Justitsministeriet
Slotsholmsgade 10
1216 København K
Att.: Mikkel Reenberg
Sendt pr. mail til: jm@jm.dk og mir@jm.dk

FINANS DANMARK

Høringssvar fra Finans Danmark vedrørende national evaluering af databeskyttelsesreglerne

Høringssvar

9. oktober 2020
Dok: FIDA-1826564804-690718-v1
Kontakt Mette Ravn

A. Indledning

Som led i Justitsministeriets nationale evaluering af databeskyttelsesreglerne iværksatte ministeriet den 10. juni 2020 en offentlig høring af relevante interessenter. Formålet med høringen er at belyse, i hvilke situationer der i praksis opleves tvivl om databeskyttelsesreglerne, og fristen for afgivelse af bemærkninger er den 10. oktober 2020.

Finans Danmark takker for muligheden for at bidrage til den nationale evaluering. Vi har i høringsperioden indsamlet en lang række praktiske eksempler på udfordringer i den finansielle sektor, som alle er indsat i Justitsministeriets skema til brug for erfaringsindsamling (afsnit C).

Som følge af den finansielle sektors betydning for samfundsøkonomien er de finansielle virksomheder underlagt en mere omfattende regulering end sædvanlige erhvervsvirksomheder. Finans Danmark er interesseorganisation for bank, realkredit, kapitalforvaltning, værdipapirhandel og investeringsfonde i Danmark, og medlemsvirksomhederne agerer i en kompleks virkelighed med et fintmasket net af regulering. Det betyder alt andet lige, at de databeskyttelsesretlige udfordringer i sektoren er mere komplekse end i andre sektorer.

Samtidig har den finansielle sektor en lang tradition for compliancearbejde, og sektorens tilgang til implementering af databeskyttelsesforordningen har været præget af samme grundighed og systematik, som kendes fra andre compliance-områder. Finans Danmarks medlemsvirksomheder har siden 2016 investeret mange økonomiske ressourcer i arbejdet med at implementere GDPR, og medlemmerne investerer fortsat meget tid i den løbende regelefterlevelse. Denne

modenhed i implementeringen bidrager også til, at de databeskyttelsesretlige udfordringer bliver mere komplekse.

I forbindelse med evalueringsprocessen er det derfor væsentligt, at Justitsministeriet er opmærksom på, at der er stor forskel på de databeskyttelsesretlige udfordringer i forskellige sektorer – og at udfordringerne bliver mere komplekse, når der er tale om en i forvejen tæt reguleret sektor som den finansielle sektor.

Finans Danmark savner generelt mere fokus på den finansielle sektors udfordringer og ser gerne, at Justitsministeriet i evalueringsprocessen dedikerer et særligt spor til den finansielle sektor – og især til håndtering af de komplekse samspilsproblemer, som er beskrevet nedenfor i afsnit B.

Disposition

Som ovenfor nævnt er de databeskyttelsesretlige udfordringer i den finansielle sektor komplekse, og nogle af problemerne lader sig ikke let beskrive i skemaform.

Høringssvaret er derfor disponeret således, at de særlige samspilsproblemer mellem GDPR og den finansielle EU-lovgivning er udførligt beskrevet i afsnit B, og ligeledes medtaget mere kortfattet i skemaet i afsnit C.

B. Særlig problemstilling: Samspilsproblemer mellem GDPR og den finansielle EU-lovgivning

Som følge af den finansielle sektors betydning for samfundsøkonomien er de finansielle virksomheder underlagt mere omfattende lovgivning end sædvanlige erhvervsvirksomheder. Langt størstedelen af denne lovgivning stammer fra EU.

Ud over en lang række generelle situationer, hvor der i praksis opleves tvivl om databeskyttelsesreglerne, har den finansielle sektor således også en særlig kategori af udfordringer, som alle bunder i samspilsproblemer mellem GDPR og den finansielle EU-lovgivning.

Samspilsproblemerne er komplekse, og det er derfor fundet hensigtsmæssigt med en uddybende beskrivelse af konkrete udfordringer i denne kategori. Nedenfor beskrives således fem konkrete samspilsproblemer, som også mere kortfattet er medtaget i skemaet til erfaringsindsamling (skemaets punkt 1a-1e).

1. Introduktion til samspilsproblemerne

På en række områder er der krydsfelter mellem GDPR og andre regler i den finansielle særlovgivning, som stiller krav om, at finansielle virksomheder behandler

persondata. Det betyder i praksis, at virksomhederne i flere tilfælde er usikre på, om det er kravene i GDPR eller den finansielle særlovgivning, som er gældende i den specifikke situation. I nogle tilfælde er det oplevelsen, at det ikke er muligt at efterleve begge regelsæt samtidig. Derfor er der behov for en afklaring af, hvordan reglerne spiller sammen.

Den finansielle særlovgivning stammer i overvejende grad fra EU. Som eksempler på EU-regelsæt (og heraf følgende dansk implementering), hvor der er komplicerede samspilsproblemer med GDPR, kan nævnes:

- Fjerde og femte hvidvaskdirektiv, implementeret i hvidvaskloven,
- MiFID II-direktivet, som blandt andet er implementeret i lov om finansiel virksomhed og tilhørende bekendtgørelser, herunder bekendtgørelsen om de organisatoriske krav til værdipapirhandlere,
- Kapitalkravsforordningen, CRR, og
- Andet betalingstjenestedirektiv, PSD2, implementeret i lov om betalinger

Listen er ikke udtømmende, idet det dog er samspillet mellem GDPR og hvidvaskreglerne, som lige nu fylder meget i en dansk kontekst.

