

Persondataforordningen og digitale forretningsprocesser

ved hjælp af Dynamic Condition Response (DCR) grafer

Thomas T. Hildebrandt

Leder af forskningsgruppen for
Process Intelligens, Modelling og Optimering

(samarbejde med S. Debois, M. Marquard, D. Basin)

OpenITU

15. september, 2017



Kort om mig selv

2000: PhD i datalogi, Aarhus Universitet

2000-2003: Studieprogramleder for Internet & software teknologi, IT Universitet i København (ITU)

2004-2011: Daglig leder af PhD-skole for ITU, KU, RUC og DTU

2007- Leder af flere forskningsprojekter indenfor sikkerhed og digitalisering af forretningsprocesser sammen med virksomheder bla. Microsoft, Resultmaker, Exformatics, DSB, BaneDanmark, ...

2012-: Konsulent & facilitator af interessegrupper for digitalisering infinet.dk, cfir.dk & videndanmark.dk

Hvad slags data ?

Relevant personhenførbart data: Data der bliver behandlet automatisk eller gemt, og som kan henføres til en person - direkte eller indirekte (navn eller anden ID, lokation & tid, IP nummer, genetisk...)

Fra lønseddel

Dansk Supermarked

Personnummer: 111111
 CPR nummer: 11 11 1111
 Navn: 1111
 Adresse: 1111

Lønopskrift for periode 1. oktober 2011 - 31. oktober 2011

Spørgsmål	Grunder	Enheder	Sum	Skat
1000: Løn 2011 10 11			1111	1111
1001: Fast løn		1111	1111	1111
1002: Variable		1111	1111	1111
1003: Funktionslønsdel		1111	1111	1111
1004: Funktionslønsdel		1111	1111	1111
1005: Adgangsbetrag		1111	1111	1111
1006: Løn 2011 10 11			1111	1111
1007: Løn 2011 10 11			1111	1111
1008: Løn 2011 10 11			1111	1111
1009: Løn 2011 10 11			1111	1111
1010: Løn 2011 10 11			1111	1111
1011: Løn 2011 10 11			1111	1111
1012: Løn 2011 10 11			1111	1111
1013: Løn 2011 10 11			1111	1111
1014: Løn 2011 10 11			1111	1111
1015: Løn 2011 10 11			1111	1111
1016: Løn 2011 10 11			1111	1111
1017: Løn 2011 10 11			1111	1111
1018: Løn 2011 10 11			1111	1111
1019: Løn 2011 10 11			1111	1111
1020: Løn 2011 10 11			1111	1111
1021: Løn 2011 10 11			1111	1111
1022: Løn 2011 10 11			1111	1111
1023: Løn 2011 10 11			1111	1111
1024: Løn 2011 10 11			1111	1111
1025: Løn 2011 10 11			1111	1111
1026: Løn 2011 10 11			1111	1111
1027: Løn 2011 10 11			1111	1111
1028: Løn 2011 10 11			1111	1111
1029: Løn 2011 10 11			1111	1111
1030: Løn 2011 10 11			1111	1111
1031: Løn 2011 10 11			1111	1111
1032: Løn 2011 10 11			1111	1111
1033: Løn 2011 10 11			1111	1111
1034: Løn 2011 10 11			1111	1111
1035: Løn 2011 10 11			1111	1111
1036: Løn 2011 10 11			1111	1111
1037: Løn 2011 10 11			1111	1111
1038: Løn 2011 10 11			1111	1111
1039: Løn 2011 10 11			1111	1111
1040: Løn 2011 10 11			1111	1111
1041: Løn 2011 10 11			1111	1111
1042: Løn 2011 10 11			1111	1111
1043: Løn 2011 10 11			1111	1111
1044: Løn 2011 10 11			1111	1111
1045: Løn 2011 10 11			1111	1111
1046: Løn 2011 10 11			1111	1111
1047: Løn 2011 10 11			1111	1111
1048: Løn 2011 10 11			1111	1111
1049: Løn 2011 10 11			1111	1111
1050: Løn 2011 10 11			1111	1111
1051: Løn 2011 10 11			1111	1111
1052: Løn 2011 10 11			1111	1111
1053: Løn 2011 10 11			1111	1111
1054: Løn 2011 10 11			1111	1111
1055: Løn 2011 10 11			1111	1111
1056: Løn 2011 10 11			1111	1111
1057: Løn 2011 10 11			1111	1111
1058: Løn 2011 10 11			1111	1111
1059: Løn 2011 10 11			1111	1111
1060: Løn 2011 10 11			1111	1111
1061: Løn 2011 10 11			1111	1111
1062: Løn 2011 10 11			1111	1111
1063: Løn 2011 10 11			1111	1111
1064: Løn 2011 10 11			1111	1111
1065: Løn 2011 10 11			1111	1111
1066: Løn 2011 10 11			1111	1111
1067: Løn 2011 10 11			1111	1111
1068: Løn 2011 10 11			1111	1111
1069: Løn 2011 10 11			1111	1111
1070: Løn 2011 10 11			1111	1111
1071: Løn 2011 10 11			1111	1111
1072: Løn 2011 10 11			1111	1111
1073: Løn 2011 10 11			1111	1111
1074: Løn 2011 10 11			1111	1111
1075: Løn 2011 10 11			1111	1111
1076: Løn 2011 10 11			1111	1111
1077: Løn 2011 10 11			1111	1111
1078: Løn 2011 10 11			1111	1111
1079: Løn 2011 10 11			1111	1111
1080: Løn 2011 10 11			1111	1111
1081: Løn 2011 10 11			1111	1111
1082: Løn 2011 10 11			1111	1111
1083: Løn 2011 10 11			1111	1111
1084: Løn 2011 10 11			1111	1111
1085: Løn 2011 10 11			1111	1111
1086: Løn 2011 10 11			1111	1111
1087: Løn 2011 10 11			1111	1111
1088: Løn 2011 10 11			1111	1111
1089: Løn 2011 10 11			1111	1111
1090: Løn 2011 10 11			1111	1111
1091: Løn 2011 10 11			1111	1111
1092: Løn 2011 10 11			1111	1111
1093: Løn 2011 10 11			1111	1111
1094: Løn 2011 10 11			1111	1111
1095: Løn 2011 10 11			1111	1111
1096: Løn 2011 10 11			1111	1111
1097: Løn 2011 10 11			1111	1111
1098: Løn 2011 10 11			1111	1111
1099: Løn 2011 10 11			1111	1111
1100: Løn 2011 10 11			1111	1111

