

Finanstilsynets AML/TEK-konference

DGI Byen

Torsdag den 18. november 2021

DAGENS PROGRAM

- 10.00 – 10.10 **Velkommen**
v/Jesper Berg, direktør, Finanstilsynet
- 10.10 – 10.40 **Udfordringer i forhold til samspillet mellem reglerne i GDPR og hvidvaskreglerne**
v/Kenni Elm Olsen, specialkonsulent, Datatilsynet
- 10.40 – 11.10 **Retssikkerhedsmæssige udfordringer ved øget brug af data**
v/Henrik Rothe, projektleder i Justitia, adjungeret professor CBS
- 11.10 – 11.25 Pause
- 11.25 – 11.55 **Potentialet ved øget deling af data**
v/Anita Nedergaard, Country AML Responsible, Nordea Bank Danmark
- 11.55 – 12.25 **Resultater fra et pilotprojekt: Databaseret indsats styrker kampen mod hvidvask**
v/Thais Lærkholm Jensen, Head of Data Analytics and Science, Danmarks Nationalbank
- 12.25 – 12.30 **Afslutning**
v/Rikke-Louise Ørum Petersen, vicedirektør, Finanstilsynet

AML/TEK-konference

18. november 2021 Specialkonsulent Kenni Olsen, Datatilsynet.



DATATILSYNET

Retten til privatliv

- Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende
- Retten til privatliv er ikke absolut
 - Under iagttagelse af proportionalitetsprincippet kan der indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse
- Bekæmpelsen af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, er anerkendt som et mål af almen interesse, der kan begrunde begrænsninger til retten til privatlivet og beskyttelsen af personoplysninger
- Det er en betingelse, at begrænsningen bl.a.:
 - Er egnet til at gennemføre målet
 - ikke går videre, end hvad der er nødvendigt og passende for gennemførelsen af målet
- Udfordring: Balancering af hensyn



Principper for behandling af personoplysninger

- Databeskyttelsesforordningens artikel 5, stk. 1, litra a-f, indeholder en række (grundlæggende) principper for behandling af personoplysninger, som altid skal være opfyldt. Det betyder, at personoplysninger skal:
 - behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede («lovlighed, rimelighed og gennemsigtighed«)
 - indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål («formålsbegrænsning«)
 - være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles («dataminimering«)
 - være korrekte og om nødvendigt ajourførte («rigtighed«)
 - opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles («opbevaringsbegrænsning«)
 - behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hædeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger («integritet og fortrolighed«)



Krav om lovligt grundlag

- Databeskyttelsesforordningens artikel 6 regulerer, hvornår der lovligt kan behandles personoplysninger, og behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende:
 - Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
 - Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
 - Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
 - Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.
 - Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
 - Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.



Behandling af særlige kategorier af personoplysninger

- Særlige kategorier af personoplysninger (følsomme personoplysninger) er: race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering
 - Ved profilering af den registrerede, kan der ”skabes” følsomme oplysninger
- Som udgangspunkt forbudt at behandle følsomme personoplysninger, jf. databeskyttelsesforordningens artikel 9, stk. 1
- Forbuddet gælder ikke, hvis den dataansvarlige kan identificere en undtagelse til dette forbud i enten forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører forordningens artikel 9
 - Relevant at overveje er udtrykkeligt samtykke (artikel 9, stk. 2, litra a) eller væsentlige samfundsinteresser (artikel 9, stk. 2, litra g)
 - Anvendelsen af artikel 9, stk. 2, litra g, kræver, at der findes et grundlag i enten EU-ret eller national lovgivning



Udfordringer

- Hvidvaskreglerne pålægger de forpligtede enheder nogle (vidtrækkende) forpligtelser, f.eks. forpligtelser om kundekendskab, monitorering af transaktioner og rapportering af mistænkelige transaktioner, som i omfang og rækkevidde ikke altid er helt klare, herunder i forhold til hjemmel
 - Fører til en "Better safe than sorry" tilgang
 - Fører til omfattende behandling af personoplysninger, herunder potentielt følsomme oplysninger, hvor det ikke er nødvendigt
 - Anvendelse af tredjeparter, hvis regulering er uklar
- Løsning
 - Lang sigt: Tydeliggørelse af forpligtelserne i reglerne ("RTS")
 - Kort sigt: "Man gør det så godt man kan"



Udfordringer

- Hvidvaskreglerne indeholder nogle (meget) lange (generelle) opbevaringsfrister
 - Eksempel: Hvidvasklovens § 30
- Hvorfor er det en udfordring?
 - (Dataminimering)
 - (Opbevaringsbegrænsning)
- Løsning
 - Kravene til opbevaring specificeres i forhold til type af oplysning og baggrunden for indsamling



Udfordringerne fremgår af et brev fra EDPB til Kommissionen



Ms Mairead McGuinness
European Commissioner for Financial services,
financial stability and Capital Markets Union

Mr Didier Reynders
European Commissioner for Justice
by e-mail only

Brussels, 19 May 2021
Ref: OUT2021-0088

Dear Commissioner McGuinness,
Dear Commissioner Reynders,

This letter follows the adoption by the EDPB, on 15 December 2020, of a Statement on the protection of personal data processed in relation with the prevention of the use of the financial system for the purposes of money laundering and terrorist financing¹, as well the adoption by the European Commission of an Action Plan² for a comprehensive Union policy on preventing money laundering and terrorist financing and the launch of a public consultation³ in May 2020.

The Commission aims to present new legislative proposals in 2021, *inter alia*, establishing a single rulebook on these topics (i.e. a Regulation or a more detailed revised Directive), ensuring EU level supervision (either by granting new powers to an existing EU Agency or by establishing a new dedicated body), and creating a support and coordination mechanism for Financial Intelligence Units.

The core purpose and function of the AML Directives and their subsequent transposition into EU member state domestic laws are for... "the prevention of the use of the financial system for the purposes of money laundering or terrorist financing". It is important to keep this statement in mind when considering the data protection implications of AML laws, because the key method for

Hørings svar fra Finans Danmark

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

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.



Udfordringer

- Databeskyttelsesforordningen er teknologineutral, men brugen af ”ny” og/eller avanceret teknologi kan udgøre en udfordring, herunder i forhold til:
 - Gennemsigtighed / transparens
 - Usaglighed (bias)
 - Skal trænes på rigtige data (kræver også hjemmel og at formålet er foreneligt)
 - Skal ske i overensstemmelse med databeskyttelsesforordningens artikel 22
- Deling af oplysninger mellem enheder, herunder via en offentlig myndighed:
 - Vil have meget stor indvirkning på privatlivet
 - Formålsforskydning
 - Private: ”Blacklisting”
 - Offentlige: Kontrol med andre ting (skat, sociale ydelser mv.)



Tak for jeres tid!

