Personvernkommisjonen v/Ingvild
Næss

Dato: 25.06.2021
Vår ref.:
Deres ref.:

# Innspill til personvernkommisjonen

## 1. Innledning

Finans Norge viser til kontakt med Ingvild Næss om muligheten for å gi innspill til personvernkommisjonen. På vegne av våre medlemmer benytter vi denne muligheten til å gi innspill om hva kommisjonen bør fokusere på i sitt arbeid. Nedenfor redegjør vi for noen utvalgte personvernrelevante problemstillinger finansbransjen erfarer og står overfor, sett fra vårt ståsted.

## 2. Tillit i en digital tidsalder

Det er viktig at vi har en digital økonomi som alle har tillit til. Tillit oppnår vi ved å være åpne om hvordan vi behandler personopplysninger, ved å kommunisere til rett tid og i rett kontekst, samt ved å kommunisere på en forståelig måte ved bruk av klart og enkelt språk. Å gjennomføre dette i praksis er krevende - selv med de beste intensjoner. Konsekvensen kan være at tilliten til den digitale økonomien synker dersom vi ikke lykkes med å være tilstrekkelig transparente i hvordan vi kommuniserer med de registrerte.

Spanske Caixa-bank fikk nylig bot fra det spanske datatilsynet for måten banken gir informasjon til sine kunder på.[1] Informasjonen som ble gitt til de registrerte ble kritisert av tilsynsmyndigheten, blant annet fordi tilsynet fant at informasjonen ikke var forståelig for kundene. Banken hadde altså gitt informasjon, men hadde ikke lyktes i å gjøre det på en tilfredsstillende måte.

Personvernforordningen stiller klare krav til hvilken informasjon som må gis, og når den skal gis, men regelverket sier lite om hvordan informasjonen skal gis. Ansvaret for å finne en passende måte å gi informasjon på påhviler de behandlingsansvarlige. Det hadde like fullt vært til hjelp om myndighetene kunne bidra med mer praktisk veiledning/verktøy som virksomhetene kunne støtte seg på i slike vurderinger, noe som vil kunne bidra til å sikre en mer ensartet praksis. Finans Norge oppfordrer personvernkommisjonen til å adressere behovet for enda tydeligere anbefalinger fra myndighetene om *hvordan* de behandlingsansvarlige bør informere.

Det er videre et spørsmål om hvordan vi kan sikre god forståelse hos de registrerte, herunder hvordan de registrerte kan oppnå en bedre selvbestemmelse og kontroll over egne personopplysninger på

[1] https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank_en



Hansteens gt. 2 ● Telefon 23 28 42 00 ● firmapost@finansnorge.no ● PB 2473, 0202 Oslo ● Org.nr. 994 970 925 ● finansnorge.no

generelt grunnlag. I denne forbindelse er det relevant å trekke frem uklarheter knyttet til anvendelsen av ekomloven og forhåndssamtykke i nettleser til å sette cookies, samt det å benytte berettiget interesse for markedsføring som behandlingsgrunnlag for behandlingsaktivitetene. Her spriker praksisen blant norske virksomheter. Vi håper kommisjonen vil se nærmere på denne problemstillingen i sitt arbeid.

## 3. Samhandling offentlig-privat sektor/teknologi som en utfordrer til lovhjemlet utlevering av personopplysninger

Det er for tiden et høyt fokus på effektivisering og digitalisering av samhandlingen mellom offentlig sektor og finanssektoren, herunder automatisering av offentlige etaters innhenting av informasjon fra finansforetak. Det er tidvis uklart hvorvidt underliggende regelverk er utformet på en måte som tar høyde for en overgang fra en "manuell" til automatisert innhenting, og som ivaretar de nødvendige rettsikkerhetsgarantier, vurdering av personvernkonsekvenser og øvrige krav i henhold til personvernregelverket, for eksempel i henhold til personvernforordningen artikkel 6 nr. 3 og 35 nr. 10.