til ID & DNA



Brug af persondata



ikke nyt at benytte persondata i forretningsprocesser....

Digitalisering

Digitaliseringen gør det nemmere at indsamle, bruge og genbruge data



Digitalisering

Digitaliseringen gør det nemmere at indsamle, bruge og genbruge data



...men også at miste overblikket over, hvor data er gemt, hvem der har adgang, hvordan den bruges og til hvilket formål

Mulighed for bevidst misbrug

KRIMI

Skandale: Se og Hør bag ulovlig overvågning af kendte og kongeliges hævekort

MORTEN MÆRSK
FØLG ▾

SIMON ANDERSEN
FØLG ▾

UFFE JØRGENSEN ODDE
FØLG ▾

KARINA SVENSGAARD
FØLG ▾

— 27. APR. 2014 - 21:56



08. DEC. 2016 KL. 18.06

DR dk

Uber overvåger dig nu efter turen er slut

Opdatering af Uber-appen giver det kontroversielle transport-firma udvidede beføjelser til at følge brugernes bevægelser.



eller ved uheld

Kinesere fik ved fejl udleveret danske CPR-numre

Godt fem millioner danske CPR-numre og helbredsoplysninger blev ved en fejl leveret til kinesisk visummyndighed. Det skriver Datatilsynet i en afgørelse.