Datatilsynet

Carl Jacobsens Vej 35

2500 Valby

Tlf. 33 19 32 00

dt@datatilsynet.dk

datatilsynet.dk



DATATILSYNET

Potentialet ved øget deling af data

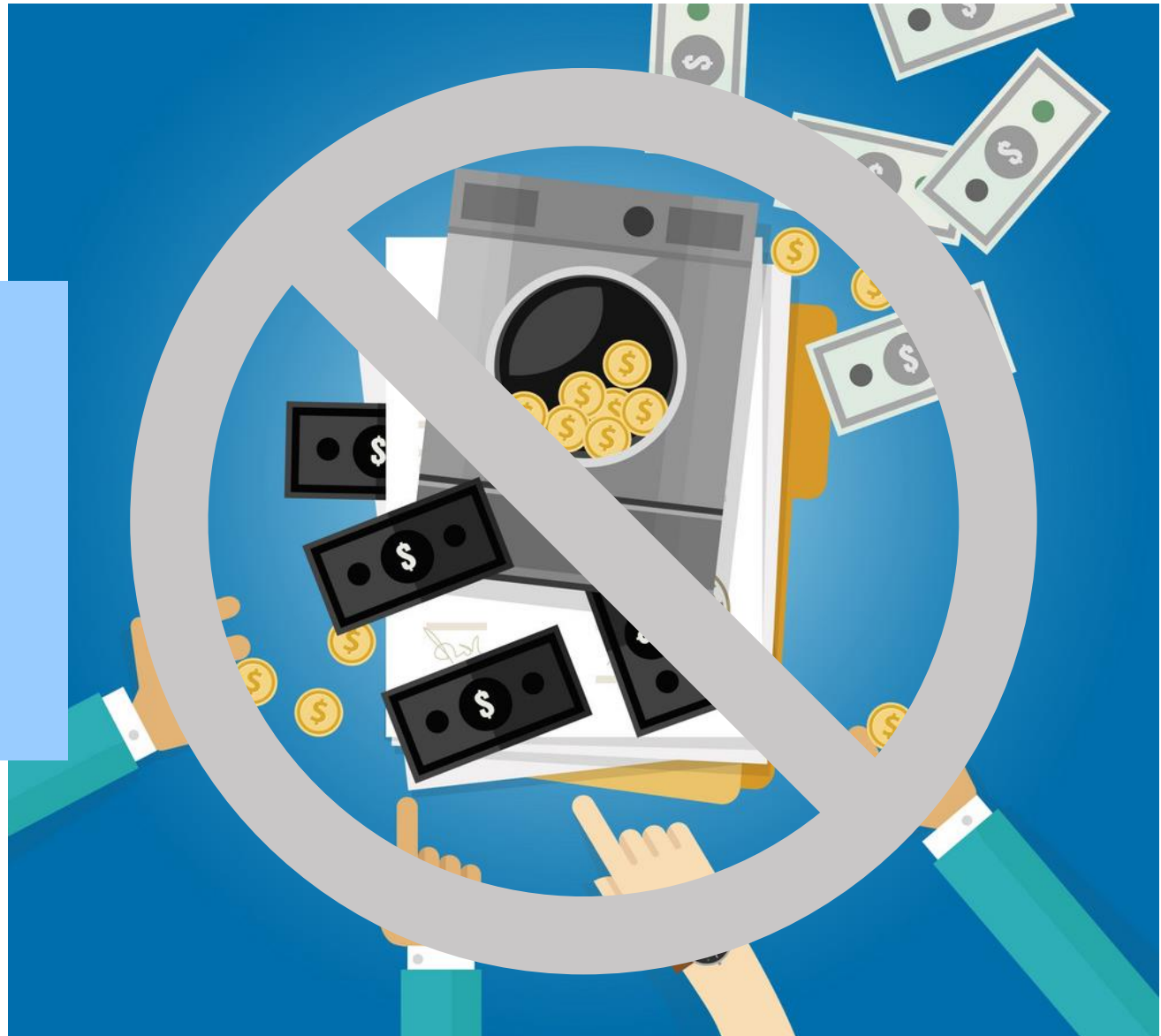
Anita Nedergaard, Country AML Responsible, Nordea Danmark