Grunden til, at samspilsproblemerne opstår og udfordrer implementeringen af GDPR i den finansielle sektor, er, at der ligger forskellige hensyn bag de forskellige regelsæt.

Hensynet bag GDPR er beskyttelse af individet mod andres uberettigede behandling af personlige data. Det er imidlertid ikke dette beskyttelseshensyn, som i første række ligger bag reglerne om behandling af persondata i de ovenfor nævnte EU-regelsæt. Tværtimod er det bærende hensyn bag **hvidvaskdirektivet** at forebygge hvidvask af penge og finansiering af terrorisme; det bærende hensyn bag **MiFID II-direktivet** er blandt andet at styrke beskyttelsen af investorer og øge de finansielle markeders sikkerhed og effektivitet; det bærende hensyn bag **kapitalkravsforordningen** er at sikre den finansielle stabilitet i EU, og det bærende hensyn bag **PSD2-direktivet** er at fremme konkurrence på betalingsområdet ved at pålægge bankerne at åbne for adgangen til forbrugernes betalingskonti og tilknyttede betalingsdata.

De konkrete samspilsproblemer på det finansielle område er nedenfor inddelt i fem tilfældegrupper a)-e), som illustrerer kompleksiteten i de overvejelser, der skal foretages:

a) EU-lovgivningen generelt: Samspilsproblemer ved valg af behandlingshjemmel

Databeskyttelsesforordningen indeholder en række grundlæggende krav, som enhver behandling af personoplysninger skal overholde. Det drejer sig blandt andet om, at den dataansvarlige skal sikre, at personoplysninger indsamles til udtrykkeligt angivne og legitime formål, og at oplysningerne ikke efterfølgende viderebehandles på en måde, som er uforenelig med disse formål.

Netop her opstår udfordringen i forhold til behandling af personoplysninger med hjemmel i den finansielle særlovgivning, når og hvis hjemlen i særlovgivningen ikke er klar og præcis nok til entydigt at fastslå forpligtelsernes omfang og rækkevidde. Det gælder fx omfanget af personoplysninger, der skal indhentes som led i kundekendskabsprocedurer efter hvidvasklovens § 11 og de oplysninger, der skal opbevares efter hvidvasklovens § 30.

Her skal den dataansvarlige finansielle virksomhed populært sagt oplysning for oplysning selv vurdere, om behandling kan ske med hjemmel i artikel 6, stk. 1, litra c, om retlig forpligtelse (*"behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige"*).

Viser det sig efterfølgende, at den dataansvarlige har fortolket særlovgivningen for vidtgående og behandlet **flere oplysninger**, end behandlingshjemlen i artikel 6, stk. 1, litra c, tillader, vil der umiddelbart – medmindre andre behandlingsgrundlag finder anvendelse – mangle hjemmel til persondatabehandlingen under GDPR.

Omvendt i tilfælde hvor den dataansvarlige vurderer, at der ikke er en decideret retlig forpligtelse til den pågældende databehandling, men at denne databehandling er formålstjenlig for det resultat, der tilstræbes med særlovgivningen, eksempelvis at forebygge hvidvask af penge og finansiering af terrorisme. I sådanne tilfælde er den dataansvarlige nødsaget til at anvende artikel 6, stk. 1, litra f, som behandlingsgrundlag (*"behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse…"*), hvilket med andre ord betyder, at den dataansvarlige er nødsaget til at foretage en kompleks legitim interesseafvejning, fordi der ligger andre hensyn bag hvidvaskreglerne (og de øvrige ovenfor nævnte EU-regelsæt) end individets interesser.

b) Hvidvaskdirektivets område: Samspilsproblemer ved indsigtsanmodninger

Hvidvasklovens § 30 indeholder en meget vidtgående opbevaringsregel, hvorefter oplysninger, dokumenter og registreringer skal opbevares i mindst fem år efter kundeforholdets ophør eller en enkeltstående transaktions gennemførelse, idet

personoplysninger dog skal slettes 5 år efter forretningsforbindelsens ophør eller en enkeltstående transaktions gennemførelse.

Det er ikke usædvanligt, at bankkunder er kunder samme sted i en livsalder, og hvidvasklovens § 30 kan derfor føre til ekstremt lange opbevaringsperioder. Hvis kunden forbliver hos samme bank i en livsalder, kan opbevaringsperioden for personoplysninger strække sig over 70 år eller mere. Der er således markant forskel på omfanget af databehandling afhængigt af, om kunderne løbende skifter bank eller forbliver hos samme bank i en livsalder.

En opbevaringsperiode, som strækker sig over mange årtier, giver særlige udfordringer i forhold til de registreredes rettigheder. Herunder ikke mindst i forhold til indsigtsanmodninger, hvor det er uafklaret, om årtier gamle transaktionsdata og kontoudtog kan undtages fra retten til indsigt, eller om indsigt skal gives i det samlede datamateriale gennem en livsalder. Det gamle datamateriale vil i langt de fleste tilfælde befinde sig under lås og slå på et datawarehouse, da det er materiale, som ikke længere aktivt anvendes, men som alene opbevares med det formål at hjælpe myndighederne med at opklare hvidvask af penge og finansiering af terrorisme.

c) Hvidvaskdirektivets område: Samspilsproblemer ved efterlevelse af principperne om dataminimering og opbevaringsbegrænsning

Det følger af dataminimeringsprincippet i GDPR art. 5, stk. 1, litra c, at den dataansvarlige skal sikre, at de oplysninger, som behandles, er tilstrækkelige, relevante og *"begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles"*. Derudover må det i henhold til princippet om opbevaringsbegrænsning ikke være muligt *"at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles"*, jf. GDPR art. 5, stk. 1, litra e.

