



Justis- og beredskapsdepartementet
sendes elektronisk

Dato: 16.10.2017
Vår ref.: 17-1100
Deres ref.: 17/4200

Høringssvar: Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett

Vi viser til Justis- og beredskapsdepartementets høring av 06.07.2017; Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett.

Finans Norge har følgende hovedsynspunkter til forslaget:

- Konesjonsplikten for finansforetak i gjeldende lov bør ikke videreføres.
- Unntaket for den registrertes innsynsrett i interne dokumenter må videreføres.

Innledende synspunkter

Harmonisering

Personvernforordningens regler, som i hovedsak må anvendes slik de står der hvor det ikke er nasjonalt handlingsrom, innebærer i seg selv en harmonisering av personvernregelverket i EU- og EØS-området. Etter Finans Norges syn er det viktig at dette følges opp gjennom en ensartet anvendelse av regelverket på nasjonalt nivå for å sikre like konkurransevilkår på et felleseuropeisk marked. Som departementet redegjør for må forordningen implementeres i EØS-avtalen og at det i den forbindelse må foretas visse tilpasninger. Det er viktig at disse tilpasningene ikke medfører materielle endringer. Videre er det svært viktig at denne prosessen ikke forsinker forordningens ikrafttredelse i Norge og EØS-området.

Artikkel 29-gruppens veiledere

Foruten forordningen med fortale er rettskildebildet på området relativt beskjedent. Artikkel 29-gruppen har kommet med retningslinjer («guidelines») på enkelte særlige problemstillinger som departementet viser til i høringsnotatet. Finans Norge er positive til felleseuropeiske retningslinjer da dette underbygger harmonisert anvendelse. Vi finner imidlertid grunn til å påpeke at retningslinjene ikke nødvendigvis er direkte overførbare for norske forhold. Artikkel 29-gruppens veileder «Guidelines on Data Protection Officers» slår for eksempel kort fast at en banks behandling av personopplysninger må anses å være

behandling i stor skala. I samme avsnitt konstateres det at en enkeltstående lege eller en advokats behandling av personopplysninger ikke vil oppfylle kravene til stor skala. Etter vårt syn vil enkelte norske finansforetak, som eksempelvis mindre sparebanker, i europeisk sammenheng komme i samme størrelseskategori som de nevnte behandlingsansvarlige. Artikkel 29-gruppen viser til.

Kapittel 7 - behandlingsgrunnlag

Generelt

Behandlingsgrunnlaget i gjeldende lov § 8 første ledd annet alternativ, at adgangen til behandling er fastsatt i lov, har ingen direkte parallell i forordningen. Finans Norge er enig i departementets vurdering av at dette neppe medfører noen realitetsendring. De fleste behandlinger vil, som departementet gir uttrykk for, faller inn under behandlingsgrunnlagene i artikkel 6 nr. 1 bokstav e og c; «rettslig forpliktelse», «i allmennhetenes interesse» eller «utøvelse av offentlig myndighet».

Rettslig forpliktelse

Departementet legger til grunn at forordningen ikke oppstiller krav om at formålet må fremgå eksplisitt av en egen lov- eller forskriftsbestemmelse, og at det er tilstrekkelig at formålet fremgår mer indirekte, eksempelvis gjennom forarbeidene. Problemstillingen er av stor praktisk betydning for finansforetak, som er underlagt omfattende regulering knyttet til internkontroll, rapportering mv. Som eksempel kan nevnes bruk av IRB-modeller, som blant annet krever at personopplysninger (historiske kundeopplysninger) benyttes for validering. Andre eksempler er kredittvurdering ved utlån og krav til risikoberegninger innen forsikring. Slike lovpålagte plikter angir sjelden uttrykkelig formålet, men som regel fremgår dette forutsetningsvis. Finans Norge er enig med departementet i at vilkåret om rettslig forpliktelse bør være oppfylt der hvor formålet fremgår indirekte.

Kapittel 8 - behandling av sensitive personopplysninger

Statistiske formål

Finans Norge legger til grunn at “statistiske formål” i artikkel 9 nr. 2 bokstav j også omfatter utarbeidelse av statistikk i privat virksomhet. Det vises til beskrivelsen av statistiske formål i portalens avsnitt 162.

Finansforetak benytter statistikk i blant annet risikoanalyser. Disse analysene danner grunnlag for tariffer (generelle risikovurderinger) og for individuelle risikovurderinger, foruten solvens- og soliditetskrav. Statistikken kan bygge på underlagsmateriale som ikke alltid er anonymisert eller pseudonymisert.

Det er ikke hensiktsmessig å bygge på samtykke fra enkeltpersoner for disse behandlingsformålene, blant annet fordi et samtykke når som helst skal kunne trekkes tilbake. Interesseavveiningsbestemmelsen i artikkel 6 bokstav f vil kunne anvendes for

alminnelige personopplysninger, men gir ikke behandlingsgrunnlag når det gjelder særlige kategorier av personopplysninger.