18.11.2021

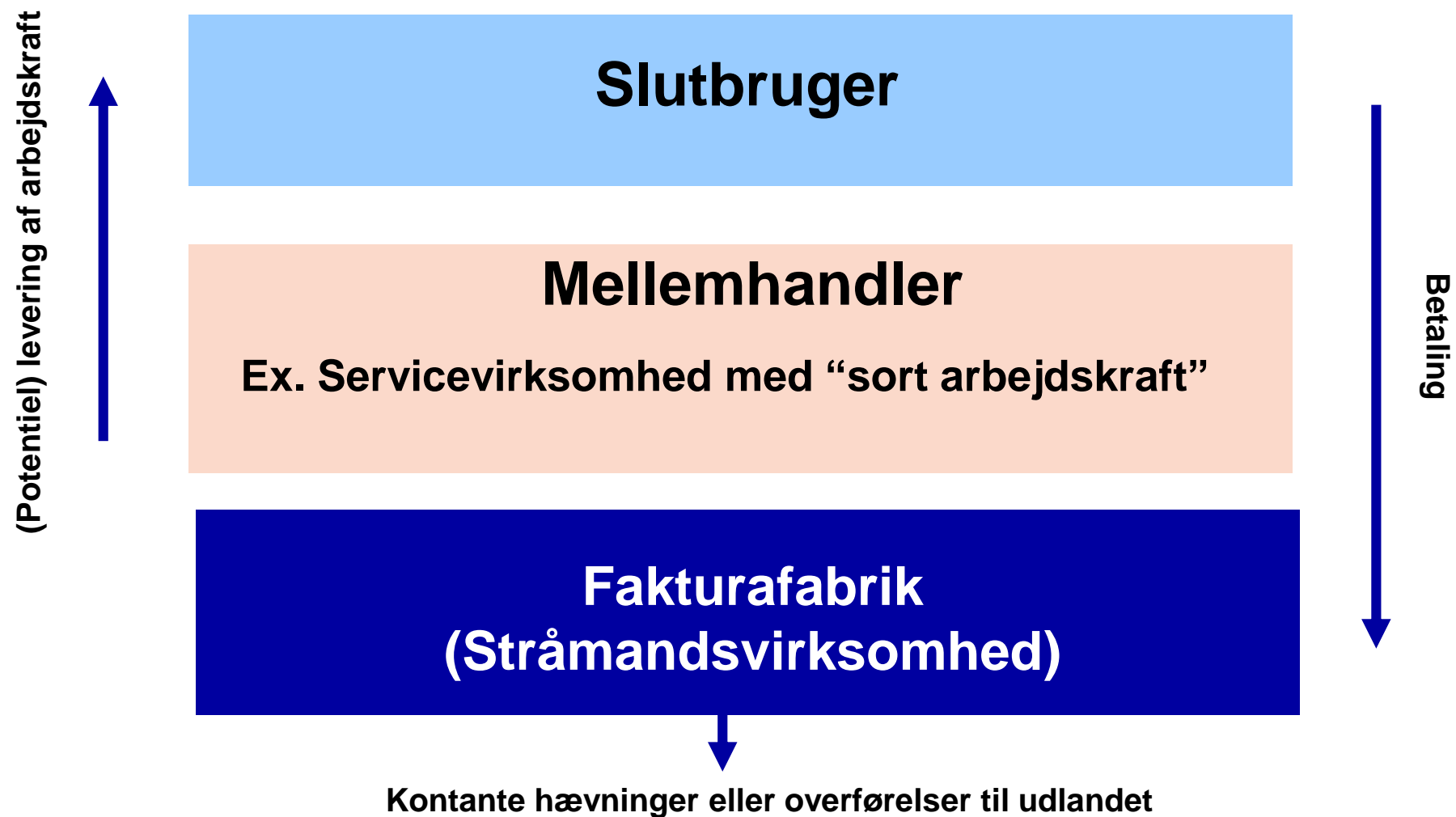


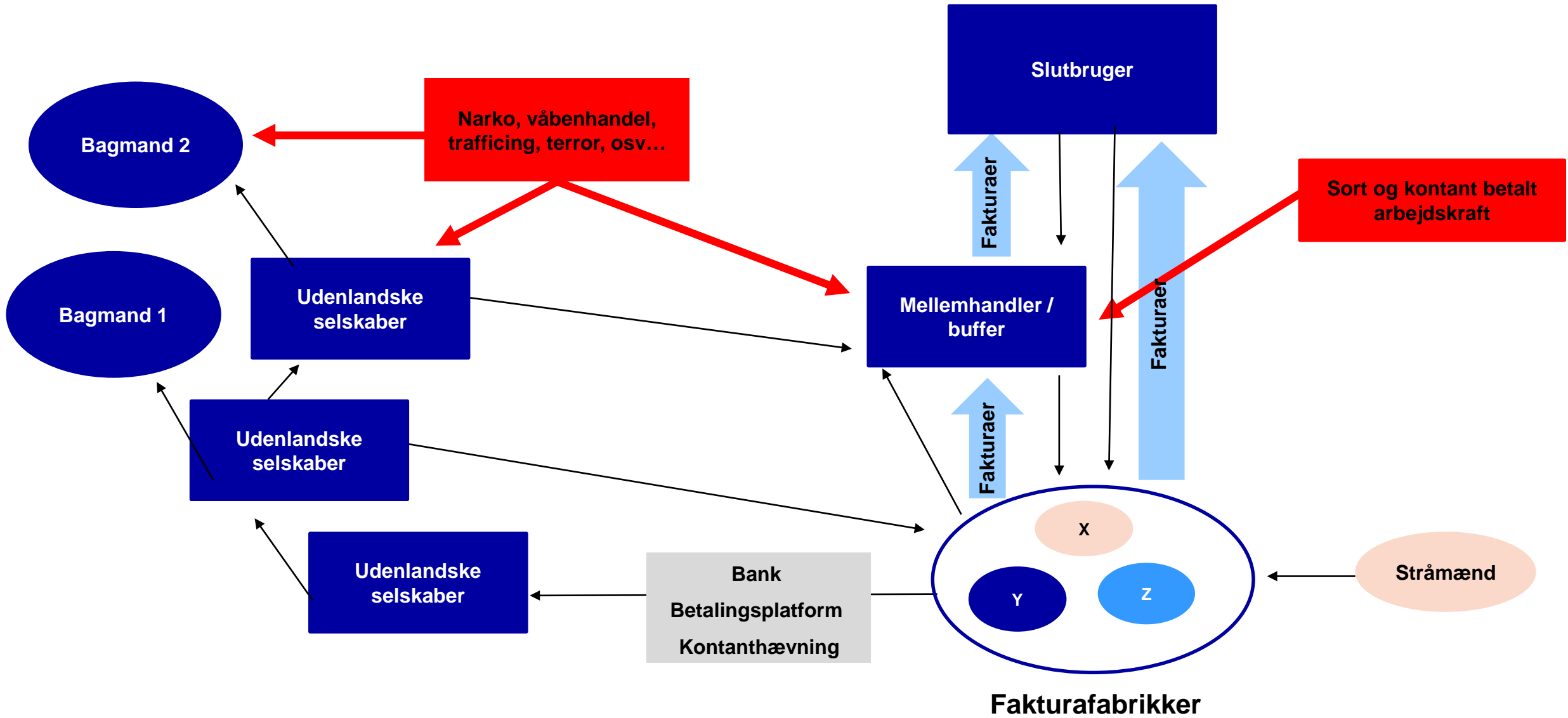
Agenda

- **Hvorfor deling af kundeinformation?**
 - Hvordan fungerer en fakturafabrik?
 - Kundeeksempel
- **Fordele ved mere informationsdeling**
- **En balanceret tilgang**
- **Opsummering**
- **Spørgsmål**

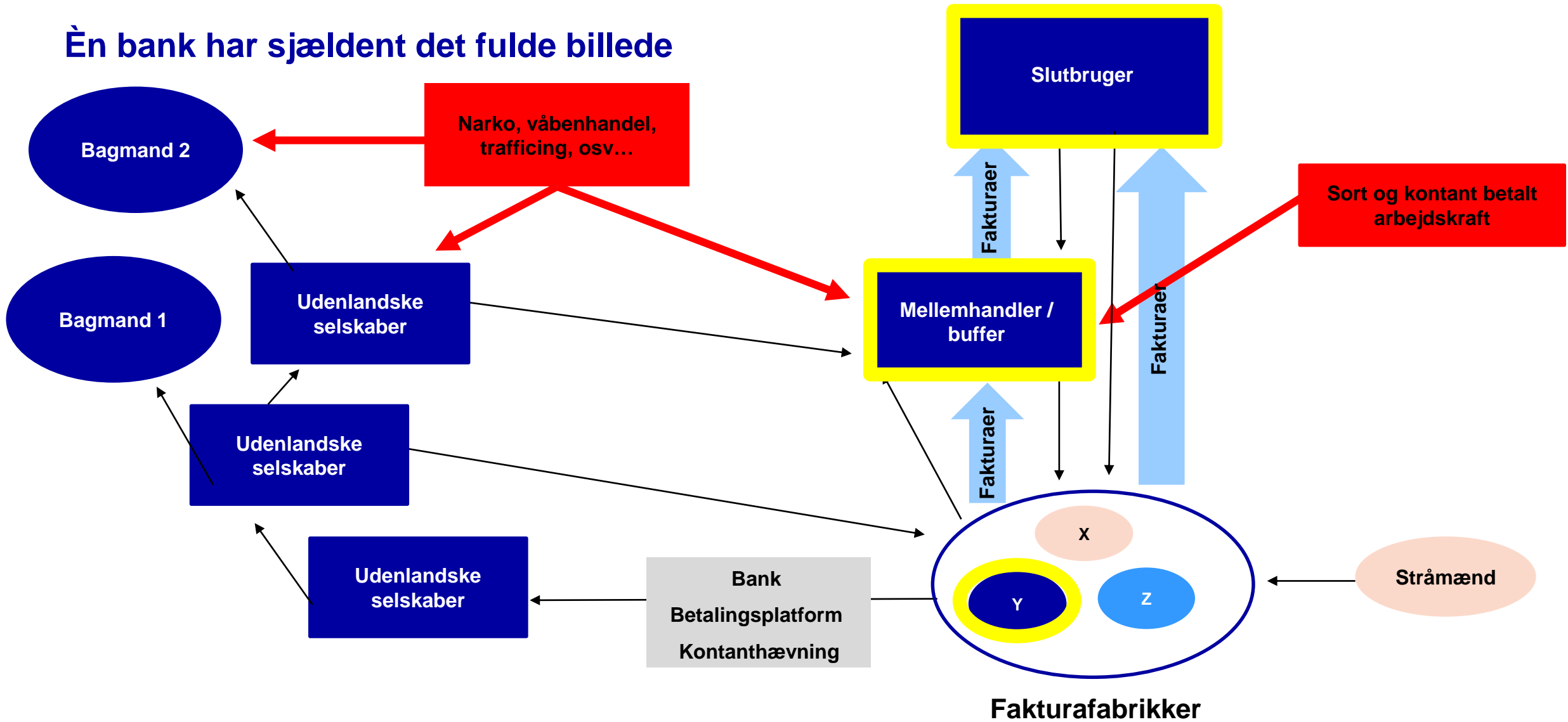


Hvordan fungerer en fakturafabrik?





En bank har sjældent det fulde billede



Eksempel :

1. Advarsel information

- Vi bliver opmærksom på en sær kundefærd i forbindelse med vores kontrol af covid-støtte ordninger eller en traditionel TM-alarm.
- Hvorfor overfører vores kunde til x-virksomhed?
Eks. Hvorfor overfører en frisør til en produktionsvirksomhed?

3. Begrundelse og resultat

- Mistanke om falske faktura, dvs. skatte-momsunddragelse – og måske anden kriminalitet

1. Indrapporterer SAR
2. Opsiger kundeforholdet

2. Undersøgelse



Undersøgelse af transaktioner

- Hvem overfører ellers penge til produktionsvirksomheden?
- Det viste sig, at rigtig mange kunder overførte til de samme to konti i et andet pi.



Tjek af andre informationer

- Hvem er vores kunde?
- Opbygning, struktur, ejerforhold, historik i virksomheden og i vores engagement.
- Offentlige oplysninger; virk.dk, google, tinglysningen.dk

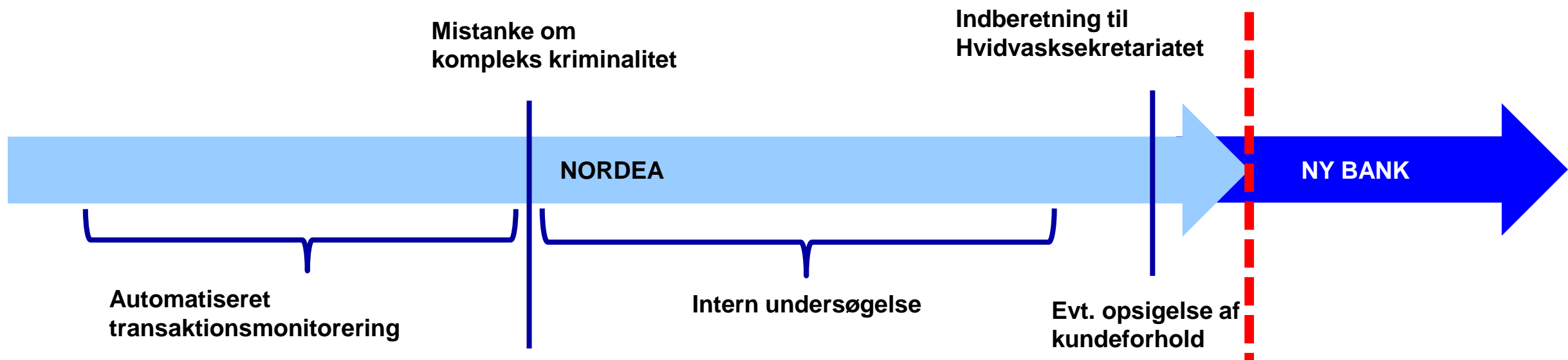


Kundekontakt

- Kan mistanken afkræftes?
- Hvad fortæller kunden om de forhold, som vi finder "sære"?

