stenge for at forsikringsselskapene skal skulle benytte denne typen opplysninger, da dette vil kunne få dramatiske konsekvenser for bransjen. Etter vår oppfatning må dette klarere fremgå, for eksempel ved fastsettelse av et unntak.

Se for øvrig vår konkrete kommentar til henholdsvis artikkel 9, 17 og 81 under punkt 4 nedenfor.

d) Reglene om finansinstitusjoners utlevering av personopplysninger.

I norsk rett foreligger det en rekke bestemmelser som regulerer en finansinstitusjons utlevering av personopplysninger. Som eksempler kan nevnes:

1. Forsikringsvirksomhetsloven § 1-6 annet ledd, sparebankloven § 21 og forretningsbankloven § 18 inneholder omtrent likelydende regler som fastslår at taushetsplikt ikke er til hinder for at finansinstitusjoner i særlige tilfelle, og i henhold til styrevedtak/fullmakt fra styret, gir annen finansinstitusjon opplysninger som foretaket har mottatt under utøvelse av virksomheten dersom formålet har vært å avdekke eller motvirke økonomisk kriminalitet eller annen alvorlig kriminalitet, eller for forsikring sitt vedkommende, å sikre en ensartet helsebedømmelse.
2. Folketrygdloven § 21-4b er det rettslige grunnlaget for at finansinstitusjoner og NAV skal kunne ha en informasjonsutveksling med det formål å avdekke trygdemisbruk.
3. Hvitvaskingsloven § 20 annet ledd fastslår at finansinstitusjoner og forsikringsselskaper uten hinder av taushetsplikt kan utveksle nødvendige kundeopplysninger seg imellom når det anses nødvendig for å foreta undersøkelser etter samme lov § 17.
4. Finansieringsvirksomhetsloven § 4b-4 hjemler, som nevnt ovenfor, at finansinstitusjoner som utfører betalingstjenester skal ha anledning til å bearbeide og utveksle betalingsinformasjon for å motvirke betalingsbedragerier.
5. Samordningsloven § 27 nr. 2 (og forskrift av 6.7.2000 nr. 727 om registrering og utveksling av opplysninger (meldesystem) for å gjennomføre bestemmelsene i samordningsloven mv.) sikrer at tjenestepensjonsleverandører mv. og NAV kan utveksle opplysninger seg imellom slik at det skjer korrekt samordning og tilpassing av ytelser fra pensjons- eller trygdeordninger som omfattes av loven.

Alle disse hjemlene har betydelig samfunnsmessig funksjon da de har til formål å motvirke og avsløre svik og bedrageri, samt – når det gjelder nr. 5 ovenfor – å sikre korrekt beregning av ytelser under offentlige tjenestepensjonsordninger. Etter FNOs vurdering er det mulig at artikkel 9 bokstav j "(..) for at udføre en opgave af hensyn til vigtige samfundsinteresser, og for så vidt den er hjemlet i EU-retten eller medlemsstatslovgivning, som fastsetter de fornødne garantier" gir tilstrekkelig grunnlag for den informasjonsutveksling som kan skje i medhold av folketrygdloven § 21-4b, hvitvaskingsloven § 20 og samordingsloven § 27 nr. 2. FNO vil imidlertid stille spørsmål ved om det er rom i forordningen for de øvrige, svært viktige informasjonsutvekslingsregler. De øvrige bestemmelsene er videre og mer generelle, og det bør søkes avklart hvorvidt disse "fastsetter de fornødne garantier".

e) Register over forsikringssøkere og forsikrede (ROFF) og sentralt skaderegister (FOSS).