Også i relation til disse principper er der udfordringer i forhold til den finansielle særlovgivning, hvis den dataansvarlige selvstændigt skal vurdere nødvendigheden af særlovenes opbevaringskrav i forhold til formålene bag reguleringen, eller hvis den dataansvarlige – hvilket er tilfældet på hvidvaskområdet – kan blive mødt med, at tredjelande som USA stiller krav om endnu længere opbevaringsperioder.

Hvidvasklovens § 30 indeholder som ovenfor nævnt en – for langvarige kundeforhold – meget vidtgående opbevaringsregel, hvorefter personoplysninger skal slettes fem år efter kundeforholdets ophør eller en enkeltstående transaktions gennemførelse.

Samspilsproblemerne mellem denne regel og principperne i GDPR art. 5, stk. 1, litra c, og GDPR art. 5, stk. 1, litra e, giver anledning til en række komplekse udfordringer i sektoren, hvor følgende tilfældegrupper kan fremdrages til illustration:

- Kautionister og pantsættere: Skal banken opbevare oplysninger på kautionisten, indtil låntager ophører som kunde?
- Tidligere ægtefæller: Hvordan efterleves dataminimeringsprincippet for den fraskilte part, der ophører som kunde i banken (når den anden ægtefælle forbliver kunde)?
- Fuldmagtsforhold: Kræver dispositionsfuldmagter henholdsvis forespørgselsfuldmagter differentierede sletteregler?

d) MiFID II-direktivets område: Samspilsproblemer ved efterlevelse af principperne om dataminimering og opbevaringsbegrænsning

På MiFID II-direktivets område er record-keeping kravet i § 10, i bekendtgørelsen om de organisatoriske krav til værdipapirhandlere[1] en særlig udfordring. Det gælder særligt den bødesanktionerede regel i bekendtgørelsens § 10, stk. 5, jf. stk. 10, hvorefter al telefonkommunikation med nye og eksisterende kunder, *"der fører til eller kan føre til transaktioner"* skal optages. Optagelserne skal værdipapirhandleren opbevare i minimum fem år, og hvis Finanstilsynet anmoder herom, skal optagelserne opbevares i indtil syv år.

Hvis det ikke kan udelukkes, at et telefonopkald vil blive omfattet af MiFID II-kravet, skal samtalen formentlig optages (jf. formuleringen: *"der fører til eller kan føre til transaktioner"*). Viser det sig efterfølgende, at der alligevel ikke var tale om en MiFID II-samtale, savnes der vejledning om, hvorledes der skal forholdes med den nu optagne samtale? Bibeholder samtalen sin karakter af en samtale, *"der fører til eller kan føre til transaktioner"*? Og hvis ja, skal samtales så opbevares i minimum fem år i overensstemmelse med bekendtgørelsens § 10? Eller ændrer samtalen karakter til en samtale, som nu falder uden for MiFID II-kravet, og derfor i henhold til GDPR skal slettes?

Det er sjældent muligt på forhånd at forudse, hvordan en telefonsamtale med nye eller eksisterende kunder udvikler sig, og definitionen på en optagelsespligtig samtale: *"der fører til eller kan føre til transaktioner"* åbner for komplicerede fortolkningsspørgsmål i relation til samspillet med GDPR's principper om dataminimering og opbevaringsbegrænsning.

[1] BEK nr. 921 af 26/06/2017

e) Kapitalkravsforordningens område: Samspilsproblemer ved efterlevelse af principperne om dataminimering og opbevaringsbegrænsning

Nogle kreditinstitutter behandler personhenførbare data til brug for udvikling og drift af interne ratingbaserede modeller (IRB) til opgørelse af kapitalkrav til institutternes kreditrisici. IRB-modellerne reguleres af kapitalkravsforordningen (CRR), der sammen med en række RTS'er og guidelines stiller krav om og opstiller retningslinjer for, hvilke oplysninger modellerne skal være baseret på, ligesom grundlaget for modellerne skal kunne valideres og revideres. Som følge af disse krav er kreditinstitutterne forpligtet til at opbevare en række oplysninger på et så detaljeret niveau, at oplysningerne er personhenførbare.

Institutterne skal løbende vurdere, hvilke oplysninger de skal opbevare, detaljeringsgrad, periode etc. for at leve op til kravene i den finansielle regulering uden samtidig at overtræde principperne om dataminimering og opbevaringsbegrænsning, og der efterspørges i høj grad vejledning om disse komplekse EU-samspilsproblemer. Dette ikke mindst henset til kreditmodellers eksplorative natur, hvor det ikke er muligt på forhånd at kategorisere, hvilke oplysninger der måtte være relevante. En oplysning, der ikke er relevant i 2020, kan fx vise sig relevant i 2025.