En advarsel til andre banker, kan stoppe den kriminelle adfærd tidligere

- Afdækning af en fakturafabrik tager uger. Der ligger meget arbejde med at kvalificere indberetningen til Hvidvasksekretariatet og efterfølgende opsige kundeforholdet
- Kunden flytter til en anden bank uden vi kan gøre til eller fra – og processen starter forfra
- Der findes op mod 90 pengeinstitutter i Danmark – det giver de kriminelle frit spil



Fordele ved mere informationsdeling

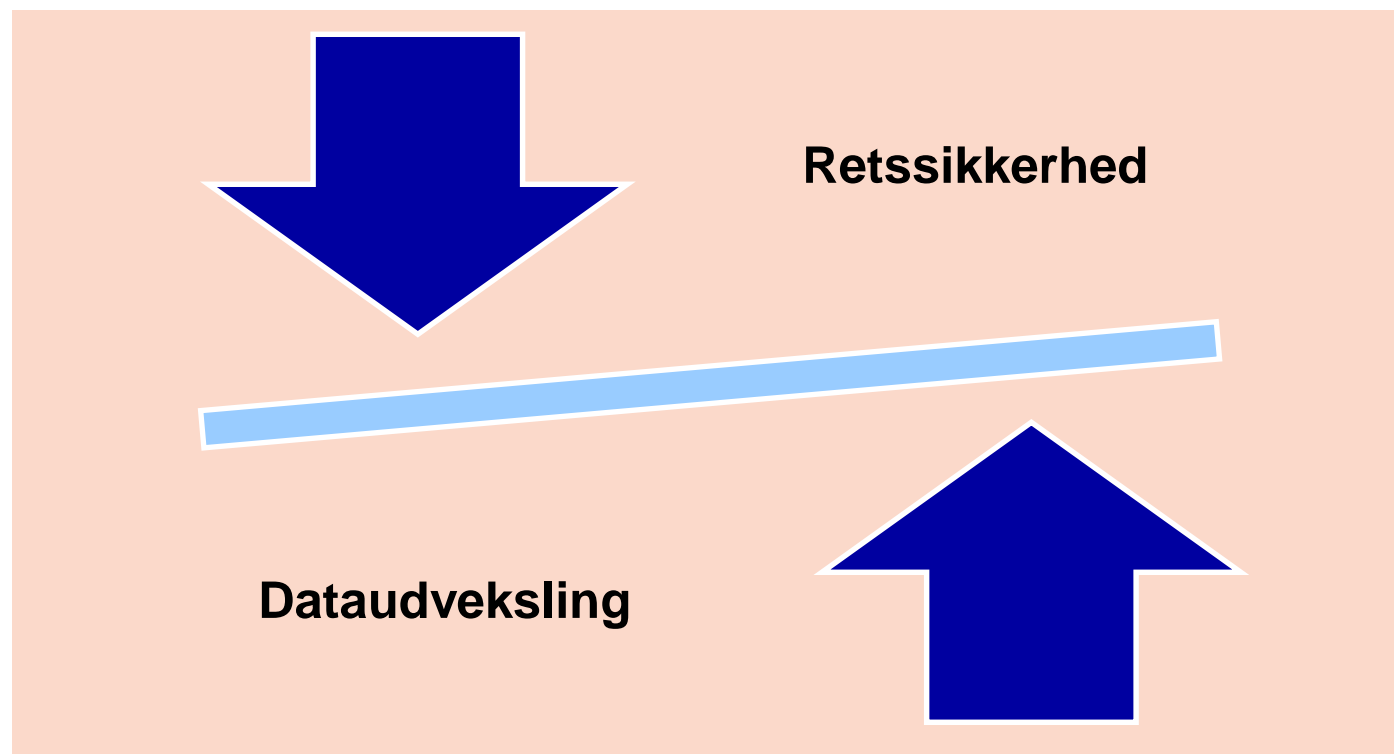
- **Deling af information mens vi undersøger**
 - Samarbejde på tværs af pengeinstitutterne (og gerne også relevante myndigheder) om undersøgelserne
 - Undersøgelserne bliver mere effektive
 - Underretningerne til Hvidvasksekretariatet kan blive mere fyldestgørende og dermed i højere grad direkte anvendelige
 - Mulighed for flere beslaglæggelser – mindre attraktivt miljø.
- **Gevinst:** hurtigere stop for den kriminelle aktivitet

- **Deling af information efter opsigelse af kundeforholdet**
 - Det modtagne pengeinstitut vil få mulighed for at holde særligt øje med kunden
 - En fortsættelse af den kriminelle adfærd opdages hurtigere, dvs. bankens procestid forkortes
 - Kundeforholdet vil typisk være etableret i det nye pengeinstitut inden information deles
- **Gevinst:** hurtigere stop for den kriminelle aktivitet

OBS!

En transaktion/et risikoflag ctr. mistænkelig adfærd.

Hvordan finder vi den rette balance?



Finansiell kriminalitet

Hvidvask

Terrorfinansiering

Brud på sanktioner

Skatteunddragelse

Bestikkelse og korrupsion

Svindel

Socialt bedrageri

Forsikringssvindel

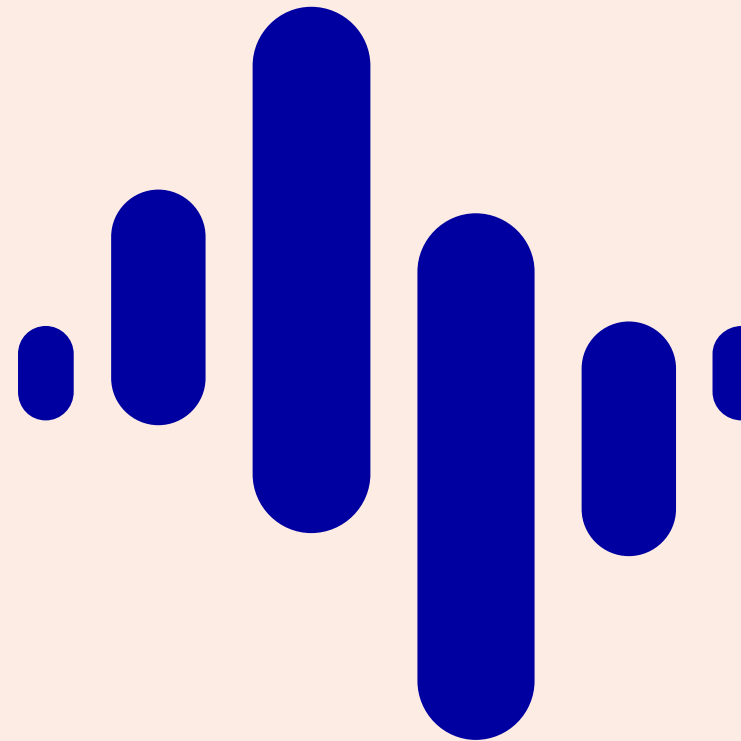
Opsummering

- Hastighed er en *key driver*. De kriminelle lukrerer på, at vi er langsomme, og at vi ikke må dele oplysninger!
- Den "manuelle" datadeling er effektiv ved bekæmpelse af den organiserede kriminalitet.
- Den "manuelle" deling er let og kan let implementeres
- Vi kan ikke fjerne kriminaliteten – men vi kan gøre det sværere at være kriminel, så de egentlige bagmænd vælger andre lande til deres aktivitet.
- Ressourcer er en mangelvare – lad os bruge dem, vi har, til en bedre fælles indsats.