Særlig om personvernrådgivers tilråding

Den foreslåtte bestemmelsen om tilråding fra personvernrådgiver er egnet til å legge et utilbørlig press på personrådgiveren, et press som vil kunne komme i konflikt med kravene til rådgiverens uavhengighet, jf. forordningens artikkel 38 nr. 3. Den foreslåtte bestemmelsen i ny lov § 6 bokstav d bør følgelig utgå..

Fagforeningsmedlemskap

Mange kollektive forsikringsordninger i Norge er inngått med fagforeninger som forsikringstaker. Fagforeningsmedlemskap er etter artikkel 9 nr. 1 en sensitiv personopplysning i likhet med gjeldende personopplysningslov § 9 første ledd bokstav a).

Slike kollektive forsikringsordninger, tredjepartsavtaler der fagforeningen er forsikringstaker og medlemmene av fagforeningen er sikret etter avtalen, inneholder som regel store grupper av personer som dermed ikke har noe direkte avtaleforhold med forsikringsselskapet. For disse forsikringene vil ikke samtykke som behandlingsgrunnlag være praktisk. Dette kommer også til uttrykk i dagens generelle forsikringskonsesjon, som etter å ha gjort rede for at behandling av sensitive personopplysninger må skje på grunnlag av skriftlig samtykke eller lov sier «Unntatt fra dette krav er behandling av fagforeningsopplysninger i kollektive forsikringsordninger». Unntaket bør videreføres, enten i lov eller i forskrift.

Kapittel 10 - behandling av personopplysninger om straffedommer og lovovertrедelser

I gjeldende personopplysningslov § 2 nr. 8 er mistanke om straffbare forhold ansett som en sensitiv personopplysning. Datatilsynet har i sin praksis over tid lagt til grunn at personopplysningsloven § 8 bokstav f og § 9 første ledd bokstav e, sammenholdt med konsesjonen kan benyttes i forbindelse med forsikringsselskapers behandling av saker hvor det foreligger mistanke om svik.

Etter forordningen er ikke mistanke om bedrageri mot foretaket en sensitiv personopplysning, jf. artikkel 9. Finans Norge mener at mistanke om bedrageri mot foretaket heller ikke omfattes av artikkel 10. Etter vår vurdering kan således personopplysninger knyttet til mistanke om bedrageri mot foretaket, herunder utredningsarbeid innen finansforetak, behandles i medhold av de alminnelige behandlingsgrunnlag i artikkel 6.

Dersom departementet likevel skulle være av den oppfatning at finansforetaks utredningsvirksomhet omfattes av artikkel 10; «(...) personopplysninger om straffedommer

og lovovertreddelser (...)» må det etableres nasjonal hjemmel. Dette gjelder særlig for banker som ikke har tilsvarende hjemler som forsikringsselskap har etter forsikringsavtaleloven § 8-1 og § 18-1. Finansforetak er stadig, og i økende grad, utsatt for bedragerier og at det er av stor samfunnsmessig betydning at foretakene har tilstrekkelige hjemler for å opprettholde arbeidet med å bekjempe denne formen for kriminalitet.

I forbindelse med finansforetaks arbeid mot hvitvasking og terrorfinansiering vil det i enkelte tilfeller være behov for å oppbevare dommer etc. som del av en begrunnelse for forsterkede kundetiltak. Dette er opplysninger som etter vår vurdering omfattes av artikkel 10 og krever hjemmel i lov. Etter vår vurdering er det imidlertid til en viss grad uklart hvorvidt gjeldende hvitvaskingslov gir tilstrekkelig hjemmelsgrunnlag. Krav om tilstrekkelig hjemmelsgrunnlag for også slike personopplysninger bør i alle fall hensyntas i den nye hvitvaskingsloven slik Datatilsynet påpeker i sin høringsuttalelse til ny hvitvaskingslov.

Kapittel 12 – den registrertes rettigheter

12.3.2 Unntak fra retten til informasjon og innsyn

Finans Norge støtter i hovedsak de foreslåtte unntakene i den registrertes innsynsrett. Vi mener videre at unntak for innsynsrett i «interne dokumenter som ikke er utlevert til andre» som i dag finnes i personopplysningsloven § 23 (1) bokstav e, må videreføres i ny personopplysningslov.

De rettslige rammer for adgang til å gjøre unntak

Justisdepartementet uttaler i høringsnotatet at det etter departementets syn ikke vil være adgang til å videreføre unntaket for innsynsrett i «interne dokumenter» som i dag finnes i personopplysningsloven § 23 første ledd bokstav e, med grunnlag i forordningens art 23. Finans Norge deler ikke denne tolkningen.

Personvernforordningen artikkel 15 kan avvikes gjennom nasjonal lovgivning dersom særlige vilkår er oppfylt, jf. artikkel 23. Relevant i denne sammenheng er art 23 nr. 1 bokstav i: «vern av den registrertes interesser eller andres rettigheter og friheter». Sitatet svarer til ordlyden i [Europa-parlamentet og Rådets direktiv 95/46/EF](#) (dansk utgave) artikkel 13 nr. 1 bokstav g, som ligger til grunn for gjeldende personopplysningslov.