Som eksempler på artikler i kapitalkravsforordningen, hvorom vejledning på EU-niveau er påkrævet, kan følgende eksempler på lange – i nogle tilfælde endog meget lange – opbevaringsperioder fremhæves:

- Artikel 180 om særlige krav vedrørende sandsynlighed for misligholdelse (PD)-estimater, hvorefter, i henhold til stk. 1, litra h, den underliggende historiske observationsperiode skal *"strække sig over mindst fem år for mindst én kilde."* Hvilket suppleres af et krav om, at: *"Hvis den omhandlede observationsperiode strækker sig over længere tid for en kilde, og de pågældende data er relevante, anvendes den lange periode."*

- Artikel 185 om validering af interne estimater, hvorefter sammenligningerne i henhold til litra b, *"skal baseres på historiske data, som går så langt tilbage i tiden som muligt"*, og institutternes interne vurderinger af deres ratingsystemers funktion i henhold til litra c, *"skal baseres på den længst mulige periode"*.

C. Skema til brug for erfaringsindsamling

Nedenstående skema belyser situationer, hvor der blandt Finans Danmarks medlemmer er tvivl om fortolkningen af databeskyttelsesreglerne:

Konkret beskrivelse af problemstillingen	Hvilken regel knytter problemstillingen sig til?	Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?	Har problemstillingen været drøftet med en DPO? Hvad blev resultatet af drøftelsen?
SAMSPILSPROBLEMER			
1a. EU-lovgivningen generelt: Samspilsproblemer ved valg af behandlingshjemmel	GDPR art. 6(1)(c) over for GDPR art. 6(1)(f)	Samspilsproblemer ved valg af behandlingshjemmel kan ikke løses lokalt af den enkelte finansielle virksomhed. Det er en myndighedsopgave (i) at sikre bedre vejledning om de komplicerede sammenhænge mellem GDPR og eksisterende regler i den finansielle EU-lovgivning, som stiller krav om, at finansielle virksomheder behandler persondata, samt (ii) fremadrettet at arbejde for en bedre sammenhæng mellem reglerne, så der ikke er tvivl om, hvorledes de modstridende beskyttelseshensyn skal vægtes. Fremadrettet er det påkrævet, at GDPR nøje indtænkes, når danske myndigheder forhandler nye forordnings- og direktivforslag på det finansielle område, og når ny finansiel regulering fra EU implementeres i dansk ret.	Ja. Hver enkelt case er en konkret vurdering. I de tilfælde, hvor hjemlen i den finansielle særlovgivning ikke er klar og præcis nok til entydigt at fastslå forpligtelsens omfang og rækkevidde, er det ikke altid muligt at efterleve GDPR og særlovgivningen på samme tid. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 adresseret samme problemstilling (GDPR 13: Behov for bedre sammenhæng mellem GDPR og finansiel EU-lovgivning), og Justitsministeriet har, uden at gå i detaljer med de komplekse problemer, svaret, at man er enig i, at samspillet mellem GDPR og den finansielle EU-regulering kan give anledning til fortolkningstvivl.
1b. Hvidvaskdirektivets område: Samspilsproblemer ved indsigtsanmodninger	GDPR art. 15	Samspilsproblemer i forhold til indsigtsanmodninger kan ikke løses lokalt af den enkelte finansielle virksomhed. Det er en myndighedsopgave at forene de modstridende beskyttelseshensyn (beskyttelse af individet over for samfundets interesse i at modvirke hvidvask af penge og finansiering af terrorisme) og sikre en rimelig afvejning af finansielle virksomheders ressourceforbrug over for individets ret til indsigt i materiale, som kan have en opbevaringsperiode på 70 år eller mere, og som befinder sig under lås og slå på et datawarehouse.	Ja. Manuel rutine i mangel af bedre. Der savnes konkret vejledning om samspillet mellem hvidvasklovens § 30 og de registreredes ret til indsigt. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 adresseret samme problemstilling (GDPR 13: Behov for bedre sammenhæng mellem GDPR og finansiel EU-lovgivning), og Justitsministeriet har, uden at gå i detaljer med de komplekse problemer, svaret, at man er enig i, at samspillet mellem GDPR og den finansielle EU-regulering kan give anledning til fortolkningstvivl.