- Hvis vi gør ingenting – Danmark vil (fortsat) være en attraktiv lokalitet for flere af denne type af sager....

Nordea

Spørgsmål?



Nordea

Tak!

Anita Nedergaard, Country AML Responsible, Nordea Danmark



DANMARKS
NATIONALBANK

Resultater fra et pilotprojekt: Databaseret indsats styrker kampen mod hvidvask

18. november, 2021

Thais Lærholm Jensen, Head of Data Analytics and Science



Sammenstillet data afslører flere mistænkelige forhold

En risikobaseret metode på baggrund af flere datakilder identificerer dobbelt så mange mistænkelige transaktioner.



Datadrevet indsats giver øget effektivitet og fokus

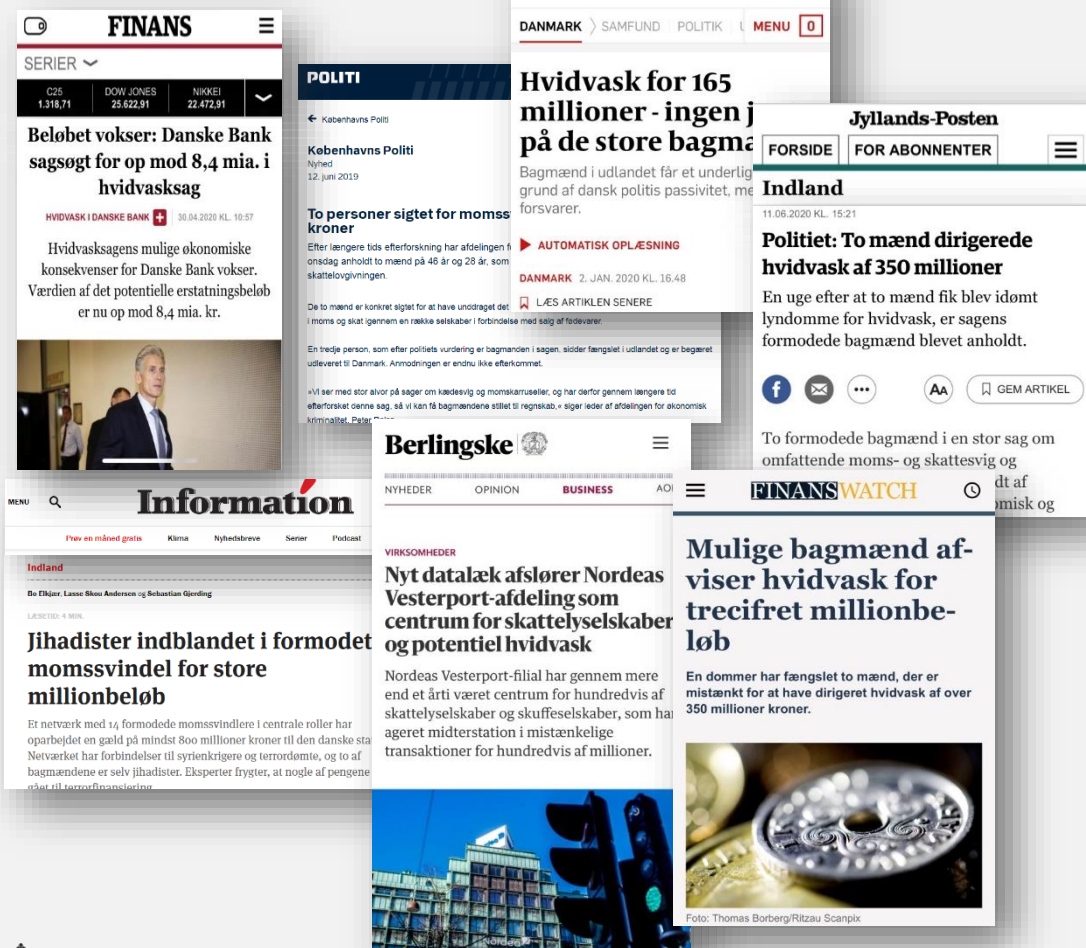
En udvidet datadrevet tilgang kan understøtte bedre prioritering af ressourcer hos myndigheder og finanssektoren.



Fuldt potentiale kræver lovændring

Det fulde potentiale afhænger af brug af data på tværs af banker og myndigheder. En sådan sammenstilling vil kræve en lovændring.

Hvidvask er en væsentlig samfundsmæssig udfordring



Hvidvask er en væsentlig samfundsmæssig udfordring



Kilde: Finansforbundet 2020

Der er væsentlige strukturelle udfordringer i det nuværende system mod hvidvask

1

Tidskrævende at behandle mange "falsk positive"

Foruddefinerede scenarier udløser et stort antal falske alarmer, som medarbejdere i banker og myndigheder manuelt skal forholde sig til

2

Den enkelte bank har kun adgang til egne data

Denne begrænsning gør det usandsynligt, at komplekse hvidvasknetværk, der bevidst involverer flere banker og konti, udløser en alarm hos den enkelte bank

Udfordring 1: Det er tidskrævende at behandle mange falsk positive

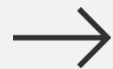
1

ALLE KUNDERS
TRANSAKTIONER

Antal transaktioner,
2020

3,3

mia. transaktioner

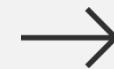


BANKERS AML-ENHEDER
(1. FORSVARSLINJE)

Antal alarmer,
anslået 2020

0,5-1

mio. alarmer



HVIDVASKSEKRETARIATET
(2. FORSVARSLINJE)

Modtagne
underretninger,
anslået 2020

73

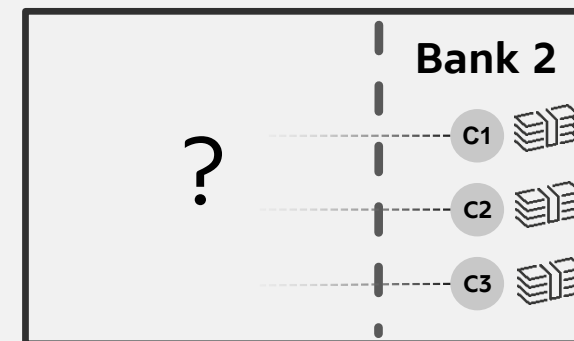
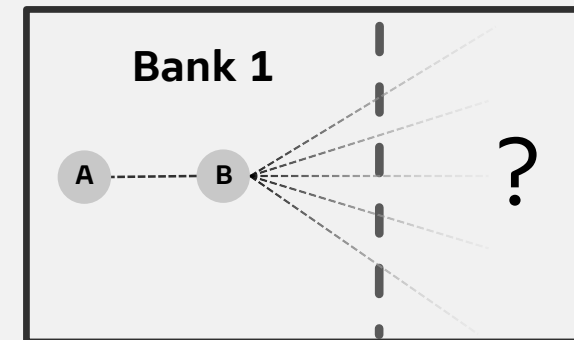
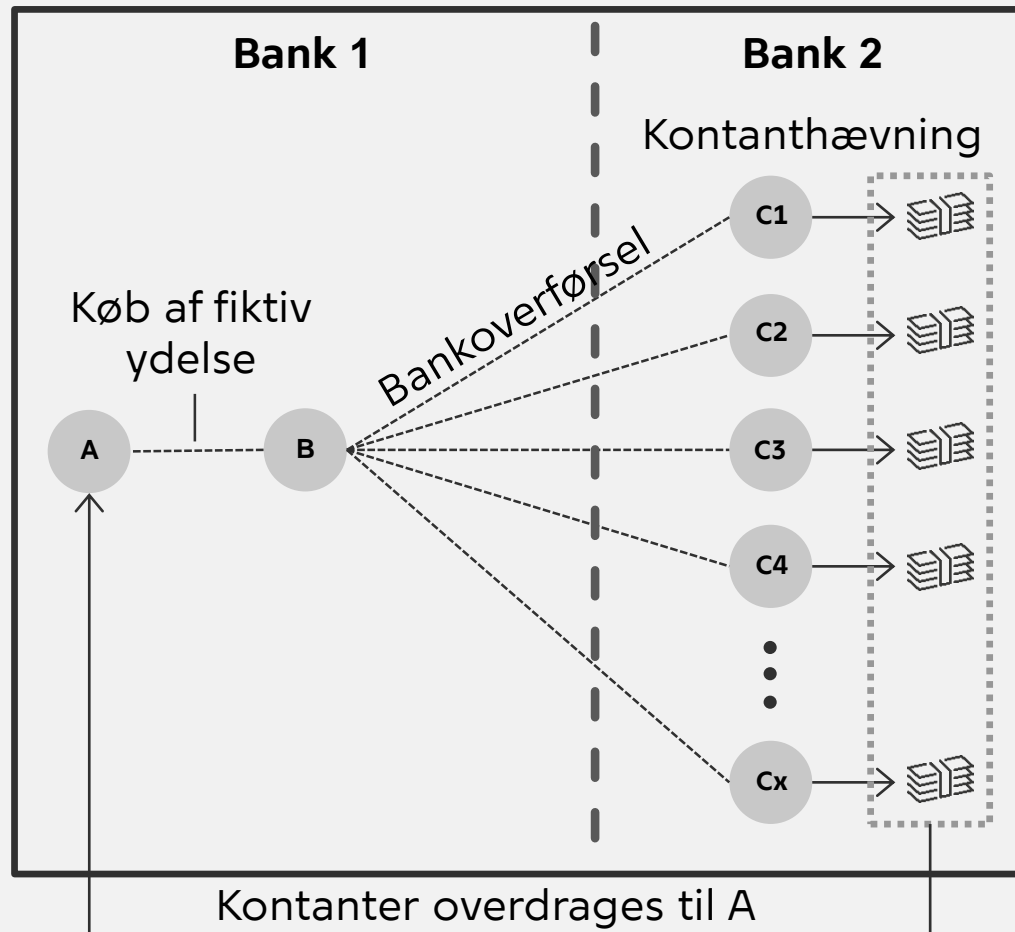
tusinde
underretninger