Ved vedtakelsen av dagens personvernlovgivning fant man at: «Unntakene [i pol § 23] er av en slik karakter at de omfattes av direktivet artikkel 13.», jf. [Ot prp nr 92 \(1998-1999\) pkt. 16](#) med merknader til § 23. Vi kan ikke se at det foreligger rettskilder som tilsier at samme formulering skal tolkes annerledes i forordningen.

Vår vurdering støttes av høringsnotatene fra våre naboland. I Danmark har Justisministeriet den oppfatning at «[r]ettstilstanden for det nationale råderum efter artikel 23, stk. 1, ses at

være en videreførelse af den gældende retstilstand efter databeskyttelsesdirektivet», se [Betænkning Databeskyttelsesforordningen \(2016/679\) del I bind 1 s 400](#). I Sverige er departementet av samme oppfatning, se [Betänkande av Dataskyddsutredningen SOU 2017 : 39 side 206](#) og det foreslås å videreføre unntak for innsynsrett/registerutdrag i «løpende text som utgör utkast eller minnesanteckning».

Justisdepartementets begrunnelse er dels basert på at dagens unntaksregel ikke er «knyttet til arten av opplysningene eller til hva disse skal brukes til, men utelukkende til hvor opplysningene finnes». Finans Norge mener dette ikke er et riktig utgangspunkt.

Unntaket i personopplysningsloven § 23 for opplysninger i interne dokumenter er utformet etter modell av forvaltningslovens innsynsbestemmelser. Tilsvarende unntak finnes også i offentlighetsloven. I [NOU 2003: 30 kapittel 10.2.2](#) er arten av opplysningene, at det er opplysninger med usikker kvalitet, trukket frem som sentral i begrunnelsen for unntaket. Videre gjelder unntaksregelen «tekst som er utarbeidet for den interne saksforberedelse». Det er altså bruken i intern saksforberedelse som er avgjørende, ikke hvor de finnes. I den grad departementets tolkning er korrekt, antar vi at også unntakene i forvaltningsloven og offentlighetsloven må vurderes på nytt.

Behovet for unntak

Justisdepartementet mener at begrensningen i innsynet som unntaket representerer i mange tilfeller vil kunne favne videre enn det som kan anses nødvendig og proporsjonalt. Finans Norge deler ikke denne oppfatningen.

De samme kjennetegnene ved interne dokumenter som beskrives ovenfor gjør seg gjeldende for interne notater i banker og forsikringsforetak. Interne opplysninger som omfattes av dagens unntak kan typisk være at kundebehandleren underveis gjør notater som kan tjene som nyttig informasjon senere i saksbehandlingen. Dette kan for eksempel være et notat om påfallende atferd i en kundesamtale, men som ikke alene er tilstrekkelig til å begrunne unntak fra innsyn på grunn av mistanke om straffbart forhold eller at avsløringsforbudet i hvitvaskingsloven får anvendelse. Et annet eksempel er at det noteres ned tegn på at rettslig handleevne kan være redusert, på et tidspunkt hvor det ikke er grunnlag for å konkludere. Det kan også være opplysninger som ligger tett opptil taushetsplikt om forretningsmessige forhold. Dette er avveininger som det vil være uforholdsmessig arbeidskrevende å foreta i forbindelse med registrering av opplysningene, eller ved innsynsbegjæringer.

Vi finner også grunn til å peke på andre praktiske konsekvenser av å ikke videreføre et unntak for opplysninger i interne dokumenter. Ved en begjæring om innsyn må selskapet gå gjennom alle interne dokumenter manuelt for å vurdere hvilke opplysninger det kan gis innsyn i. Dette vil være en kostnadskrevende prosess og vil øke risikoen for at

taushetsbelagte opplysninger og vurderinger kommer på avveien. I tillegg vil det være en risiko for at vurderinger som i dag lagres forblir muntlige slik at de i ettertid ikke kan etterspores. Dette er i strid med forordningens prinsipp om integritet og fortrolighet, samt prinsippet om gjennomsiktighet.

En utvidet innsynsrett i forhold til dagens rettstilstand kan ha negativ betydning for tilliten til finansforetakene. I enkelte type saker, for eksempel ansvarsforsikringer, vil forsikringsforetakene registrere personopplysninger om en kravstiller som ikke nødvendigvis er kunde i selskapet. Kravstillerens interesse vil ofte stå i motsetning til forsikringstakers (kundens) interesser. En innsynsrett for kravstiller i selskapets interne vurderinger av for eksempel skyldforhold, vil derfor kunne være uheldig for tillitsforholdet mellom selskap og kunde.

Av betydning for proporsjonalitetsvurderingen vil Finans Norge bemerke at unntaket kun gjelder opplysninger i tekst som er utarbeidet for den interne saksforberedelse hos den behandlingsansvarlige, og at unntaket ikke lenger gjelder dersom opplysningen deles. Vi understreker også at behandlingen av opplysningene hos den behandlingsansvarlige er underlagt de generelle prinsippene for behandling av personopplysninger, herunder prinsippene om formålsbegrensning, relevans, lagringsbegrensning, integritet og fortrolighet. Finans Norge mener derfor de grunnleggende rettighetene og frihetene ivaretas på tross av unntaket og at unntaket både er nødvendig og forholdsmessig.