🕒 20. juli 2016 kl. 14:28

Information

Styrelseslæge ville sende følsomme patientdata til sig selv: Havnede hos it-kriminelle

Styrelsen for Patientsikkerhed oplyser, at der ikke alene er lækket patientdata, men at de 'uden for enhver tvivl' er havnet hos kriminelle datahøstere.

Henning Mølsted  @Henningcph Mandag, 5. september 2016 - 15:55

81

version

Persondataforordningen



siger blandt andet at:

Persondataforordningen



siger blandt andet at:

Persondata må - by-design & default - kun benyttes, når det er nødvendigt til et oplyst og eksplicit godkendt *formål* (bla. artikel 5 og 12)

Persondataforordningen



siger blandt andet at:

Persondata må - by-design & default - kun benyttes, når det er nødvendigt til et oplyst og eksplicit godkendt *formål* (bla. artikel 5 og 12)

“Personoplysningerne bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres behandling. Dette kræver navnlig, at det sikres, at perioden for opbevaring af personoplysningerne ikke er længere end strengt nødvendigt “

Persondataforordningen



siger blandt andet at:

Persondata må - by-design & default - kun benyttes, når det er nødvendigt til et oplyst og eksplicit godkendt *formål* (bla. artikel 5 og 12)

“Personoplysningerne bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres behandling. Dette kræver navnlig, at det sikres, at perioden for opbevaring af personoplysningerne ikke er længere end strengt nødvendigt “

Persondataforordningen



siger blandt andet at:

Persondata må - by-design & default - kun benyttes, når det er nødvendigt til et oplyst og eksplicit godkendt *formål* (bla. artikel 5 og 12)

“Personoplysningerne bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres behandling. Dette kræver navnlig, at det sikres, at perioden for opbevaring af personoplysningerne ikke er længere end strengt nødvendigt “

Man skal kunne gøre rede for, hvordan man har sikret sig:

Persondataforordningen



siger blandt andet at:

Persondata må - by-design & default - kun benyttes, når det er nødvendigt til et oplyst og eksplicit godkendt *formål* (bla. artikel 5 og 12)

“Personoplysningerne bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres behandling. Dette kræver navnlig, at det sikres, at perioden for opbevaring af personoplysningerne ikke er længere end strengt nødvendigt “

Man skal kunne gøre rede for, hvordan man har sikret sig:

“For at sikre, at personoplysninger ikke opbevares i længere tid end nødvendigt, bør den dataansvarlige indføre tidsfrister for sletning eller periodisk gennemgang. “

Krav til den dataansvarlige

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål
- kunne slette eller anonymisere persondata

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål
- kunne slette eller anonymisere persondata
- kunne udlevere persondata i maskinlæsbart format

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål
- kunne slette eller anonymisere persondata
- kunne udlevere persondata i maskinlæsbart format
- kunne forklare automatiserede beslutninger

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål
- kunne slette eller anonymisere persondata
- kunne udlevere persondata i maskinlæsbart format
- kunne forklare automatiserede beslutninger
- sikre at persondata er up-to-date før de bruges

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål
- kunne slette eller anonymisere persondata
- kunne udlevere persondata i maskinlæsbart format
- kunne forklare automatiserede beslutninger
- sikre at persondata er up-to-date før de bruges
- dokumentere behandling og overholdelse af lov

Krav til den dataansvarlige

Forordningen tvinger den dataansvarlige til at

- oplyse om formålet med indsamling af persondata
- kun at benytte persondata til det oplyste formål
- kun at benytte persondata, hvis nødvendigt
- kun at gemme persondata med gyldigt formål
- kunne slette eller anonymisere persondata
- kunne udlevere persondata i maskinlæsbart format
- kunne forklare automatiserede beslutninger
- sikre at persondata er up-to-date før de bruges
- dokumentere behandling og overholdelse af lov

og forpligte tredjeparts behandlere at gøre det samme!