Kilde: Hvidvasksekretariatet, Nationalbanken og pilotprojektet



Udfordring 2: Banken er begrænset af ikke at kende modpartens risiko

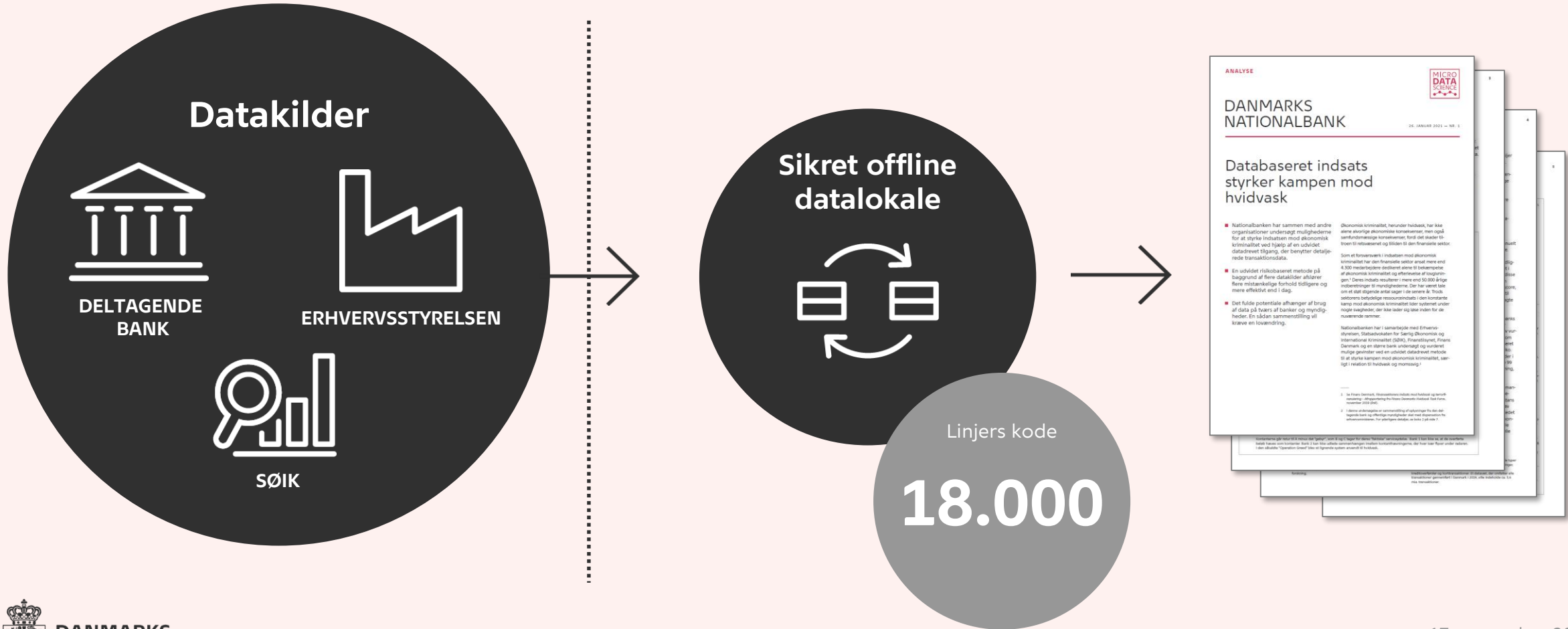
2



Pilotprojektet undersøgte, om en udvidet datadrevet tilgang kan forbedre indsatsen mod økonomisk kriminalitet ...

MIA KR

Irreversibel
data-anonymisering



... Ja, en udvidet datadrevet tilgang kan forbedre opdagelse og effektivitet i indsatsen mod hvidvask



Sammenstillet data afslører flere mistænkelige forhold

En risikobaseret metode på baggrund af flere datakilder identificerer dobbelt så mange mistænkelige transaktioner.



Mulighed for øget effektivitet og fokus

En udvidet datadrevet tilgang kan understøtte bedre prioritering af ressourcer hos myndigheder og finanssektoren.

Sammenstillet data afslører dobbelt så mange mistænkelige forhold, som ikke vurderes i dag ...



To tilgange – samme konklusion

MODEL



Anvende eksisterende data for, hvad det nuværende system hidtil har fundet

SCENARIER



Tage udgangspunkt i objektivet definerede mistænkelige mønstre

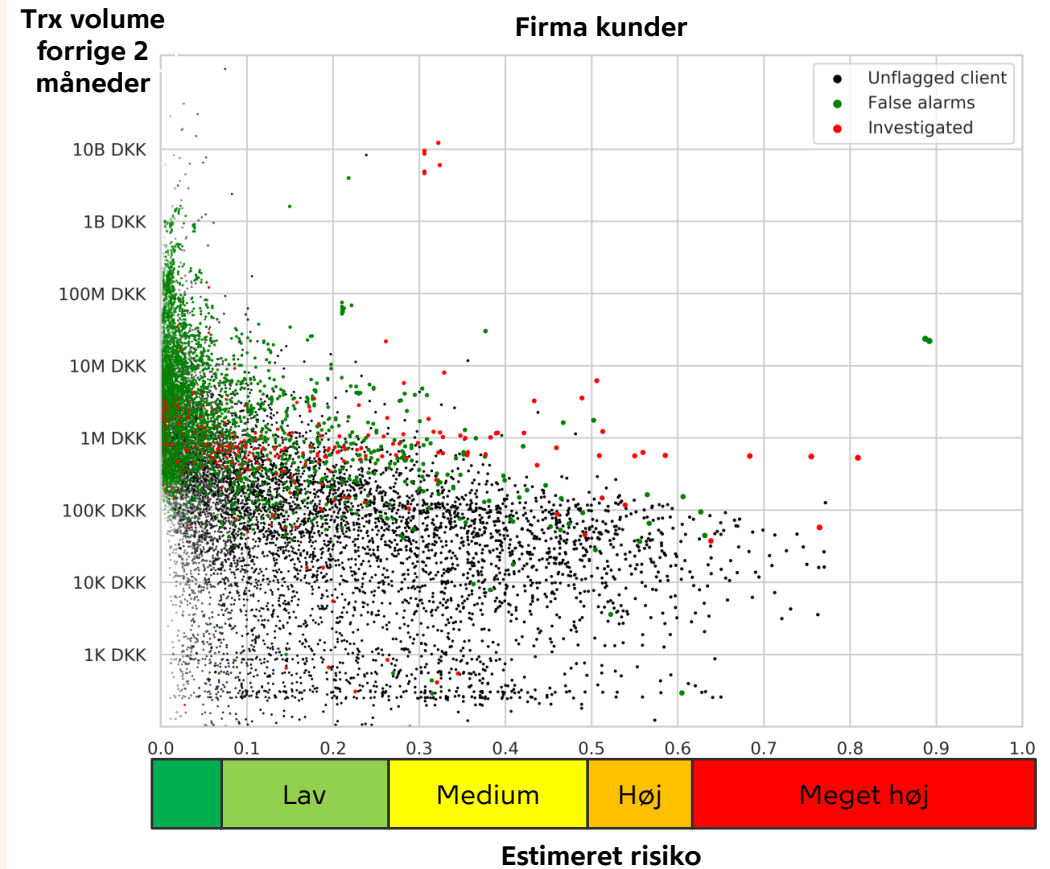
Sammenstillet data afslører dobbelt så mange mistænkelige forhold, som ikke vurderes i dag ...