1c. Hvidvaskdirektivets område: Samspilsproblemer ved efterlevelse af principperne om dataminimering og opbevaringsbegrænsning	GDPR art. 5(1)(c) og GDPR art. 5(1)(e)	Samspilsproblemer ved efterlevelse af GDPR art. 5(1)(c) og 5(1)(e) kan ikke løses lokalt af den enkelte finansielle virksomhed. Det er en myndighedsopgave at vejlede bedre om sammenhængen mellem GDPR og hvidvasklovens opbevaringsregler. Vejledningsbehovet er ikke begrænset til hvidvasklovens § 30, men behovet for vejledning opstår særlig hyppigt i relation til § 30, hvor følgende tilfælde kan fremdrages til illustration: - Kautionister og pantsættere: Skal banken opbevare oplysninger på kautionisten, indtil låntager ophører som kunde? - Tidligere ægtefæller: Hvordan efterleves dataminimeringsprincippet for den fraskilte part, der ophører som kunde i banken (når den anden ægtefælle forbliver kunde)? - Fuldmagtsforhold: Kræver dispositionsfuldmagter henholdsvis forespørgselsfuldmagter differentierede sletteregler?	Ja. Hver enkelt case er en konkret vurdering. Der savnes konkret vejledning om sletning i løbende kundeforhold. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 adresseret samme problemstilling (GDPR 13: Behov for bedre sammenhæng mellem GDPR og finansiel EU-lovgivning), og Justitsministeriet har, uden at gå i detaljer med de komplekse problemer, svaret, at man er enig i, at samspillet mellem GDPR og den finansielle EU-regulering kan give anledning til fortolkningstvivl.
1d. MiFID II-direktivets område: Samspilsproblemer ved efterlevelse af principperne om dataminimering og opbevaringsbegrænsning	GDPR art. 5(1)(c) og GDPR art. 5(1)(e)	Samspilsproblemer ved efterlevelse af GDPR art. 5(1)(c) og 5(1)(e) kan ikke løses lokalt af den enkelte finansielle virksomhed. Det er en myndighedsopgave at vejlede bedre om sammenhængen mellem GDPR og MiFID II-direktivets opbevaringsregler, herunder (i) hvilke telefonsamtaler der **ikke** skal optages, (ii) hvilke telefonsamtaler der skal optages og straks derefter slettes, og (iii) hvilke telefonsamtaler der skal optages og gemmes i fem/syv år. Det er sjældent muligt på forhånd at forudse, hvordan en telefonsamtale med nye eller eksisterende kunder udvikler sig, og definitionen på en optagelsespligtig samtale: *"der fører til eller kan føre til transaktioner"* åbner for komplicerede fortolkningsspørgsmål i relation til samspillet med GDPR's principper om dataminimering og opbevaringsbegrænsning.	Ja. Drøftelserne om bedste model for optagelse af telefonsamtaler pågår. Udfordringen er, at lovgivningen kræver, at alle telefonsamtaler: *"der fører til eller kan føre til transaktioner"* skal optages, samtidig med at principperne i GDPR art. 5(1)(c) og 5(1)(e) skal efterleves. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 adresseret samme problemstilling (GDPR 13: Behov for bedre sammenhæng mellem GDPR og finansiel EU-lovgivning), og Justitsministeriet har, uden at gå i detaljer med de komplekse problemer, svaret, at man er enig i, at samspillet mellem GDPR og den finansielle EU-regulering kan give anledning til fortolkningstvivl.
1e. Kapitalkravsforordningens område: Samspilsproblemer ved efterlevelse af principperne om dataminimering og opbevaringsbegrænsning	GDPR art. 5(1)(c) og GDPR art. 5(1)(e)	Samspilsproblemer ved efterlevelse af GDPR art. 5(1)(c) og 5(1)(e) kan ikke løses lokalt af den enkelte finansielle virksomhed. Det er en myndighedsopgave at vejlede bedre om sammenhængen mellem GDPR og kapitalkravsforordningen og forene de modstridende beskyttelseshensyn bag disse to forordninger (beskyttelse af individet over for hensynet til at sikre den finansielle stabilitet i EU).	Ja. Der savnes konkret vejledning. Principperne i GDPR art. 5(1)(c) og 5(1)(e) er vanskeligt forenelige med kravene i kapitalkravsforordningen,

		I lyset af den finansielle sektors betydning for samfundsøkonomien er det påkrævet, at medlemsstaternes nationale finanstilsyn inddrages i dette vejledningsarbejde. Konsekvenserne ved at slette IRB-data kan være uoverskuelige, og der efterspørges en klar udmelding om, at sektoren kan fortsætte som hidtil med at opbevare og anvende de indsamlede IRB-data (til de formål, hvortil de er indsamlet).	herunder kapitalkravsforordningens artikel 180(1)(h), artikel 185(b) og artikel 185(c). Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 adresseret samme problemstilling (GDPR 13: Behov for bedre sammenhæng mellem GDPR og finansiel EU-lovgivning), og Justitsministeriet har, uden at gå i detaljer med de komplekse problemer, svaret, at man er enig i, at samspillet mellem GDPR og anden finansiel EU-regulering kan give anledning til fortolkningstvivl.
PRINCIPPER FOR BEHANDLING AF PERSONOPLYSNINGER			
2. Viderebehandling til andet formål – hvor går uforenelighedsgrænsen?	GDPR art. 5(1)(b) og GDPR art. 6(4) og GDPR art. 9	Det følger af GDPR art. 5(1)(b), at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må *"viderebehandles på en måde, der er uforenelig med disse formål"*. I praksis er denne grænse svær at drage. Som eksempel fra det finansielle område kan nævnes indsamling og behandling af transaktionsoplysninger med hjemmel i betalingsloven. Visse af sådanne transaktionsoplysninger (særligt kundens faste, månedlige udgifter og herunder faste, månedlige fagforeningskontingenter) er også relevante i forbindelse med rådgivning og budgetlægning. Hvor går uforenelighedsgrænsen i sådanne tilfælde?	Ja. Der indhentes samtykke, hvis betalingsoplysninger bruges som led i rådgivning/budgetlægning. Dette sker ud fra et forsigtighedsprincip, men er det også nødvendigt ud fra en hjemmelsbetragtning?
3. Viderebehandling til statistiske formål	GDPR art. 5(1)(b) og GDPR art. 5(1)(e)	Der savnes konkret vejledning/fortolkningsbidrag til definitionen af "viderebehandling til statistiske formål". Der er store samfundsmæssige gevinster forbundet med dataanalyse/business intelligence/big data m.v., hvilket aktualiserer behovet for vejledning på området.	Ja. Vejledning og fortolkningsbidrag savnes.
4. Dataminimeringsprincippet, når ikke-relevante persondata uanmodet oplyses i e-mails eller under telefonsamtaler	GDPR art. 5(1)(c)	I praksis sker det ofte, at ikke-relevante persondata uanmodet modtages via e-mails eller oplyses under telefonsamtaler, som der er pligt til at optage og gemme i henhold til MiFID II-direktivet. Man kan og bør opfordre til, at kunden ikke indsender flere oplysninger end nødvendigt, men dette kan ikke altid styres. Den store udfordring er, at det påvirker integriteten af materialet, hvis de overflødige data slettes/skal slettes, ligesom det kan være særdeles vanskeligt at slette uddrag af telefonsamtaler.	Ja. Overflødige data skal slettes, men frygten er, at det i tilfælde af konflikt kan få konsekvenser, at originalmaterialet er ændret.
5. Generelle udfordringer i forhold til	GDPR art. 5(1)(e)	I praksis er det vanskeligt for de dataansvarlige at vurdere, hvad der udgør det rette tidsrum.	Ja.

