

# Finans og Leasing

Interesseorganisation for danske finansieringsselskaber

Torveporten 2, 4. sal  
DK-2500 Valby  
Telefon: +45 27 36 90 19  
E-mail: [post@finansogleasing.dk](mailto:post@finansogleasing.dk)  
[www.finansogleasing.dk](http://www.finansogleasing.dk)  
CVR nr. 75 36 12 11

## Finanstilsynet

Att. Cecilie Sander Bernbom (sendt på mail til [ceb@ftnet.dk](mailto:ceb@ftnet.dk))

Århusgade 110

2100 København Ø

## Høringssvar vedr. udkast til vejledningen om hvidvaskloven jf. Finanstilsynets mail af 13. juli 2018

Tak for en god og konstruktiv dialog der har været omkring tilblivelsen af vejledningen. Det er meget positivt, at Finanstilsynet har givet sig tid til at inddrage branchen og afholdt en hel møderække for at gennemgå vejledningen side for side.

Der er dog enkelte ”udestående” som Finans og Leasing fortsat er uenige med tilsynet i og som vi fortsat ikke mener er blevet besvaret i den ellers udmærkede ovenfor beskrevne proces.

Vi henholder os i øvrigt til alle vores tidligere høringssvar i processen, men vil gentage nedenstående pointer:

### Vedr. NemID

Som det fremgår af udkastet til vejledningen sondres der mellem digitale signaturer/NemID i modsætning til andre kilder til kontrol af identitet herunder pas/kørekort.

Endvidere fremgår, at digitale signaturer/NemID kun anerkendes som eneste kontrolkilde til identitet ved ”begrænset” risiko. På side 56 nævnes NemID på linje med pas/kørekort/sundhedskort mv<sup>1</sup>., men på side 58-59 fremgår at:

*” NemID er en pålidelig og uafhængig kilde, men i de tilfælde, hvor der ikke kun er tale om begrænset risiko, vil det være nødvendigt for virksomheden at benytte sig af andre kontrolkilder eller mitigerende tiltag sammen med NemID for at kunne opnå tilstrækkeligt kendskab til kunden i forbindelse med gennemførelse af kundekendskabsproceduren.”*

Finans og Leasing er af den opfattelse, at der ikke er hjemmel i loven til at 1) sondre mellem digitale signaturer/NemID ift. andre kilder til kontrol af id-oplysninger og 2) at der ikke er hjemmel i loven til at fastsætte at digitale signaturer/NemID kun kan anvendes som eneste kontrol af id-oplysninger ved begrænset risiko.

---

<sup>1</sup> ”For fysiske personer kan kontrollen f.eks. bestå af opslag i CPR (Det Centrale Personregister), oplysninger fra SKAT, offentligt udstedte legitimationsdokumenter, som f.eks. pas, kørekort, NemID, legitimationskort, sundhedskort, dåbs- eller navneattest.”

# Finans og Leasing

Interesseorganisation for danske finansieringsselskaber

Det er Finans og Leasings opfattelse, at vejledningens afsnit om NemID skal ændres til følgende:

*"NemID er en pålidelig og uafhængig kilde, men i de tilfælde hvor ~~der er høj risiko~~ ~~der ikke kun er tale om begrænset risiko~~, vil det være nødvendigt for virksomheden at benytte sig af andre kontrolkilder eller mitigerende tiltag sammen med NemID" (s.62).*

Dette bygges på følgende 6 argumenter:

## 1) Digitale signaturer, herunder NemID anerkendes i loven på lige fod med pas/kørekort

Det er Finans og Leasings opfattelse, at den seneste hvidvasklov (vedtaget 2. juni 2018<sup>2</sup>) er teknologineutral i den forstand at digitale signaturer anerkendes på lige fod med analoge dokumenter (pas/kørekort) til kontrol af identitetsoplysninger. Dette bygges på følgende citater fra loven:

- 1) "Digitale signaturer" nævnes flere steder i loven/bemærkninger fuldt ud på linie med andre kilder til kontrol af id-oplysninger, herunder på følgende sider i lovbemærkningerne: s. 36, s. 99 (x2), s. 100, s. 133<sup>3</sup>.
  - a. S. 36 "Nye teknologier m.v. åbner mulighed for en lang række andre måder at kontrollere en kundes identitet på, f.eks. ved hjælp af elektroniske signaturer. Erhvervs- og Vækstministeriet vurderer derfor, at det skal fremgå tydeligt af hvidvaskloven, at en virksomhed eller person omfattet af lovforslaget skal kontrollere kundens identitetsoplysninger ved en uafhængig og pålidelig kilde, men at det ikke behøver at være kontrol i form af et identitets- eller legitimationskort"
  - b. S. 99 " Det vil i sådanne tilfælde i stedet for billedlegitimation være relevant at anvende f.eks. en digital signatur"
  - c. S. 99 " Andre uafhængige og pålidelige kilder kan være private udbydere af sådanne oplysninger, digitale signaturer, telefonbøger og verificering af dokumenter fra en uafhængig og pålidelig tredjemand. Kontrollen kan foretages ved hjælp af dokumenter, data eller oplysninger. En kontrol kan derfor være et opslag i et it-system, en søgning i en database m.v."
  - d. S. 100 " Der kan også ske kontrol ved øvrige eksterne kilder, som f.eks. Det Centrale Personregister eller i form af en digital signatur, der er udstedt af en pålidelig og uafhængig kilde"
  - e. S. 133 " Virksomheder og personer, som anvender digital signatur eller verifikation via elektroniske databaser som led i kontrollen, skal opbevare et teknisk revisionsspor, som dokumenterer den gennemførte kontrol."