Det fremgår av forarbeidene til personopplysningsloven § 23 at unntaket «dels er praktisk begrunnet, og dels forankret i hensyn som underbygger unntaksreglene i offentlighetsloven § 5 første ledd og forvaltningsloven § 18 annet ledd første punktum», Ot. Prp. 92 (1998-1999) s. 121. Finans Norge mener denne vurdering fortsatt er gyldig, og tilsier at unntaket for opplysninger i interne dokumenter bør videreføres. For bank og forsikringsforetak er unntaket av reell praktisk betydning.

Finans Norge ber på denne bakgrunn Justisdepartementet videreføre dagens unntak i personopplysningsloven § 23 første ledd f.

12.3.3 Korrigering, sletting og begrensning av behandling

Retten til begrensning

Retten til begrensning av behandlingen er en ny rettighet som innføres ved forordningen. Det er uklart hvilken rekkevidde bestemmelsen har.

Den aktuelle bestemmelsen er ikke primært myntet på finansnæringen og kan medføre utfordringer. Dersom en bankkunde skal kunne kreve begrensning i behandlingen, ved for eksempel en uenighet om saldo på en konto, kan det stilles spørsmål ved om banken skal

være avskåret fra videre behandling av disse opplysningene inntil uenigheten er avklart. Dette vil i ytterste konsekvens bety at den registrertes konto og kort også må sperres for å unngå ytterligere behandling av personopplysningene forårsaket av kundens kortbruk eller lignende, at omstridte poster må trekkes ut ved skatterapportering mv. Slike konsekvenser for både kunden og banken ser ikke ut til å være vurdert av lovgiver og det må avklares hvorvidt det i et tilfelle som nevnt vil være tilstrekkelig å «fryse» et øyeblikksbilde av den omtvistede saldo og forutgående transaksjoner som grunnlag for de diskusjoner som partene skal ha – uten å stoppe all behandling av personopplysninger.

Tilsvarende gjelder for forsikringsvirksomhet. Behandlingen av personopplysningene kan ikke stanses midlertidig uten konsekvenser for leveransen av forsikringstjenestene og gjennomføring av pålagte risikoberegninger, premieberegning og myndighetsrapportering.

Forordningen artikkel 18 nr. 2 tillater likevel behandling for «å fastsette, gjøre gjeldende eller forsvare rettskrav eller for å verne en annen fysisk eller juridisk persons rettigheter eller av hensyn til viktige samfunnsinteresser i Unionen eller en medlemsstat». Finans Norge antar at unntaket må forstås slik at retten til begrensning har liten praktisk betydning der behandlingen skjer på grunnlag av en gjensidige forpliktende avtale med en kunde, jf. artikkel 6 bokstav b, og der behandlingen skjer som følge av en rettslig forpliktelse, jf. artikkel 6 bokstav c. Eksempelvis bør en begjæring om begrenset behandling ikke påvirke et finansforetaks anledning til å forfølge et pengekrav, eller plikten til å utføre myndighetsrapportering og risikoberegninger. Dersom Justisdepartementet er av en annen oppfatning må unntak i medhold av artikkel 23 vurderes.

12.2.4 Retten til dataportabilitet

Høringsnotatet behandler ikke de sentrale problemstillinger som retten til dataportabilitet reiser. Det vises i stor grad til Artikkel 29-gruppens guidelines, som drøfter spørsmål rundt informasjonssikkerhet/identitetskontroll, hvilke personopplysninger som omfattes samt hvordan etterlevelse skal skje. I motsetning til PSD2-regelverket, gis det imidlertid ikke noen nærmere avgrensninger for hvor langt tilbake i tid retten til dataportabilitet strekker seg. I og med at retten ikke bare omfatter personopplysninger gitt av den registrerte, men også omfatter personopplysninger generert ved bruk av tjenester, vil omfanget innenfor eksempelvis bank bli svært stort i og med at transaksjonsopplysninger fra konto og kortbruk antas omfattet. Finans Norge mener at det å måtte legge til rette for portering av så store datamengder til den registrerte også innebærer en stor personvernrisiko, i og med at dette vil bli lagret på den registrertes private lagringsmedier. De uklare rammene for omfanget av dataportabilitet og personvernkonsekvensene av å gi den registrerte en slik generell rett, bør etter Finans Norges oppfatning utredes og konkretiseres nærmere av departementet og/eller Datatilsynet.

12.2.5 Innsigelsesrett

Innsigelsesrett

Finans Norge deler departementets forståelse av at artikkel 21 representerer en innsigelsesrett (opt-out rett) for den registrerte ved behandlingsaktiviteter som har sitt behandlingsgrunnlag i artikkel 6 nr 1, bokstav e «allmenn interesse» og bokstav f «berettiget interesse».