Det er en rekke ulike initiativ til effektivisering og digitalisering, på tvers av ulike offentlige etater og underliggende regelverk. Dette gjør det utfordrende å etablere en samlet tilnærming til hvordan ulike regelverk skal vurderes og eventuelt utvikles, med henblikk på å legge til rette for løsninger som ivaretar interessene til både offentlig sektor, finanssektoren og den registrerte.

Finans Norge oppfordrer kommisjonen til å løfte denne problemstillingen på prinsipielt grunnlag. I dag bruker en rekke aktører som er involvert mye ressurser, i det de henvises til å gjennomføre de nødvendige prosesser hver for seg. Det blir mye unødig og tidkrevende dobbeltarbeid, med fare for en fragmentert regelverksforståelse og praksis. Dette kunne vært unngått dersom problemstillingene hadde vært avklart på mer prinsipielt grunnlag, samlet for alle involverte i digitaliseringsprosjekter.

Når formålet er utlevering av personopplysninger fra finansnæringen til kontrollformål i offentlig sektor, er det viktig at legalitetsprinsippet vurderes grundig, og at den nødvendige demokratiske prosessen ivaretas på en forsvarlig måte. Videre er det en fordel med en samlet og overordnet vurdering fra lovgiver av personvernkonsekvenser, for eksempel i henhold til personvernforordningen artikkel 35 nr. 10. Finans Norge har erfaring med at finansnæringen settes i en krevende posisjon i slike prosjekter. Vi savner at denne problemstillingen adresseres på en helhetlig måte, og ikke bare prosjektbasert fra gang til gang. Temaet henger tett sammen med lovgivers vurdering av personvernkonsekvenser i lovarbeidet som omtales nedenfor.

## 4. Personvernhensyn må ivaretas bedre ved ny og sektorspesifikk lovgivning

Finansnæringen erfarer at forholdet mellom ny lovgivning og reglene om personvern i personvernforordningen gjennomgående får for lite oppmerksomhet, og at nødvendige vurderinger i den forbindelse ofte er for svake i utredningsarbeidet. Finansnæringen er underlagt svært mange lovpålagte forpliktelser som medfører at en må behandle personopplysninger, for eksempel i henhold til finansforetaksloven.

Finans Norge ser gjentatte eksempler på at det ikke er tilstrekkelig klart hvilke personopplysninger som kan behandles med rettslig forpliktelse som behandlingsgrunnlag, og hva som er klar nok

lovhjemmel for utlevering, for å nevne noe. Hjemler for informasjonsplikt er videre gjennomgående lite tilfredsstillende uformet. Ved behandling av særlige kategorier av personopplysninger, som ofte er nødvendig for forsikringsforetak å behandle, er det spesielt viktig at det går klart frem av særlovgivningen at dette er tillatt. Finansnæringen erfarer at det tidvis kan være utfordrende å etablere et lovlig grunnlag i henhold til kravene i personvernforordningen artikkel 9, selv om kundeavtalene forutsetter at slike særlige kategorier av personopplysninger behandles. Dette fører igjen til mye unødig tolkningstvil. Når lovgiver ikke gjør nødvendige vurderinger av personvernet, må jobben gjøres av de mange private og offentlige aktørene. Dette er en lite samfunnsøkonomisk tilnærming, igjen med fare for en fragmentert praksis.

Det er viktig at lovgivningen som utarbeides er teknologinøytral. Vår erfaring er at personvernregelverket, til tross for at det er utformet med tanke på at det skal være teknologinøytralt, ofte slår ulikt ut avhengig av teknologien (middel) som benyttes for behandlingen. Midler som benyttes av behandlingsansvarlig ved oppfyllelsen av lovpålagte forpliktelser er eksempelvis sjelden vurdert eller hensyntatt av lovgiver. Som et eksempel kan vi nevne at det ved gjennomføring av kundetiltak i henhold til hvitvaskingsloven vil være naturlig, og antagelig nødvendig, å benytte digitale analyseverktøy. Tilsvarende kan det være aktuelt å benytte API'er for overføring av opplysninger i henhold til offentlige etaters hjemler for tilgang til taushetsbelagte opplysninger, uten at dette er tidligere vurdert i lovgivningsprosessene, ref. omtalen i punkt 3 ovenfor.