Forsikringsbransjen har et register over forsikringssøkere og forsikrede (ROFF) og et Sentralt skaderegister (FOSS). Begge registrene har konsesjon fra Datatilsynet gitt i medhold av personopplysningsloven § 33, jf. § 34 til å behandle sensitive personopplysninger. Formålet med ROFF er å forbedre og sikre en ensartet risikobedømmelse ved premiefastsettelse, samt å unngå spekulasjon. Formålet med FOSS er å forebygge og avdekke forsikringssvindel. FNO administrerer disse to registrene på vegne av medlemsbedriftene. I typekonsesjonen for å behandle personopplysninger for forsikringsselskapene fremgår det at:

"c) Informasjon
Personopplysninger kan utleveres til ovennevnte registre forutsatt at den registrerte er informert om registreringen og registreringen ikke er i strid med lovbestemt taushetsplikt. Det enkelte forsikringsselskap må sørge for at det informeres **særskilt** om:

i) Når kunden vil bli registrert i disse registrene (ved avtaleinngåelse, ved avtaleinngåelse på spesielle vilkår, ved avslag, ved skademelding), hvilke opplysninger som registreres, hvorfor de registreres og hvor lenge de vil være registrert.
ii) at kunden vil bli kontrollert opp i mot fellesregistrene.

d) Opplysningstyper som kan utleveres

i) Til ROFF kan det for å bedre og sikre en ensartet risikobedømmelse ved premiefastsettelse, samt til kontroll med sikte på å unngå spekulasjon, utleveres følgende opplysninger om forsikringssøkere og forsikrede:
- navn
- fødselsnummer
- registrerende selskap
- registreringsdato
- uførhet

- særrisiko

ii) Til FOSS kan det for å effektivisere skadeforsikringsselskapenes saksbehandling i forbindelse med arbeidet med å forhindre og begrense forsikringssvindel, utleveres følgende opplysninger om forsikringstakere som melder skade med krav om forsikringsutbetaling:
- fødselsnummer
- saksnummer
- bransjekode
- selskap
- skadetype
- dato
- saksbehandlers initialer"

Det er utarbeidet en brukerveiledning som gir en ganske detaljert beskrivelse av hvordan forsikringsselskapene bruker registeret i praksis.

FNO vil for det første stille spørsmål ved om disse registrene kan opprettholdes, så fremt samtykke til utlevering innhentes fra forbruker *og* kunden får informasjon, som forutsatt i forsikringskonsesjonen i dag. Det må også avklares om forsikringsselskapene fortsatt kan utlevere de samme opplysningene til registrene som forsikringsselskapene oppgir i dag.

Både ROFF og FOSS vil inneholde begrensede helseopplysninger, jf. sitatet ovenfor fra typekonsesjonen om hvilke opplysninger som kan innhentes. Utkastet til forordning er imidlertid uklart når det gjelder forsikringsselskapenes anledning til å behandle helseopplysninger, jf. merknadene til artikkel 9 og 81 nedenfor. Dette skaper igjen usikkerhet om lovligheten av å opprettholde og bruke informasjon som er lagret i disse registrene.

f) Regler om innhenting av vandelsattest.

I finansmarkedslovgivning er det oppstilt krav om hederlig vandel for institusjonens styremedlemmer og virksomhetens daglige ledelse. Eksempler på hjemler er bl.a. forsikringsformidlingsloven § 3-3, børsloven § 10 annet ledd, verdipapirfondloven § 2-3. For å kunne dokumentere hederlig vandel, vil det kunne være nødvendig å legge frem vandelsattest/politiattest. Som nevnt i FNOs høringsuttalelse av 06.04.11 til Finansdepartementets høringsbrev av 21.01.11 om forslag til lovendringer om politiattester og vandelsvurderinger på finansmarkedsområdet, er det FNOs prinsipielle oppfatning at lovkravet om hederlig vandel, supplert med en rett til å innhente ordinær politisattest, også bør omfatte nærmere definerte grupper av ansatte. Faren for anslag fra kriminelle har ikke blitt mindre, og FNO mener følgelig at det er viktig at finansinstitusjoner også under nytt personvernregime må kunne innhente vandelsattest.