Tydelighet rundt dette er viktig, slik at det ikke oppstår uklarheter om hvorvidt innsigelsesretten etter artikkel 21 innebærer et krav om samtykke til å behandle personopplysninger til profilering slik det er blitt hevdet fra ulike hold. Det er også viktig at det er tydelig at denne reservasjonsretten ikke gjelder for behandlinger etter øvrige behandlingsgrunnlag, så som behandling med grunnlag i avtale, lov eller samtykke (artikkel 6 nr 1, bokstav a, b og c).

Artikkel 21, nr 2 og 3 stadfester en særlig rett til å kunne reservere seg mot behandling av personopplysninger til direkte markedsføring, som må anses som likeartet med den plikt en virksomhet har til å ha et internt reservasjonsregister etter markedsføringsloven § 12.

12.2.6 Automatiserte individuelle avgjørelser

Generelt

Finans Norge deler departementets forståelse av at artikkel 22 i stor grad er en videreføring av gjeldende rett. Også her er det grunn til å presisere at heller ikke artikkel 22 gir grunnlag for å hevde at det foreligger krav til forutgående samtykke for å gjennomføre automatisert behandling, herunder profilering.

Særlig om automatiserte avgjørelser av kredittsøknader

Finansnæringen benytter en rekke automatiserte prosesser og automatiserte avgjørelser per i dag og utviklingen innen næringen tilsier at dette vil øke i omfang og fortsatt være viktig i tiden fremover.

Etter artikkel 22 nr. 1 har den registrerte «rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende». Dette gjelder imidlertid etter artikkel 22 nr. 2 ikke dersom den automatiserte avgjørelsen er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og behandlingsansvarlig, dersom den automatiserte avgjørelsen er tillatt etter gjeldende rett eller dersom det foreligger uttrykkelig samtykke fra den registrerte. Dersom den automatiserte avgjørelsen er utført for å oppfylle avtale med den registrerte eller basert på samtykke er det et vilkår i artikkel 22 nr. 3 om at den registrerte skal ha rett til manuell behandling, til å uttrykke sine synspunkter og til å motsette seg avgjørelsen. For øvrig

bemerket vi at artikkel 22 nr. 3 og 4 er formulert på en måte som gjør det problematisk å forstå bestemmelsens omfang.

I fortalen punkt 71 vises det eksplisitt til automatisk avslag på en søknad om kreditt. Etter vår vurdering må imidlertid en søknad på kreditt kunne behandles automatisk etter artikkel 22 nr. 2 bokstav b. Hensynet til den registrertes personvern ivaretas gjennom at den registrerte har rett til innsyn i beslutningsgrunnlaget og retten til menneskelig inngripen etter artikkel 22 nr. 3.

Finansinstitusjoner fastsetter interne retningslinjer for behandling av kredittsøknader, blant annet for en forutsigbar og objektiv bedømmelse. Disse retningslinjene baserer seg i stor grad på lovpålagte plikter. Blant annet følger det av finansavtaleloven kapittel 3 at finansforetak plikter å vurdere en rekke forhold i forbindelse med kreditt, særlig søkerens kredittverdighet. Med bakgrunn i disse vurderingene fastsetter finansinstitusjonen en intern policy basert på risikoavveininger. Dersom søkeren ikke oppfyller vilkårene i den interne policyen avslås søknaden om kreditt.

Automatiserte avgjørelser er svært treffsikre og kostnadseffektive og medføre mer konsistente avgjørelser. Resultatet for kredittsøkeren vil være det samme uavhengig av hvorvidt behandlingen er automatisert eller foretas manuelt all den tid den baserer seg på det samme datagrunnlaget. Samtykke er heller ikke hensiktsmessig all den tid behandlingsgrunnlaget for kredittvurderingen er artikkel 6 nr. 1 bokstav c.

Særlig om kollektive avtaler

Etter ordlyden i artikkel 22 nr. 2 bokstav a er automatiserte avgjørelser tillatt dersom avgjørelsen «er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og en behandlingsansvarlig». Ordlyden tilsier at bestemmelsen kun får anvendelse på kontrakter mellom behandlingsansvarlige og den registrerte. Kollektive forsikringsavtaler inngås mellom et forsikringsselskap og typisk en forening, organisasjon eller bedrift og faller etter ordlyden utenfor. Dersom bestemmelsen skal forstås dithen at eksempelvis kollektive avtaler faller utenfor anvendelsesområdet vil dette få uheldige konsekvenser ved at saksbehandlingen for kollektive forsikringsavtaler ikke kan automatiseres selv om det i prinsippet ikke er noen forskjell på hvilke personopplysninger som behandles ved skadeoppgjør under henholdsvis kollektive og individuelle forsikringsavtaler. Etter Finans Norges syn bør det etableres en nasjonal lovhjemmel som, forutsatt at forordningens øvrige vilkår er oppfylt, tillater automatiserte behandlinger av kollektive avtaler.