Personvernkonsekvenser er sjelden behandlet på en grundig nok måte i lovgivningsprosesser, noe som fører til at alle behandlingsansvarlige virksomheter selv må gjennomføre en slik krevende prosess. Dette kunne vært unngått om lovgiver gjennomførte de nødvendige vurderingene. Vi ser behov for at utredningsinstruksen oppdateres, særskilt med tanke på utredning av personvernkonsekvenser og den erfaringen som er kommet etter innføringen av personvernforordningen[2]. Et eksempel fra nyere tid er den nye hvitvaskingsloven som ikke i tilstrekkelig grad gjennomfører personvernkonsekvensvurderinger av de enkelte behandlingsaktivitetene som finansforetak må gjennomføre. Det bør være et større fokus og krav til at personvernkonsekvenser skal utredes ved ethvert lovgivningsarbeid enn det som er praksis i dag. Dette vil bedre samsvare med forpliktelsene som personvernforordningen også pålegger myndighetene.

## 5. Eksisterende lovgivning

Finans Norge vil også nevne at manglende hjemmel for opphevelse av sektorspesifikk taushetsplikt for forskningsformål er en utfordring for finansnæringen. Personvernforordningen tilrettelegger for forskning, og angir at forskningsformål på gitte vilkår kan anses som formålsforenlig. For finansforetak er dette likevel ikke nok, da taushetspliktsreglene hindrer utlevering av data til eksterne virksomheter som ikke er oppdragstakere.

Hva kan gjøres med eksisterende lovgivning, og som vi i de senere årene har erfart at fungerer dårlig i samspill med personvernforordningen? Bør byrden bæres av de ulike aktørene og enkeltindividene, eller kan det være en idé med en slags «lovdugnad», hvor det tas noen grep som kan bidra til å gjøre en del lover mer effektive - til glede for både individene og virksomhetene?

[2] Vurdering av personvernkonsekvenser - regjeringen.no

## 6. Automatisert behandling/kunstig intelligens

Det er stadig mer fokus på at automatiserte behandlinger og bruk av kunstig intelligens (KI) utfordrer personvernet. Datatilsynet har opprettet en regulatorisk sandkasse for bruk av kunstig intelligens. EU-kommisjonen kom nylig med et forslag om lovgivning av KI, som blant annet fokuserer på krav om risikostyring, teknisk dokumentasjon, data governance, åpenhet, at mennesker følger opp løsningene, logging med mer. Det legges også opp til krav om sertifiseringer av løsningene.

Personvernforordningen har en egen bestemmelse om automatiserte avgjørelser i personvernforordningen artikkel 22. Finansnæringen opplever at bestemmelsen er vanskelig tilgjengelig og utfordrende å anvende i praksis. Bestemmelsen får ikke anvendelse for de tilfeller som enten delvis er en del av en manuell behandling, eller ikke kan sies å være en avgjørelse som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker den registrerte. Det er derfor en rekke tilfeller av automatisert behandling som ikke faller innenfor vilkårene i personvernforordningen artikkel 22. Vi er av den oppfatning at bestemmelsen ikke synes å fungere helt etter sin hensikt. Grunnen er at mange automatiserte behandlinger, som kan utgjøre en ekstra personvernrisiko i flere tilfeller, faller utenfor reglene som er ment å hensynta den risiko som automatisert behandling kan utgjøre.

Personvernrisikoen som profilering og bruk av kunstig intelligens utgjør, og nødvendige mitigerende tiltak, vil riktignok fanges opp i en personvernkonsekvensvurdering for behandlinger med høy personvernrisiko. Men det er ikke slik at all behandling fordrer en slik konsekvensvurdering. Hvordan sikre at enkeltpersoner forstår hvordan personopplysninger behandles og hvorfor utfallet ble som det ble? Hvordan sikre at ingen diskrimineres i slike prosesser? I tillegg til å se utfordringene fra enkeltpersoners hold, er det behov for praktisk veiledning til virksomhetene.