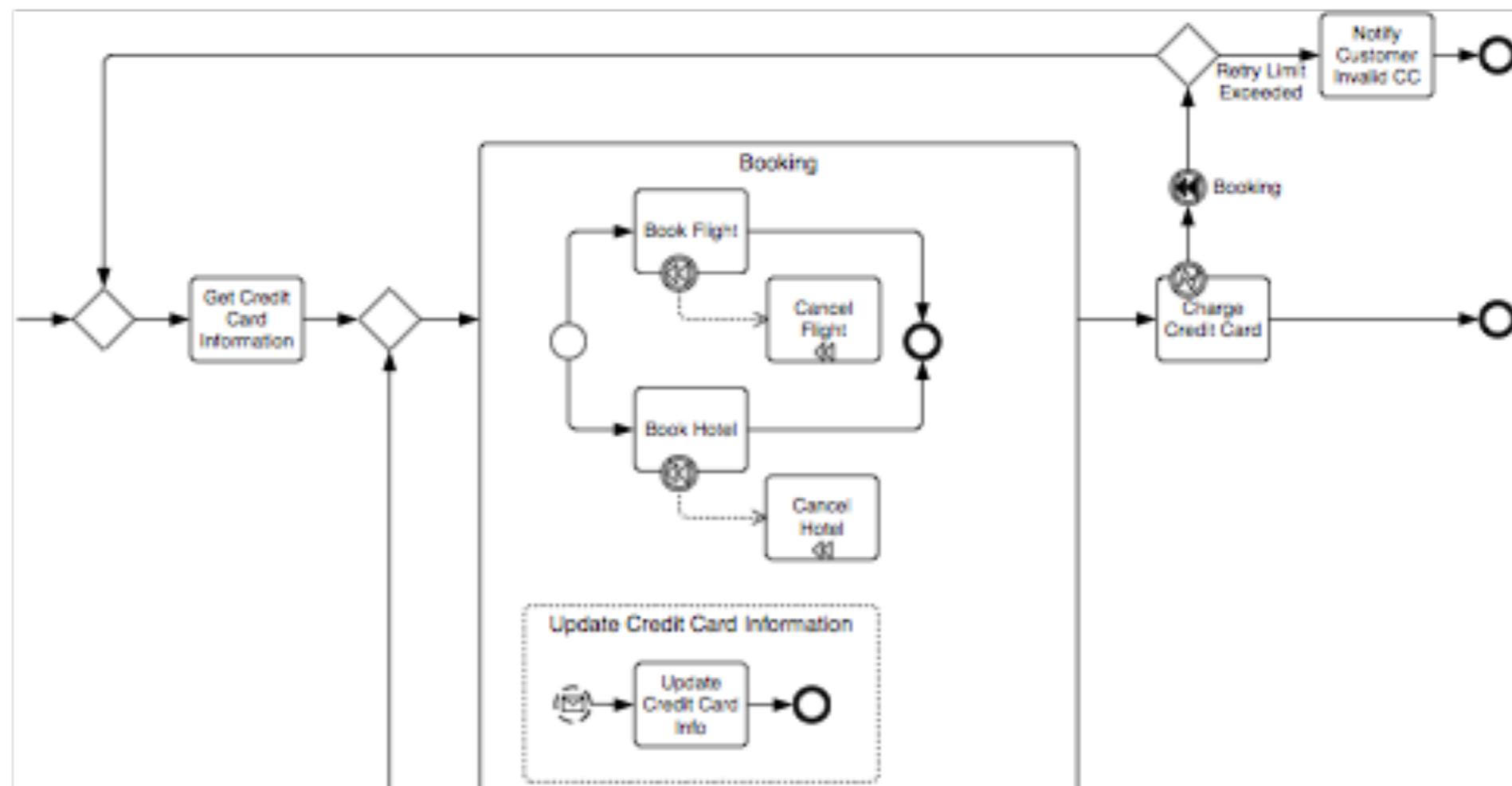
Kend formålet med databehandling

Strengt nødvendigt at få styr på formål for persondataindsamling & -behandling!



Formål = forretningsproces

Skal vi så til at beskrive alle vores forretningsprocesser som detaljerede rutediagrammer?