Der står således intet i loven (eller i de ovenfor citerede passager) om at "digitale signaturer" skal behandles anderledes end andre kontrolkilder ift. identitetskontrol, og der står intet om at nogle kontrolkilder er bedre i nogle risikoklasser og andre er bedre i andre risikoklasser.

## 2) NemID anvendes kun til kontrol af ID-oplysninger (ikke andre dele af KYC-proces)

Ifølge loven består forpligtelsen "Know your customer" (KYC) jf. § 11 af tre adskilte dele, som der skal sondres imellem:

- A) § 11, stk. 1 nr 1+2 vedr. identitetskontrol, som består af indhentning af navn + cpr (§11, stk. 1, nr 1, a) samt kontrol heraf (§11, stk. 1, nr 2) og

<sup>2</sup> [https://www.ft.dk/samling/20161/lovforslag/l41/20161\\_l41\\_som\\_vedtaget.htm](https://www.ft.dk/samling/20161/lovforslag/l41/20161_l41_som_vedtaget.htm)

<sup>3</sup> [https://www.ft.dk/ripdf/samling/20161/lovforslag/l41/20161\\_l41\\_som\\_fremsat.pdf](https://www.ft.dk/ripdf/samling/20161/lovforslag/l41/20161_l41_som_fremsat.pdf)

# Finans og Leasing

Interesseorganisation for danske finansieringsselskaber

B) §11, stk. 1, nr. 4) vedr. formål og beskaffenhed og

C) § 11 stk. 1 nr. 5) løbende overvågning.

Det er kun A) delen (identitetskontrollen) af KYC som NemID skal bruges til. NemID'en vil således ikke træde i stedet for hele KYC-processen (i nogen risikoklasse for den sags skyld)– den bruges ikke til tjek af resten af KYC-delen (§11, stk. 1, nr 4 og 5).

Ifølge bemærkningerne til lovens § 11, stk. 1, nr 2) skal der som kontrol foretages ”en kontrol” eller ”et opslag” ”...*At kontrollen skal foretages på grundlag af dokumenter, data eller oplysninger indhentet fra en pålidelig og uafhængig kilde betyder, at kontrollen ikke kan baseres alene på oplysninger indhentet fra kunden...*” og ”...*En kontrol kan derfor være et opslag i et it-system, en søgning i en database m.v....*” (vores understregninger)

### 3) Distancekunder/forhold medfører ikke automatisk høj risiko

På side 38 i lovbemærkningerne fremgår:

*”Dette betyder blandt andet, at det, at en kunde ikke har været fysisk til stede for at legitimere sig, fremover ikke automatisk medfører øget risiko for hvidvask og terrorfinansiering. Dette vil i stedet bero på en konkret risikovurdering.”*

Dvs. at blot fordi NemID ofte anvendes i distanceforhold medfører det ikke at der altid er tale om høj risiko. I øvrigt kan NemID også anvendes ved fysisk fremmøde (f.eks. ved betaling via ens mobiltelefon eller tablet i en butik).

### 4) Loven omtaler tre risikoklasser ”begrænset”, ”mellem” og ”øget”

Det er op til virksomhederne selv via deres risikovurdering at vurdere hvor mange risikoklasser man ønsker at operere med i sin virksomhed. Loven nævner som eksempel øget, mellem og begrænset jf. lovforslagets side 99.<sup>4</sup> Dvs. at lovens udgangspunkt er neutral/mellem risiko, og derefter kan diverse risikofaktorer føre til hhv. øget/høj eller lav/begrænset risiko.