## 7. Teknologi og sikkerhet

Den internasjonale standarden for hva som er tilfredsstillende informasjonssikkerhet etter personvernforordningen artikkel 32 er blitt meget høy. Finansnæringen er opptatt av å ivareta god informasjonssikkerhet, og vil antagelig overoppfylle informasjonssikkerhetskravene til tider ettersom vi også er underlagt krav i henhold til IKT-forskriften og europeiske krav til finansregulatorisk virksomhet. Finansnæringen savner imidlertid føringer for når informasjonssikkerheten må heves, og når den kan senkes.

Taushetsplikten kan være et effektivt organisatorisk tiltak som påvirker behovet for øvrige sikkerhetsmessige tiltak. Dette kan for eksempel gjelde ved konsernintern overføring av personopplysninger, eller der man har en særskilt tillit til den tredjepart man samhandler med, eksempelvis samhandling med et annet finansforetak.

Finansforetak er underlagt særskilte krav om at informasjonen ikke skal være for vanskelig tilgjengelig for tredjeparter,[3] samtidig som personopplysningene kanskje ikke har begrenset beskyttelsesverdi som personvernforordningen artikkel 32 legger opp til i en risikobasert tilnærming, hvor elementer som art, formål og sammenheng spiller inn i vurderingen, samt «state of the art»-vurderinger. Finansforetak pålegges i tillegg et i særklasse høyere krav til tillit og informasjonssikkerhet grunnet

[3] Iht. PSD2-krav mv.

den lovpålagte taushetsplikten som gjelder for kundeopplysninger. Vi skulle likevel sett at lovgiver ga klarere veiledning rundt nivået som kreves, særlig når det gjelder samhandling med tredjeparter og myndigheter, og lovpålagte krav til deling av kundeopplysninger.

## 8. Øvrige innspill

### 8.1 Tredjelandsoverførsler

Schrems II har skapt et krevende vakuum for virksomhetene ved at Privacy Shield ble satt til side med umiddelbar effekt, samtidig som virksomhetene i stor grad er avhengige av løsninger i tredjeland og det i liten grad finnes europeiske leverandører som kan tilby alternative løsninger med tilsvarende funksjonalitet. Situasjonen er krevende og lite praktisk i den forstand at den enkelte virksomhet må gjøre komplekse vurderinger av beskyttelsesnivået i tredjeland. Dette er vurderinger som EU-kommisjonen i praksis bruker flere år på. Kravet representerer en risiko for feilvurderinger/utilstrekkelige vurderinger, som også kan innebære en risiko for kunders, ansattes og andre registrertes personopplysninger. Finans Norge savner en nasjonal felles oppfølging av Schrems II, som både omfatter offentlige og private aktører.[4]

### 8.2 Opphopning av personopplysninger hos store IT-leverandører

Mange norske (finans)foretak benytter de samme internasjonale (sky-)tjenesteleverandører, som for eksempel AWS, Microsoft og Oracle. Her lagres blant annet opplysninger om ansatte, kunder, virksomheten m.m. Det kan være ønskelig med en vurdering av om en slik opphopning av personopplysninger hos store IT-leverandører i seg selv representerer en risiko for personvernet, herunder for tilgjengelighet og kontinuitet i tjenestene til skade/ulempe for kunder, ansatte og andre registrerte, i tillegg til virksomheten selv.

Med vennlig hilsen
**Finans Norge**

Nils Henrik Heen
Advokat/Juridisk direktør

Linda Solstad
Juridisk seniorrådgiver

[4] Se f.eks. initiativ i Tyskland og Sverige: https://www.euractiv.com/section/digital/news/germany-to-set-up-bundescloud/ og https://computersweden.idg.se/2.2683/1.750415/tunga-myndigheter-nobbar-teams