principippet om opbevaringsbegrænsning		Hvilket tidsrum er hverken kortere eller længere, men præcis det rette, *"der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles"*?	Der efterspørges flere konkrete eksempler på, hvad der udgør en legitim opbevaringsperiode – i forhold til, hvad de registrerede kan forvente?
DE REGISTREREDES RETTIGHEDER			
6. Mere bevågenhed på undtagelser til indsigtsretten	GDPR art. 15 og DBL § 22, stk. 1	Når en nuværende eller tidligere kunde anmoder om indsigt, har den pågældende i mange tilfælde en klar forventning om, at banken skal udlevere kopi af **alt** materiale indeholdende den pågældendes personlige oplysninger. Dette er dog ikke korrekt. Der er således en række interne vurderinger (kreditvurderinger- og indstillinger, ejendomsvurderinger m.v.), der helt eller delvist kan undtages fra retten til indsigt. Det er imidlertid en vanskelig kommunikativ opgave for den dataansvarlige at oplyse om disse undtagelser. Samtidig er det byrdefuldt, at den dataansvarlige i hvert enkelt tilfælde skal foretage konkrete og individuelle vurderinger af undtagelsernes rækkevidde.	Ja. Der savnes specifik vejledning om rækkevidden af undtagelserne til indsigtsretten. Samtidig opfordres Datatilsynet til i sit generelle oplysningsarbejde at have mere bevågenhed på undtagelserne. Det bør ikke komme som en overraskelse for de registrerede, at indsigtsretten ikke er absolut.
7. Dataportabilitet	GDPR art. 20	Retten til dataportabilitet giver blandt andet den registrerede mulighed for at overføre sine personoplysninger fra én dataansvarlig til en anden. Personoplysningerne skal kunne flyttes, kopieres og overføres fra ét it-miljø til et andet uden hindring, hvis det er teknisk muligt. I praksis har den finansielle sektor endnu ikke haft mange henvendelser vedrørende dataportabilitet, men det vil være en udfordring, når og hvis de kommer.	Ja. Manuel rutine i mangel af bedre. Yderligere vejledning i forhold til praktisk håndtering – også branchespecifikt – vil være nyttig.
DATAANSVARLIG OG DATABEHANDLER			
8. Tilsyn med databehandlere og underdatabehandlere	GDPR art. 24 og 32	Når en finansiel virksomhed som dataansvarlig overlader behandling af personoplysninger til andre, skal virksomheden føre tilsyn med, at de indgåede aftaler overholdes, og at databehandlere (og underdatabehandlere) har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger. Dette er ikke altid en let opgave at løfte. Ikke alle it-leverandører er forberedt på, hvad den dataansvarliges kontrol indebærer, og mange mindre it-leverandører er ikke underlagt ekstern revision. I de tilfælde, hvor underleverandøren ikke er underlagt ekstern revision, rammer Datatilsynets og FSR's revisorerklæring om persondata, ISAE 3000, og revisorerklæringen om it-sikkerhed, ISAE 3402, ofte forbi målet, da det er omfattende og bekostelige erklæringer, som kun kan udarbejdes af godkendte revisorer. Datatilsynets "Vejledende tekst om tilsyn med databehandlere og underdatabehandlere" er et skridt på vejen, men teksten er ikke konkret nok og indeholder ingen konkrete eksempler.	Ja. Et udbygget sæt retningslinjer for, hvordan man i praksis kan påse behandlingssikkerheden, vil være nyttig i forbindelse med kontraktforhandlinger. Der savnes specifikt vejledning i forhold til: (i) mindre it-leverandører, der ikke er underlagt ekstern revision, samt (ii) hvordan man generelt som dataansvarlig gennemfører en tilfredsstillende kontrol. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 påpeget en lignende problemstilling (GDPR 7: Tjeklister og vejledninger til kontrol af databehandlere), og Rege-