Som redegjort for over er fagforeningsopplysninger en sensitiv personopplysning etter forordningen og vi anmoder om at unntaket som følger av dagens forsikringskonsesjon videreføres i lov eller forskrift. Kollektive forsikringsavtaler hvor fagforeningen inngår avtalen

vil være aktuelle for automatiserte avgjørelser. Etter forordningen artikkel 22 nr. 4 kreves det imidlertid samtykke fra den registrerte for automatiserte avgjørelser og profilering på sensitive personopplysninger. Også her bør det etter vår vurdering fastsettes en videreføring av dagens konsesjon slik at fagforeningsopplysninger kan være gjenstand for automatiserte avgjørelser og profilering.

For øvrig viser vi til vårt høringssvar til ny hvitvaskingslov hvor vi påpeker at profilering og automatiske avgjørelser er viktig for finansforetaks arbeid for å forhindre hvitvasking og terrorfinansiering og at det derfor er viktig at hvitvaskingsloven gir tilstrekkelige hjemler for slike behandlinger etter personvernforordningen.

Kapittel 13 – behandlingsansvarlig og databehandler

13.6 Underretning av tilsynsmyndigheter og den registrerte ved brudd på personopplysningssikkerheten

Departementet ber om innspill til forslaget til unntak fra plikten til å underrette den registrerte, jf. høringsnotatet pkt. 13.6.3 og lovforslaget § 13 fjerde ledd.

Finans Norge støtter forslaget som etter vår vurdering er en videreføring av personopplysningsloven § 23 bokstav b. Bestemmelsen er viktig for finansforetaks anledning til å avdekke blant annet bedragerier. Dersom den registrerte får innsyn i disse opplysningene medfører dette en stor risiko for eksempelvis at den registrerte forspiller bevis.

13.7 Vurdering av personvernkonsekvenser

Departementet etterspør synspunkter på hvorvidt det bør være en plikt til vurdering av personvernkonsekvenser også i de tilfeller som omfattes av unntaksregelen i artikkel 35 nr. 10, som omfatter tilfeller der behandling har hjemmel i lov eller i unionsretten.

Etter Finans Norges vurdering bør ikke unntaket som følger av artikkel 35 nr. 10 fjernes. For finansforetak, som er pålagt en rekke behandlinger av personopplysninger gjennom lovgivning, er dette unntaket svært viktig. Et praktisk eksempel er der finansforetak må innhente en rekke personopplysninger fra kunder for å ivareta sine forpliktelser etter hvitvaskingsloven. Vurderingen av personvernkonsekvenser i slike tilfeller må etter Finans Norges syn være en oppgave for lovgiver. Rekkevidden av unntaksregelen kan etter vår vurdering avklares gjennom dialog og veiledninger fra tilsynsmyndighetene all den tid dette vil være relativt standardiserte behandlinger.

13.8 Forhåndsdrøftinger med tilsynsmyndighetene

I høringsnotatet gir departementet en beskrivelse av når det skal gjennomføres forhåndsdrøftelser med Datatilsynet i pkt. 13.8.2; «Dette medfører at Datatilsynet vil måtte

gjennomføre forhåndsdrøftinger i alle tilfeller der behandlingen kan medføre en høy risiko for personvernet, og dermed kunne legge føringer for hvilke risikoreducerende tiltak som skal settes i verk».

Formuleringen kan forstås dithen at departementet legger til grunn at det skal gjennomføres forhåndsdrøftelser der hvor det foreligger høy risiko etter artikkel 35, også i de tilfeller der den behandlingsansvarlige har satt i gang tiltak som har fjernet risikoen. Dersom departementets beskrivelse skal forstås slik, finner vi grunn til å påpeke at dette vil medføre et stort antall forhåndsdrøftelser med Datatilsynet da nedslagsfeltet for artikkel 36 blir betydelig.

En slik forståelse er etter Finans Norge oppfatning ikke i samsvar med forordningen artikkel 36 nr. 1, jf. også fortalens avsnitt 84 siste setning og avsnitt 94. Vi antar at fortolkningen kan ha en viss sammenheng med oversettelsen av artikkel 36 nr. 1 hvor det i den norske oversettelsen fremgår «Den behandlingsansvarlige skal rådføre seg med tilsynsmyndighetene før behandlingen dersom en vurdering av personvernkonsekvenser i henhold til artikkel 35 tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.» (Vår understreking)

I den engelske versjonen er terskelen for når forhåndsdrøftelse skal finne sted langt tydeligere beskrevet; «in the absence of measures». Det samme kan sies om den danske versjonen; «...at behandlingen vil føre til høj risiko i mangel af foranstaltninger».

Finans Norge legger til grunn at plikten til forhåndsdrøftelser inntreffer der hvor risikoen for personvernet er høy og hvor den behandlingsansvarlige ikke har truffet tiltak som reduserer risikoen til et akseptabelt nivå. Vi anmoder departementet om å klargjøre dette og justere ordlyden i artikkel 36 nr. 1 tilsvarende.