I

MODEL



Anvende eksisterende data for, hvad det nuværende system hidtil har fundet



Note: Grafen viser et tilfældigt udsnit af data der og sløret med tilfældig støj for at bevare anonymiteten.

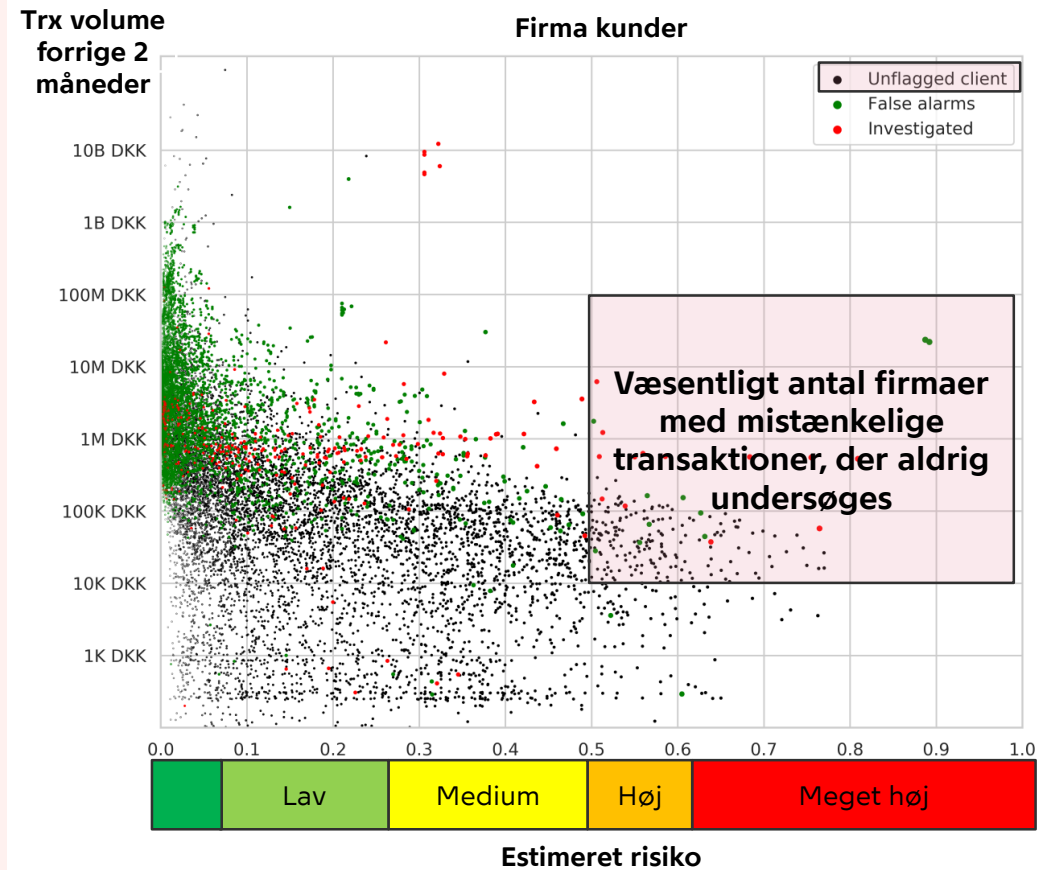
Sammenstillet data afslører dobbelt så mange mistænkelige forhold, som ikke vurderes i dag ...

I

MODEL



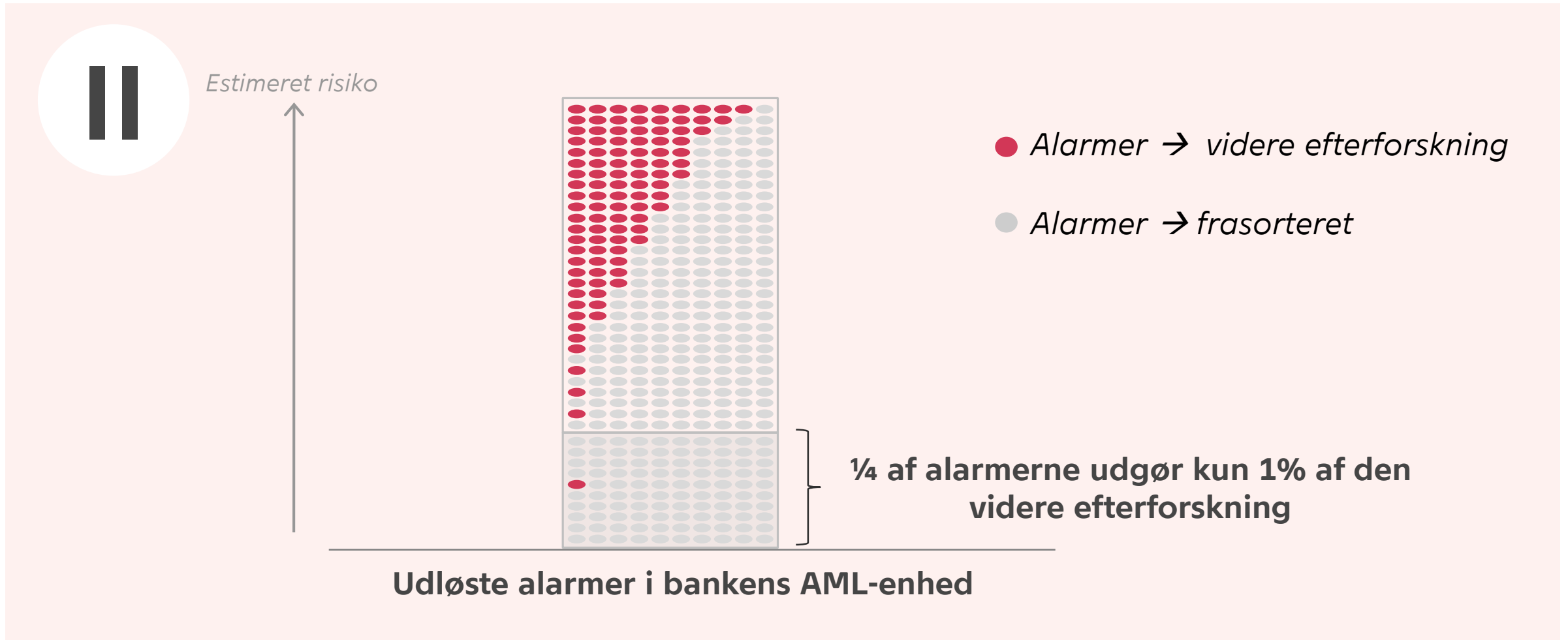
Anvende eksisterende data for, hvad det nuværende system hidtil har fundet