4. **Nye regler i amerikansk skatterapporteringsregelverk (FATCA)**
Foreign Accounts Tax Compliance Act (FATCA) ble en del av amerikansk lovverk 18.03.10 og skal tre i kraft 01.01.13. Formålet med loven er å bekjempe skatteunndragelse i form av manglende innrapportering av midler på utenlandske konti tilhørende amerikanske borgere og selskaper. Loven innfører ikke ubetydelige rapporteringsplikter mv. for banker, livsforsikringsselskaper, verdipapirforetak og fondsforvaltere, og rapporteringen vil da i utgangspunktet skje i form av utlevering av personopplysninger til amerikanske myndigheter. FNO mener det må avklares hvorvidt det innenfor forordningen åpnes for slik rapportering direkte til amerikanske myndigheter eller via norske myndigheter til amerikanske myndigheter.

5. **Konkrete kommentarer til enkeltbestemmelser i forordningen (dansk utgave)**
Artikel 6 Lovlig behandling af personoplysninger
Artikkel 6 nr. 4 lyder: "Hvis formålet med yderligere behandling ikke er foreneligt med det formål, hvortil personoplysningerne er indsamlet, skal behandlingen have sit retsgrundlag i mindst én av de grunde, der er anført i stk. 1, litra a)-e). Dette gjelder navnlig for ændring af kontraktlige vilkår og betingelser."

FNO er av det syn at det her bør henvises til punkt 1 litra a) – f), fremfor litra a)-e), da det også her må åpnes for at en behandlingsansvarlig kan behandle opplysningene etter en interesseavveining. FNO mener også at det er uklart hva som menes med den siste setningen i nr. 4. Det bør klargjøres hvorfor man her nevner endring av kontraktsvilkår som eksempel.

Artikel 7 Betingelser for samtykke
Det fremgår av artikkel 7 nr. 4 at samtykke ikke er rettsgrunnlag for behandling i de tilfeller det er vesentlig ubalanse mellom den registrerte og den behandlingsansvarlige. I de tilfeller hvor en avtale inngås mellom finansinstitusjon og forbruker, vil det normalt sett foreligge vesentlig ubalanse mellom partene. Bestemmelsen vil dermed etter sin ordlyd alltid komme til anvendelse. Samtykke vil dermed i praksis ikke lenger være et tilstrekkelig behandlingsgrunnlag for finansinstitusjoner, noe som for eksempel vil kunne få betydning for forsikringsselskapers muligheter til å innhente helseerklæringer ved inngåelse av personforsikringsavtale.

FNO er kjent med at ordlyden i fortalen punkt 34 kan tyde på at artikkelen først og fremst er tenkt brukt i ansettelsesforhold og offentligrettslige forhold. Vi mener like fullt at ordlyden i bestemmelsen bør presiseres slik at bestemmelsens rekkevidde er klar.

Artikel 9 Behandling af særlige kategorier af personoplysninger
Utkastet til artikkel 9 statuerer at behandlingen av personopplysninger kun er tillatt hvor minst ett av behandlingsgrunnlagene i bokstav a-f er oppfylt.

FNO har vanskelig for å se at finansinstitusjoners behov for behandling av sensitive opplysninger, for eksempel knyttet til helseopplysninger, har blitt tatt hensyn til i utformingen av bestemmelsens ordlyd. Særlig forsikringsselskaper må behandle helseopplysninger i avtaleinngåelsesprosedyren ved noen forsikringsprodukter. FNO mener derfor at artikkelen må presiseres, slik at det klart og tydelig fremgår at finansinstitusjoner kan behandle sensitive personopplysninger. Se også vår kommentar til artikkel 17 og 81. FNO vil også fremheve at ingen av de alternative behandlingsgrunnlagene passer for den informasjonsutveksling som kan være nødvendig ved utredning av saker hvor det er spørsmål om svik/bedrageri. For eksempler på informasjonsutvekslingshjemler, se punkt 3 over.

Under det gjeldende direktivet er det mulig for bankene å ha dataregister over misbrukere, jf. det nå nedlagte Bankenes Misbrukerregister. Det er imidlertid ikke utenkelig at slik register vil være nødvendig i fremtiden, og FNO vil stille spørsmål ved om det er mulig innenfor hjemmelen i artikkel 9 til å ha slike registre.