Det fremgår endvidere, at det kun er i tilfælde af ”øget risiko” at der skal foretages yderligere handlinger/kontrol ud over kontrollen af id-oplysningerne.:

*”Ved tilfælde med øget risiko skal der foretages yderligere handlinger, uanset at kundens identitetsoplysninger er kontrolleret. Virksomheden eller personen kan kræve yderligere dokumenter fra kunden, foretage opslag i eksterne kilder eller kræve, at første betaling sker fra en bankkonto i kundens navn m.v. alt efter, hvilke procedurer der kan medføre, at virksomheden eller personen ikke er i tvivl om, at kunden er den, denne udgiver sig for at være.” (s.100) (vores understregning)*

Det er således kun ved øget risiko (høj risiko) at der skal foretages mitigerende tiltag (og ikke som det fremgår nu af vejledningen i afsnittet om NemID, at der skal foretages mitigerende tiltag i alt andet end begrænset risiko), herunder ”normal”/mellem risiko.

At det kun er ved ”øget” risiko der skal kontrolleres ved flere kilder fremgår også af bemærkningerne til § 17 (s. 112): ” Skærpede kundekendskabsprocedurer kan udbygge de almindelige krav i § 11, som f.eks. at gennemføre kontrol af kundens identitetsoplysninger ved flere kilder for at øge kvaliteten af kontrollen...” og der skelnes i øvrigt ikke mellem hvilke forskellige kontrolkilder der kan anvendes (digitale signaturer ift. pas/kørekort mv) ved begrænset/øget risiko.

<sup>4</sup> ”I praksis kan kunder inddeles i forskellige profiler på baggrund af en vurdering af risikoen for hvidvask og terrorfinansiering, f.eks. øget risiko, mellem risiko, begrænset risiko eller evt. flere grupper afhængig af virksomhedens størrelse, forretningsmodel eller andre faktorer.”

[https://www.ft.dk/ripdf/samling/20161/lovforslag/l41/20161\\_l41\\_som\\_fremsat.pdf](https://www.ft.dk/ripdf/samling/20161/lovforslag/l41/20161_l41_som_fremsat.pdf)

## 5) Sikkerhed ved NemID sammenlignet andre (analoge) dokumenter (pas/kørekort)

Grundlæggende kan hverken pas/kørekort eller NemID i sin nuværende form beskyttes mod kriminelle handlinger i form af bedrageri (herunder identitetstyveri), trusler og tvang mv.

Dog må det nævnes, at hvis man anvender og opbevarer NemID som intentionen er, så har NemID den indbyggende sikkerhedsforanstaltning, at anvendelsen kræver 3 sikkerhedselementer anvendt nemlig; brugernavn, kodeord og nøglekort/nøgleviser/NemID app. Man kan ikke afvise at alle elementer kan stjæles på samme tid, men udgangspunktet må være, at de opbevares som foreskrevet/anbefalet og derfor taler sandsynligheden imod at kriminelle får fat i alle tre elementer ved et simpelt tyveri (dette er også baggrunden at der er retspraksis der fastslår, at indehavere af NemID bliver gjort erstatningsansvarlige for den uretmæssige anvendelse af deres NemID). Mens simpelt tyveri af en tegnebog i mange tilfælde vil give adgang til f.eks. kørekort og sundhedsbevis.

Alt andet lige må det endvidere antages, at det er vanskeligere, at forfalske NemID end fysisk pas/kørekort, da det første kræver it-mæssige færdigheder hvorimod pas/kørekort kan ændres fysisk og forfalskes.

Hertil kommer endvidere, at der ved brug af NemID afsættes et elektronisk revisionsspor som vil gøre det nemmere bagefter at spore den kriminelle. Dette må alt andet lige gøre det mindre ”attraktivt” for kriminelle af anvende NemID til svindel.

Der har ikke høringsprocessen (møderækken med 5 møder hen over 6 måneder + mailkorrespondancer mv.) været fremlagt nogle konkrete indicier på at NemID skulle være mindre sikkert eller mindre pålideligt til ID-kontrol end analoge ID-dokumenter.

## 6) NemID anvendes overalt i samfundet som led i bevis på en borgers identitet

NemID anvendes overalt i det danske samfund som kontrol af og bevis for en borgers identitet, herunder:

- Ift. det **offentlige** Danmark:
  - Hos SKAT kan man via NemID f.eks. ændre både årsopgørelse og den Nemkonto som overskydende skat udbetales til.
  - Man kan blive skilt med NemID.
  - Tilgå stærkt fortrolige sundhedsdata (egne og børns)
  - Man kan afgive erklæringer mv.
  - Domstole\*/Tinglysningssystemet

\*Ift. domstole fastslår retsplejelovens § 478, at eksigible gældsbreve, der er underskrevet digitalt kan tvangsfuldbyrdes, dvs. at der er sket en sidestilles af fysisk underskrevne aftaler med digitalt underskrevne aftaler ud fra overvejelser om sikkerhed for underskrivers identitet.

Derudover er der endvidere en efterhånden fast retspraksis fra domstolene, der fastlægger at indehavere af NemID bliver gjort erstatningsansvarlige for den uretmæssige anvendelse af deres NemID. Dette understreger også domstolenes anerkendelse (legitimiteten) af digitalt underskrevne dokumenter.