			ringen har svaret, at en opdateret vejledning fra Datatilsynet forventes at kunne offentliggøres i 2. kvartal 2021.
9. Forholdet mellem den dataansvarlige og underdatabehandleren	GDPR art. 28. stk. 4	I forbindelse med outsourcing af aktiviteter, vil en databehandler som oftest gøre brug af mere end én underdatabehandler. GDPR art. 28, stk. 4, pålægger en databehandler, der gør brug af en anden databehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, at pålægge denne anden databehandler de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen mellem den dataansvarlige og databehandleren. Bestemmelsen tager imidlertid ikke højde for, at de aktiviteter, som underdatabehandleren udfører på vegne af databehandleren, kan divergere væsentligt fra den samlede aktivitet, der er outsourcet til databehandleren – både for så vidt angår selve behandlingsaktiviteterne, kategorierne af personoplysninger og dermed det samlede risikobillede. En operationel løsning – som samtidig sikrer efterlevelse af reglens formål – vil være, at databehandleren foretager en selvstændig risikovurdering af underdatabehandlerens aktiviteter med henblik på fastsættelse af tekniske og organisatoriske sikkerhedsforanstaltninger, hvorefter denne risikovurdering samt beskrivelse af sikkerhedsforanstaltningerne forelægges den dataansvarlige til godkendelse.	Ja. Udfordringen er, at GDPR art. 28, stk. 4, ikke gør det klart, om (i) de sikkerhedsforanstaltninger, der er vurderet nødvendige for at etablere de behandlingsaktiviteter, der er outsourcet, skal videreføres 1:1 også i forholdet mellem databehandleren og dennes underdatabehandlere, eller (ii) om den dataansvarlige i samarbejde med databehandleren kan foretage en konkret risikovurdering af underdatabehandlerens behandlingsaktiviteter, således at der fastsættes specifikke, konkrete sikkerhedsforanstaltninger for den enkelte underdatabehandlers aktiviteter. Der savnes svar på, om den beskrevne operationelle løsning – som sikrer efterlevelse af reglens formål – også vil blive set som efterlevelse af reglens bogstav.
10. Forhandling af databehandleraftaler (og aftaler om delt dataansvar) med internationale aktører, hvor styrkeforholdet mellem parterne er ulige	GDPR art. 26 og 28	Det er i praksis ikke muligt at forhandle individuelle databehandleraftaler – eller individuelle aftaler om delt dataansvar – med store internationale aktører. Som eksempler på sådanne aktører kan nævnes Microsoft og Facebook, men der findes mange andre, primært amerikanske, aktører, hvor tilsvarende udfordringer gør sig gældende. Både på dansk og europæisk niveau savnes der opmærksomhed på disse problemer, da dét at skrifte aktør ikke altid er en reel valgmulighed.	Ja. Visse initiativer er ikke iværksat på grund af disse udfordringer. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 påpeget en lignende problemstilling (GDPR 3: Udfordringer ved brug af cloud-tjenester), og Regeringen har svaret, at Datatilsynet i 2021 forventer at kunne offentliggøre en vejledning om cloudtjenester.
ANMELDELSE AF BRUD PÅ PERSONDATASIKKERHEDEN			
11. Minimumsgrænse for anmeldelse af simple databrud: Fokus på tab af fortrolighed og underretning af de registrerede	GDPR art. 33 og GDPR art. 34	Alle databrud skal anmeldes til Datatilsynet uden unødig forsinkelse og inden 72 timer, medmindre *"det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder"*, jf. GDPR art. 33. I henhold til betragtning 85 kan et brud, *"hvis det ikke håndteres på en passende og rettidig måde"*, påføre skade såsom *"tab af fortrolighed*	Ja. Der savnes vejledning om forståelsen af betragtning 85 (*"tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt"*) i forhold til vurderingen af, hvornår *"det er usandsynligt, at*

		for oplysninger, der er omfattet af tavshedspligt". Finansielle virksomheder er underlagt tavshedspligt i henhold til § 117 i lov om finansiel virksomhed, hvorfor alle ikke-offentligt tilgængelige oplysninger om kunder betragtes som fortrolige. I henhold til GDPR art. 34, skal den registrerede underrettes, såfremt bruddet indebærer høj risiko for fysiske personers rettigheder og frihedsrettigheder. Dette indebærer i praksis, at der skal underrettes om alle brud, medmindre forhold i art. 34, stk. 3, er til stede. Der er umiddelbart ingen holdepunkter for at lade vurderingen bero på de konkrete konsekvenser ved tabet af fortrolighed.	*bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder"*, jf. GDPR art. 33. Det ville lette GDPR-byrden, hvis **konsekvenserne** ved tab af fortrolighed kunne indgå i både vurderingen af pligten til at anmelde (art. 33) og i vurderingen af pligten til at underrette (art. 34) og/eller hvis der indføres en generel bagatelgrænse, således som Erhvervslivets EU- og Regelforum har foreslået i anbefalingskataloget af 22. juni 2020 (GDPR 6: Minimumsgrænse for anmeldelse af simple databrud til Datatilsynet), og som Regeringen har forpligtet sig til at undersøge.
KONSEKVENSANALYSE VEDRØRENDE DATABESKYTTELSE			
12. Ressourcetunge konsekvensanalyser	GDPR art. 35	Konsekvensanalyser er i praksis meget ressourcetunge at udarbejde. Den dataansvarlige skal i henhold til GDPR art. 35, stk. 9, indhente *"hvis det er relevant, de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling"*. Det er i praksis vanskeligt at afgøre, hvornår pligten i art. 35, stk. 9, finder anvendelse, og hvordan den faktisk skal efterleves. Herunder er det vanskeligt at afgøre, hvor meget information de registrerede eller deres repræsentanter skal modtage om den påtænkte behandling, ikke mindst henset til den dataansvarliges forretning (nye forretningsområder) og konkurrenceretlige position.	Ja.
KRAV OM FORUDGÅENDE TILLADELSE			
13. Nationale regler om advarselsregistre	GDPR art. 36, stk. 5 og DBL § 26, stk. 1, nr. 1	Det er i praksis kompliceret at kvalificere, hvornår et register er oprettet med det primære formål at: *"advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret"*. I Datatilsynets vejledning fra november 2019 er der derfor behov for at udbygge afsnit 1 ("Hvornår er der tale om et advarselsregister?") med flere konkrete eksempler.	Ja. Vejledningen bør udbygges med eksempler.
TREDJELANDSOVERFØRSLER			
14. Tredjelandsoverførsler i lyset af sag C-318/11, *Schrems II*.	GDPR art. 46	Dommen fastslår, at EU-Kommissionens SCCs fra 2010 fortsat er gyldige og derfor fortsat kan finde anvendelse på overførsler til tredjelande uden for EU.	Ja. Efter *Schrems II*-dommen kræver anvendelsen af SCCs