13.9 Atferdsnormer

Finans Norge har ingen bemerkninger til departementets beskrivelse av atferdsnormer. Finans Norge vil imidlertid påpeke at vi er positive til utviklingen av atferdsnormer og vil ta initiativ til at det utarbeides for våre medlemmers behandling av personopplysninger.

Kapittel 14 – Personvernrådgiver

Særskilt om personvernrådgiverbegrepet

Departementet foreslår å innføre begrepet «personvernrådgiver», blant annet for å signalisere at ordningen utvides vesentlig sammenlignet med den eksisterende ordningen «personvernombud». Departementet viser i sin begrunnelse til politiregisterloven ved sitt valg av begrep i forbindelse med gjennomføringen av Direktiv (EU) 2016/680 om beskyttelse

av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner.

Finans Norge erkjenner at dagens begrep (personvernombud) kan være utvannet, dels fordi oppgavene den enkelte virksomhet tillegger ordningen i form av ansvar og oppgaver synes å variere fra virksomhet til virksomhet. Dette synliggjøres ved at flere virksomheter ikke har søkt om unntak fra meldeplikten etter personopplysningsloven § 7-12 for etablerte personvernombud. Et annet moment er at dagens ordning er frivillig.

Overgangen til personvernforordningens Data Protection Officer (DPO) innebærer et markant skifte for rollens uavhengighet, ressurstilgang, krav til personlige egenskaper, faglige kvalifikasjonskrav og tilgang til ledelsen. Ordningen blir dessuten lovpålagt for en rekke virksomheter, herunder mange virksomheter innen finansnæringen. Endringen medfører etter vårt syn at flere av virksomhetene som har etablert personvernombud etter dagens regelverk må endre sin interne organisering for å tilfredsstille personvernforordningens krav til DPO.

Finans Norge er likevel kritisk til begrepet som er foreslått.

Etter alminnelig begrepsbruk er en rådgiver en person som gir sine overordnede råd og adlyder instruks, eksempelvis en kunderådgiver i finansforetak. En begrepsbruk som det legges opp til i lovforslaget tydeliggjør ikke tilstrekkelig det ansvar og uavhengighet som ligger i rollen. Artikkel 29-gruppen er i sin veileder tydelig på at det må tas grep for å forhindre misforståelser og uklarhet rundt DPOs rolle og tittel.

DPO har etter Direktiv (EU) 2016/680, som ligger til grunn for de foreslåtte endringer i politiregisterloven og politiregisterforskriften, en betydelig svakere rolle enn den som følger av personvernforordningen. Blant annet kan denne instrueres i utførelsen av sine oppgaver, har ikke stillingsvern og rapporterer ikke til høyere ledelsesnivå. Ved å bruke et begrep som beskriver en rolle som avviker markant fra det som følger av forordningen, oppnår man ikke den signaleffekten som er formålet med navneendringen.

Finans Norge ber derfor at departementet utreder nærmere hva en passende tittel for funksjonen, som ivaretar ansvaret og uavhengigheten, bør være.

Personvernrådgivers taushetsplikt

Finans Norge støtter i hovedsak forslaget til bestemmelse om personvernrådgivers taushetsplikt, men ser at det kan stilles spørsmål ved hvor langt rådgivers plikt til å «hindre» at andre får kjennskap til «enkeltpersoners varsling» er ment å gå. For en rådgiver som er ansatt direkte i virksomheten, vil det normalt være virksomheten som utstyrer rådgiveren med e-postadresse, telefon og andre kommunikasjonskanaler som rådgiveren behøver for å

utøve sitt virke. Vi legger til grunn at rådgiveren kan basere seg på å motta varsler via slike kanaler og at rådgivers plikt til å hindre at andre får kjennskap til varslerens identitet først inntreffer ved mottak av varselet.

Kapittel 15 – Melde- og konsesjonsplikt

Konsesjonsplikt

Finans Norge støtter departementet i at konsesjonsplikten i gjeldende lov ikke videreføres.

Vi vil særlig peke på at forordningen artikkel 36 nr. 5 kun åpner for konsesjonsplikt hvor hjemmelen for behandlingen er å utføre en oppgave i «allmennhetens interesse». Dette må leses som en referanse til artikkel 6.nr. 1 e første alternativ. Etter vår erfaring er dette et lite praktisk hjemmelsgrunnlag for finansforetakenes behandlinger. En eventuell konsesjon under ny forordning vil derfor ha et meget begrenset anvendelsesområde.

Finans Norge mener at en videreføring av det gjeldende konsesjonsregimet vil være i strid med forutsetningene i forordningen. Forordningen innfører en rekke plikter og virkemidler for å ivareta personvernet, særlig plikten til å foreta en vurdering av personvernkonsekvensene etter artikkel 35 og plikten til forhåndsdrøftelse etter artikkel 36. Atferdsnormer vil også kunne bidra til å ivareta personvernet, og vi antar at det vil tas initiativ til atferdsnormer på de dominerende samfunnsområdene. Disse nye mekanismene vil etter vårt syn bidra til at personvernet er godt ivaretatt uten konsesjonsplikt.