- Ift. **private** virksomheder:
  - NemID anvendes til transaktioner i netbanker uden yderligere foranstaltninger til at foretage betydelige transaktioner, herunder aktiekøb, køb af fast ejendom mv.

# Finans og Leasing

## Interesseorganisation for danske finansieringsselskaber

- Generelt er der et politisk ønske om generelt at bruge digitale løsninger til at gøre samfundet mere effektivt, jf. <https://digst.dk/strategier/digitaliseringsstrategien/om-digitaliseringsstrategien-2016-2020/> og <https://www.regeringen.dk/nyheder/strategi-for-danmarks-digitale-vaekst/>, samt også de citerede dele af bemærkningerne til loven, og der er et ønske fra branchen om at gøre brug af de gode digitale løsninger, der allerede er udviklet.

### Opsummering og konklusion ift. brug af NemID ift hvidvask i vejledningen:

Loven indeholder ikke hjemmel til at fastsætte i vejledningen at a) digitale signaturer/NemID adskiller sig fra andre kontrolkilder, og den indeholder heller ikke hjemmel til at b) at digitale signaturer/NemID kun kan anvendes som eneste kontrolkilde i begrænset risiko. Dette bygger på følgende:

- 1) Hvidvaskloven er teknologineutral og anerkender digitale signaturer som kontrol af identitetsoplysninger på lige fod med analoge dokumenter såsom pas/kørekort.
- 2) Der skal ved KYC sondres mellem identitetskontrol og andre led i KYC. NemID anvendes kun til tjek af identiteten – ikke andre dele af KYC.
- 3) Distanceforhold medfører ikke automatisk høj risiko
- 4) Loven omtaler kun tre risikoklasser og det er kun ved ”øget” risiko (jf. § 17), at identiteten skal kontrolleres ved flere kilder og i så tilfælde skelnes ikke mellem kontrolkilder (digitale signaturer ctr pas/kørekort mv).
- 5) Finanstilsynet har ikke fremlagt dokumentation for at NemID skulle være mindre sikkert eller mindre pålideligt til ID-kontrol end analoge ID-dokumenter.
- 6) NemID anerkendes i alle dele af samfundet som bevis for en borgers identitet, og der er et ønske fra regeringen og erhvervslivet om at anvende digitale løsninger.

Ovenstående argumenter fører til den samlede konklusion, at NemID (ligesom pas/kørekort) skal kunne anvendes som eneste kontrolkilde af ID-oplysninger også i ”mellem” risiko (såvel som i begrænset risiko), og derfor foreslår vejledningens afsnit om NemID skal ændres til følgende:

*”NemID er en pålidelig og uafhængig kilde, men i de tilfælde hvor **der er høj risiko** ~~der ikke kan er tale om begrænset risiko~~, vil det være nødvendigt for virksomheden at benytte sig af andre kontrolkilder eller mitigerende tiltag sammen med NemID” (s.62).*

### Yderligere spørgsmål til høringen/vejledningen:

- Hvis der i en forening forefindes både en bestyrelse og en direktion, hvem af disse skal så betragtes som reelle ejere, som vi skal indhente navn og CPR nr. på ? (Se afsnit 9.6.4, 2. afsnit i punktet om frivillige foreninger og andelsboligforeninger).
- I afsnit 9.6.4, 3. afsnit i punktet om frivillige foreninger og andelsboligforeninger står der følgende: *Til brug for identifikation af de reelle ejere kan virksomheden f.eks. indhente foreningens stiftelsesdokumenter, vedtægter eller referater fra generalforsamlingen.* Hvordan skal det forstås i forhold til de personer, der måtte være registreret som reelle ejere i CVR registret? Hvad har forrang ? Det i CVR registrerede eller det i stiftelsesdokumentet mv. registrerede?
- Finanstilsynet har i løbet af processen givet det indtryk, at i tilfælde hvor den daglige ledelse vurderes at være en bestyrelse, er udgangspunktet, at det er hele bestyrelsen, der skal betragtes som reelle ejere jf. § 2, stk. 1, nr. 9, litra b.

# Finans og Leasing

Interesseorganisation for danske finansieringsselskaber

- Det ses ikke umiddelbart hvor i loven, at der står ordet ”hele”?
- Hvordan skal virksomheder f.eks. forholde sig, hvis der er registreret 87 bestyrelsesmedlemmer– skal man da indhente navn og CPR nr. på alle 87?
- Kunne man forestille sig en mere pragmatisk tilgang således, at det kun var de tegningsberettigede i bestyrelsen, der skal betragtes som reelle ejere?

Med venlig hilsen

Thomas Benjamin Johansen  
Chefkonsulent  
Finans og Leasing  
E-mail: [tbj@finansogleasing.dk](mailto:tbj@finansogleasing.dk)