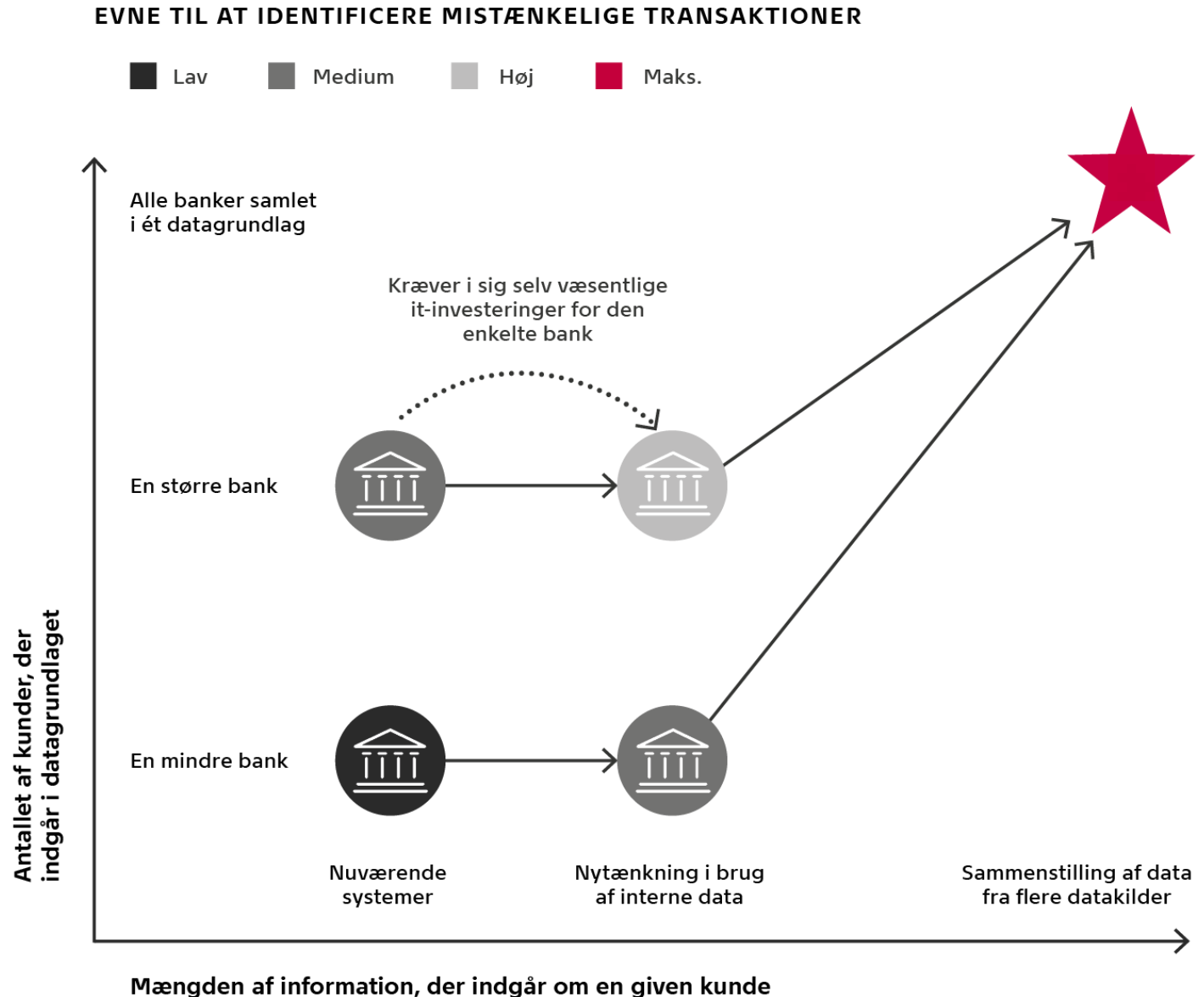
Note: Grafen viser et tilfældigt udsnit af data der og sløret med tilfældig støj for at bevare anonymiteten.



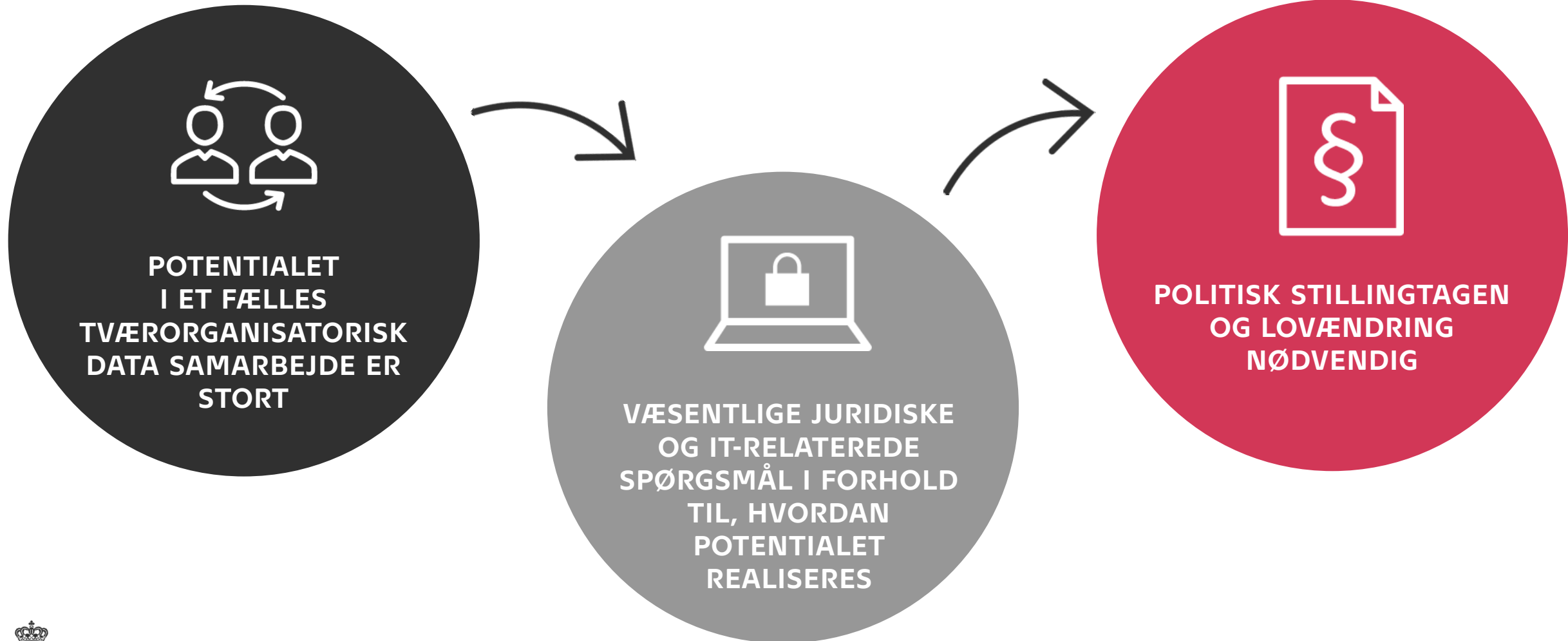
... og samtidig kan en datadrevet tilgang understøtte bedre prioritering af ressourcer hos myndigheder og finanssektoren



Realisering af det fulde potentiale forudsætter sammenstilling af data fra flere banker og myndigheder



Lovgivning er nødvendig for at realisere det fulde potentiale af data i kampen mod økonomisk kriminalitet





Sammenstillet data afslører flere mistænkelige forhold

En risikobaseret metode på baggrund af flere datakilder identificerer dobbelt så mange mistænkelige transaktioner.



Datadrevet indsats giver øget effektivitet og fokus

En udvidet datadrevet tilgang kan understøtte bedre prioritering af ressourcer hos myndigheder og finanssektoren.



Fuldt potentiale kræver lovændring

Det fulde potentiale afhænger af brug af data på tværs af banker og myndigheder. En sådan sammenstilling vil kræve en lovændring.

Mange tak