For finansnæringen kan fortsatt konsesjonsplikt også medføre en betydelig konkurranseulempe. Erfaring har vist at konsesjonsprosessen kan medføre forsinkelser ved lanseringen av nye tjenester. Dersom andre aktører på området ikke er underlagt konsesjon for tilsvarende tjenester, vil en konsesjonsplikt være en betydelig trussel mot norske finansforetaks konkurranseevne sammenlignet med andre aktører som eksempelvis fintech. Tilsvarende kan restriktive føringer i konsesjoner også innebære at det ikke oppnås harmonisering og like konkurransevilkår innenfor EU. Dette er særlig viktig for finansforetak med grensekryssende virksomhet. Samtidig erkjenner vi at det kan være behandlinger som utføres med hjemmel i artikkel 6 nr. 1 e første alternativ hvor det er behov for en regulering gjennom konsesjon. Vi er derfor positive til den foreslåtte forskriftshjemmelen.

Gjeldende konsesjoner - overgangsregler

Finans Norge vil, som nevnt over, ta initiativ til at det utarbeides atferdsnormer for finansnæringen. Vår målsetning er at disse skal være på plass og godkjent så tidlig som mulig etter forordningens ikrafttredelse. Så fort atferdsnormene er godkjente vil det etter vår vurdering ikke være behov for konsesjoner, ei heller i en overgangsperiode. Utarbeidelse av atferdsnormer krever imidlertid et visst samarbeid med Datatilsynet, idet Datatilsynet skal godkjenne og publisere atferdsnormene. Det er følgelig viktig for Finans Norge at

Datatilsynet prioriterer og har tilstrekkelig kapasitet til å arbeide med atferdsnormer i tiden fremover. Eventuelle overgangsregler for gjeldende konsesjoner bør følgelig gjelde i en kort periode og kun frem til atferdsnormene er godkjente av Datatilsynet.

En mulig videreføring av eksisterende konsesjoner i en overgangsperiode reiser imidlertid noen spørsmål. Fortalens avsnitt 171 åpner kun for å videreføre «godkjenninger» gitt av nasjonale tilsynsmyndigheter. Formuleringen er plassert i et avsnitt som omhandler frister for å bringe pågående behandlinger i samsvar med forordningen. Både ordlyd og kontekst tilsier at intensjonen kun har vært å tillate at behandlinger som er i strid med forordningen kan fortsette i en overgangsperiode. Vi kan ikke se at det er grunnlag for en tolkning som åpner for å videreføre vilkår i konsesjonene som medfører strengere begrensninger enn det som følger av forordningen. En slik tolkning vil også være i strid med forordningens generelle mål om totalharmonisering, jf. fortalens avsnitt 13, for å sikre like forutsetninger for alle virksomheter innen EU og EØS. Dette må etter vår vurdering medføre at dersom den behandlingsansvarlige kan dokumentere at behandlingen er i samsvar med forordningen, vil eventuelle ytterligere begrensninger i konsesjonene være ugyldige.

Kapittel 35 – Regler om innsyn i e-postkasse mv.

Finans Norge er enig med departementet i at det er behov for å videreføre de norske reglene om arbeidsgivers innsyn i e-postkasse mv. Reglene gir forutberegnelighet for arbeidsgiver og arbeidstaker når det gjelder vilkår for og fremgangsmåte ved innsyn.

Departementet etterspør syn på utkastet til bestemmelser om arbeidsgivers innsyn i e-postkasse mv, særlig om bestemmelsene også skal gjelde for innsyn i aktivitetslogg. Finans Norge slutter seg til Advokatforeningen uttalelse om at tittelen som er valgt for disse bestemmelsene er utdaterte sett i lys av den teknologiske utviklingen og at bestemmelsene vil gjelde for mer enn tradisjonelle e-postkasser.

Aktivitetslogger bør etter Finans Norges syn omfattes av reglene om innsyn i e-postkasse under forutsetning av at hensikten med innsyn er av samme art som ved innsyn i e-postkasse eller arbeidstakers personlige mapper.

Kapittel 38 – Økonomiske og administrative konsekvenser

Departementet peker i høringsnotatet på at gjeldende personopplysningsregelverk i betydelig grad videreføres og at selv der pliktene i noen grad endres vil det neppe medføre betydelige økonomiske eller administrative konsekvenser.

Etter Finans Norges syn må det forventes betydelige økonomiske og administrative konsekvenser som følge av flere endrede og nye krav etter forordningen. Forordningens krav om personvernkonsekvensutredning, innføring av nye tiltak som sikrer innebygd personvern,

dataportabilitet og endring av eksisterende IT-systemer vil alene medføre betydelige økonomiske og administrative kostnader, i tillegg kommer blant annet endring av dokumentasjon, gjennomgang, endring av databehandleravtaler m.m. og ansettelse av personvernrådgiver. For finansnæringen antas det å beløpe seg til flere hundre millioner.

Med vennlig hilsen

Finans Norge

sign.

Idar Kreutzer

administrerende direktør

sign.

Evy Ann Hagen

direktør og advokat