Artikel 12 Procedurer og ordninger for udøvelse af den registreredes rettigheder
FNO har i utgangspunktet ikke problemer med at registrerte kan inngi forespørsler om informasjon om registrerte opplysninger elektronisk, jf. artikkelens annet ledd. Vi mener likevel at finansinstitusjoner ikke kan gi ut informasjon uten at vedkommende som spør er identifisert på en tilfredsstillende måte. Det bør heller ikke oppstilles en plikt til å gi informasjon elektronisk med mindre den kan gis ut på en etter omstendighetene tilfredsstillende sikker måte, for eksempel for bankers del via nettbank eller i kryptert form.

Bestemmelsens sjette ledd gir kommisjonen hjemmel til å utarbeide standardformularer til kunder. FNO mener det må være opp til bransjen selv hvordan kommunikasjonen med kundene skal skje. Det vil kunne være svært kostnadskrevende å legge om informasjonssystemer som over lang tid er bygget opp. Vi vil også stille spørsmål ved om bruk av standardskjemaer vil ivareta hensynet til teknologinøytralitet som nettopp benyttes som et argument for harmonisering, samt om standardformularer som i praksis vil dekke en lang rekke typetilfeller kan utformes slik at de blir tilstrekkelig brukervennlige. Dersom kravet blir stående i forordningen mener vi at finansinstitusjoner må unntas fra kravet.

Artikel 15 Den registreredes ret til indsigt
Når det gjelder andre ledd vil FNO vise til vår kommentar under artikkel 12.

Artikel 17 Ret til at blive glemt og ret til sletning
FNO vil bemerke at finansinstitusjoner er underlagt regler bl.a. i bokføringsloven og hvitvaskingsloven som gjør at personopplysninger må oppbevares i visse perioder også etter

at et kundeforhold er avsluttet. Vi antar at Kommisjonen har ment å ta høyde for nettopp dette i bestemmelsens nr. 3 litra d).

Ved såkalt langhalet forretning (særlig aktuelt bl.a. innenfor personforsikring) vil forsikringsselskapene måtte lagre informasjon om forsikringsavtalene for å kunne behandle og ta stilling til krav som fremsettes. Avtaleinformasjon lagres så lenge som det er nødvendig i henhold til foreldelsesfristen for vedkommende type krav. Behandlingsgrunnlag vil som regel være uttrykkelig samtykke (jf. personopplysningsloven § 8 innledningsvis og § 9 bokstav a og/eller avtale (jf. § 8 bokstav a). Avtaleforpliktelser er ikke uttrykkelig nevnt i artikkelen som grunnlag for lagring etter at den registrerte har bedt om sletting, og dette vil være problematisk for finansnæringen. FNO mener derfor at artikkelen på dette punkt må endres.

Denne bestemmelsen vil også være uheldig for kredittopplysningsvirksomhet.

Artikel 18 Ret til dataportabilitet
Bestemmelsen oppstiller en rett til dataportabilitet. Slik FNO ser det er denne bestemmelsen klart rettet mot sosiale nettverk og skylagring, og vi kan ikke se at den er egnet til å bruke i kundeforhold mellom forbruker og finansinstitusjoner.

Etter FNOs vurdering reiser bestemmelsen en rekke problemstillinger, og vi vil rent summarisk trekke frem enkelte:

For det første er det ikke gitt noen retningslinjer om hvordan den behandlingsansvarlige som mottar forespørselen om portering, skal kunne vite at personen som kommer med forespørselen er rette vedkommende. Finansinstitusjoner er underlagt taushetsplikt og aktørene må forholde seg til strenge sikkerhetsrutiner for å unngå svindel og bedrageri. Det er dermed vitalt at de det utarbeides sikkerhetsmekanismer og legitimasjonskrav som gjør at finansinstitusjonene kan være sikre på at forespørselen kommer fra kunden og ikke andre som utgir seg for å være denne. Det er også uklart hvilke opplysninger som må gis ut som følge av porteringshenvendelse.