		Dommen fastslår imidlertid også, at eksportører af personoplysninger (dataansvarlige i EU), der anvender Kommissionens SCCs, sammen med importøren (den dataansvarlige eller databehandleren i et land uden for EU) skal foretage en konkret vurdering af, om lovgivningen i det land, personoplysningerne overføres til, muliggør, at importøren reelt kan efterleve de krav (fx efterlevelse af dataeksportørens instruks), der stilles i standardkontraktbestemmelserne. Denne vurdering kræver, at dataeksportøren har meget stor indsigt i importlandets lovgivning.	stor indsigt i importlandets lovgivning. Det er derfor ønskeligt med en konkret og operationel udmelding fra Datatilsynet/Det Europæiske Databeskyttelsesråd; gerne i form af en positiv (eller negativ) liste over lande/leverandører, der fremover kan overføres persondata til på grundlag af SCCs. Erhvervslivets EU- og Regelforum har i anbefalingskataloget af 22. juni 2020 også påpeget denne problemstilling (GDPR 4: Overførsel til tredjelande), hvor tilbagemeldingen fra Regeringen har været, at Datatilsynet i regi af Det Europæiske Databeskyttelsesråd er i gang med at analysere konsekvenserne af dommen.
DATATILSYNETS VIRKSOMHED			
15. Manglende transparens om Datatilsynets praksis, herunder hvilke sager der indstilles til bøde i det strafferetlige system	DBL § 33	Datatilsynet offentliggør på sin hjemmeside afgørelser truffet på baggrund af henholdsvis klager og tilsyn. Det er dog kun afgørelser, som skønnes at have principiel karakter og/eller vidererækkende betydning, som offentliggøres. Det er imidlertid også relevant at offentliggøre afgørelser, som ikke nødvendigvis har principiel karakter og/eller vidererækkende betydning. Det er især problematisk, at Datatilsynet ikke offentliggør alle sager, som indstilles til bøde i det strafferetlige system. Den manglende offentliggørelse gør det vanskeligt at få indblik i, hvad Datatilsynet (i indstillingen til anklagemyndigheden) har lagt vægt på ved fastsættelse af bødens størrelse. Når straffesagen er afsluttet, er det fortsat ikke offentligt tilgængeligt, hvordan bødens størrelse er beregnet (procent af omsætningen), og sagsbehandlingen ved politi og domstole er desværre ofte lang, hvilket yderligere medvirker til, at det er svært at skabe overblik over praksis i forhold til bødeniveau.	Ja. Det er hensigtsmæssigt, at Datatilsynet skaber yderligere transparens om sin afgørelsesvirksomhed, således som også Erhvervslivets EU- og Regelforum har foreslået i anbefalingskataloget af 22. juni 2020 (GDPR 2: Behov for større gennemsigtighed om Datatilsynets praksis), og som Regeringen har tilkendegivet at ville følge.

--oo0oo--

Justitsministeriet har ifølge procesplanen for den nationale evaluering iværksat en bred erfaringsindsamling med det formål at "kaste nærmere lys over de kon-

krete situationer, der ifølge interessenterne er uklare, når databeskyttelsesreglerne skal efterleves i praksis" samt at "formidle mulige løsninger og eventuel vejledning om konkrete problemstillinger".

Nærværende høringssvar har specifikt kastet lys over den finansielle sektors særlige udfordringer med en forhåbning om, at Justitsministeriet nu vil arbejde videre med sektorens særlige problemstillinger – meget gerne i et selvstændigt spor i den nationale evaluering.

For så vidt angår samspilsproblemerne mellem GDPR og den finansielle EU-lovgivning er udfordringerne ens for alle finansielle virksomheder i EU, hvorfor løsninger i sidste ende skal findes på EU-niveau, hvilket Justitsministeriet og Datatilsynet må hjælpe med at sikre. For så vidt angår de øvrige problemstillinger kan mange emner afhjælpes nationalt, hvilket forhåbentlig vil ske som en udløber af evalueringen.

Finans Danmark står naturligvis til rådighed for yderligere dialog, hvis bemærkningerne ovenfor giver anledning til spørgsmål eller kommentarer.

Med venlig hilsen

Mette Ravn
Direkte: 30161136
Mail: mra@fida.dk