Dersom det er slik at kunden skal kunne bruke opplysningene på ny overfor andre finansinstitusjoner, vil FNO stille spørsmål med hvordan finansinstitusjonene skal kunne stole på opplysninger som mottas. Vi har også vanskeligheter med å se for oss hvordan finansinstitusjonene skal kunne oppfylle kravene til kundekontroll som følger av tredje hvitvaskingsdirektiv artikkel 6-8 og som er gjennomført i hvitvaskingsloven kapittel 2, dersom en slik regel om portering innføres. Legges det til grunn at det kun er første finansinstitusjon som skal foreta kundekontroll, vil dette kunne føre til at institusjoner med dårlige hvitvaskingsrutiner vil kunne bli "brukt" til å få opprettet falske personidentiteter.

Videre vil vi stille spørsmål ved om en porteringshenvendelse etter artikkel 18 også må anses som et krav om sletting etter artikkel 17. Hvis svaret her er bekreftende, må det igjen stilles spørsmål ved om en porteringshenvendelse også må anses som en oppsigelse av kundeforholdet.

Etter vår vurdering er denne bestemmelsen kilde til flere spørsmål enn svar for finansnæringen – og den kan også få den betydning at den enkeltes personvern blir svekket sammenlignet med i dag. Vi mener derfor at rekkevidden til bestemmelsen må snevres inn slik at den ikke vil gjelde for finansinstitusjoner.

Artikel 31 Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden og artikel 32 Meddelese af brud på persondatasikkerheden til den registrerede
Kommisjonen slår i artikkel 31 og 32 fast at den behandlingsansvarlige uten unødig opphold og senest innen 24 timer etter at sikkerhetsbruddet ble kjent, må rapportere om bruddet til tilsynsmyndigheten og til den registrerte.

FNO er av den oppfatning at bestemmelsen legger til grunn en for vidtgående varslingsplikt. For det første legges det til grunn at ethvert avvik skal varsles. Etter FNOs vurdering kan det skje sikkerhetsbrudd uten at personopplysninger kommer på avveie. Varsling av denne typen avvik vil gi finansinstitusjoner unødvendig merarbeid og vil kunne føre til unødvendig belastning og bekymring for datasubjektene. Etter FNOs vurdering bør det settes en terskel for hvilke databrudd som skal varsles, og etter vår oppfatning er det naturlig å se hen til personopplysningsforskriftens § 2-6 som gir anvisning på at Datatilsynet skal varsles dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig.

Varslingsfristen er også urealistisk kort. Det vil for eksempel være svært utfordrende for finansinstitusjonen både å identifisere bruddet, få rettet det opp og få varslet kunden innen en slik tidsfrist. Ved varsling av kunden vil man også ha en utfordring med å få utformet varselet slik at det beskriver sikkerhetsbruddet og konsekvensen av sikkerhetsbruddet på en god måte. Dette kan for eksempel være særlig utfordrende dersom bruddet manifesterer seg på ulike måter overfor forskjellige kunder, og dersom sikkerhetsbruddet skjer på natten eller i helgen.

Artikel 37 Den databeskyttelsesansvarliges hverv
FNO vil stille spørsmål ved om personvernombud vil kunne utføre andre oppgaver enn de som skal gjøres i henhold til denne artikkelen litra a)-h).

Artikel 43 Videregivelse ved anvendelse af bindende virksomhedsregler
Det er viktig at det tilrettelegges for at bindende virksomhetsregler kan benyttes så vel i rene aksjekonsern som i samarbeidende grupper, for eksempel samarbeidende banker som Terrabankene og Sparebank 1 Gruppen, slik at konkurransegrunnlaget for konsern og samarbeidende grupper blir likt. Ordlyden i bestemmelsen bør dermed utvides til å omfatte konsernlignende organiseringer.

Artikel 64 til 72 Det Europæiske Databeskyttelsesråd
FNO vil stille spørsmål ved hvilken rolle EØS/EFTA-landene vil spille i et slikt tilsynsråd. Slik vi ser det bør norske myndigheter kunne delta på lik linje med EU-land. Som et minimum må norske myndigheter få en permanent observatørplass.

Artikel 77 Ret til erstatning og erstatningsansvar
Artikkelen oppstiller en rett til erstatning ved påført skade. Det fremgår imidlertid ikke hvilket ansvarsgrunnlag som skal legges til grunn, om både økonomisk og ikke-økonomisk tap skal dekkes eller hvordan eventuell erstatning skal utmåles. FNO er av det syn at det er høyst uklart hvordan denne bestemmelsen forholder seg til nasjonale erstatningsregler.

Artikel 79 Administrative sanktioner
FNO er av det syn at sanksjonsnivået er uforholdsmessig høyt. Det synes som Kommisjonen ved fastsettelse av nivået har sett hen til sanksjonsnivået i konkurranseretten. Etter FNOs vurdering er det forskjell mellom overtredelse av konkurranserettslige regler og overtredelse av personvernsregler. I konkurranseretten, i motsetning til personvernretten, vil brudd på reglene gjerne være direkte motivert av betydelig økonomisk vinning. En administrativ sanksjon av en viss størrelse vil i denne typen saker ha en inndragningsfunksjon. Denne funksjonen vil det normalt sett ikke være behov for ved brudd på personvernlovgivningen, som normalt sett ikke vil gi noen større økonomisk vinning. Vilkårene i bestemmelsene i forordningen er dessuten i stor grad uklare og skjønnsmessige, og FNO vil stille spørsmål ved om det er i samsvar med legalitetsprinsippet å fastsette et så høyt sanksjonsnivå for brudd på denne typen bestemmelser.

FNO ser videre at bestemmelsen legger anvisning på at den administrative sanksjonen skal måles ut fra global omsetning. FNO vil stille spørsmål ved hva som ligger i begrepet global omsetning. Vi kan heller ikke se at det her er avklart hvordan boten skal utmåles for eksempel dersom det er datterselskap i konsern eller en filial som har overtrådt reglene i forordningen.

I tredje ledd gis det videre anvisning på at enkelte personer kan unngå sanksjon ved første overtredelse, og heller få en skriftlig advarsel. FNO er av det syn at denne regelen må gjelde for alle behandlingsansvarlige – den foreslåtte løsningen medfører urimelig

forskjellsbehandling. Etter vår vurdering vil store behandlingsansvarlige ha vel så gode, i mange tilfeller bedre, rutiner for behandling av personopplysninger, enn det små behandlingsansvarlige har.

Artikel 81 Behandling af personoplysninger om helbredsforhold
Artikkel 81 regulerer behandling av helseopplysninger. FNO mener det er uklart om forsikringsselskapers behandling av helseopplysninger i tilstrekkelig omfang omfattes av første ledd litra c. (Bestemmelsens første ledd litra a og b oppfattes klart nok ikke å omfatte forsikringsselskaper). Vi viser under dette punkt også til vår kommentar til artikkel 9 og artikkel 17.

6. Avsluttende bemerkninger

FNO ber om at Justisdepartementet tar hensyn til finansnæringens synspunkter i det videre arbeidet med lovgivningsprossessen i EU. Etter vår oppfatning er det svært viktig at Justisdepartementet forsøker å få en avklaring på hvilket rom som gjenstår for nasjonale regler under det foreslåtte regimet og hvilke hjemler i norsk lovgivning som kan opprettholdes eller som må bortfalle. Dersom for eksempel konsesjonsordningen etter personopplysningsregelverket må falle bort, mener FNO at departementet, innenfor rammen av forordningen, må vurdere å opprette nye hjemler i lov som gir uttrykk for det samme som konsesjonen.

Med vennlig hilsen
Finansnæringens Fellesorganisasjon

Trond Søyland
seksjonsdirektør

Charlotte Tvedt
Charlotte Tvedt
juridisk seniorrådgiver