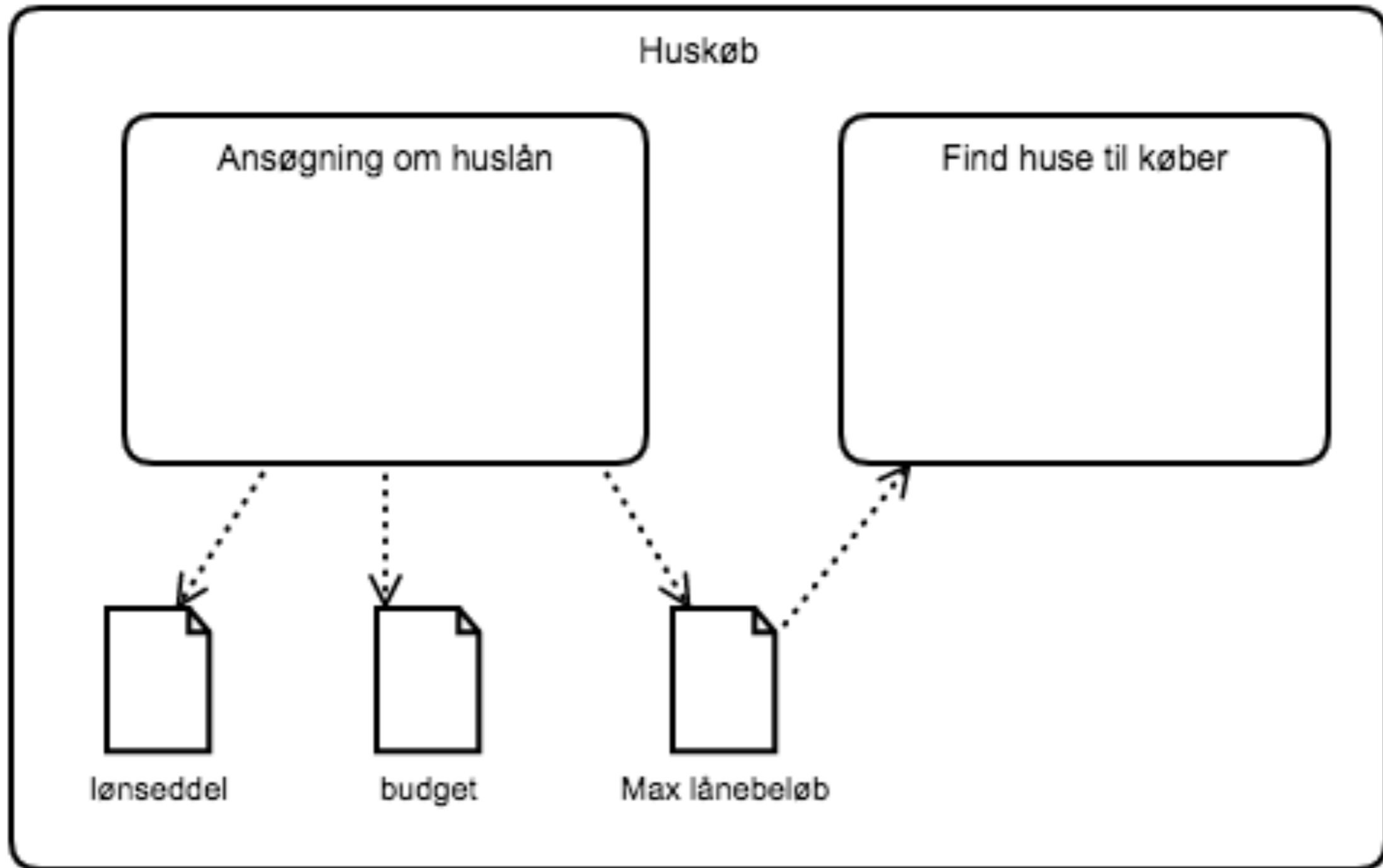
Nej, rutediagrammer er ufleksible, dyre og svære at vedligeholde

Data-indsamling & behandling

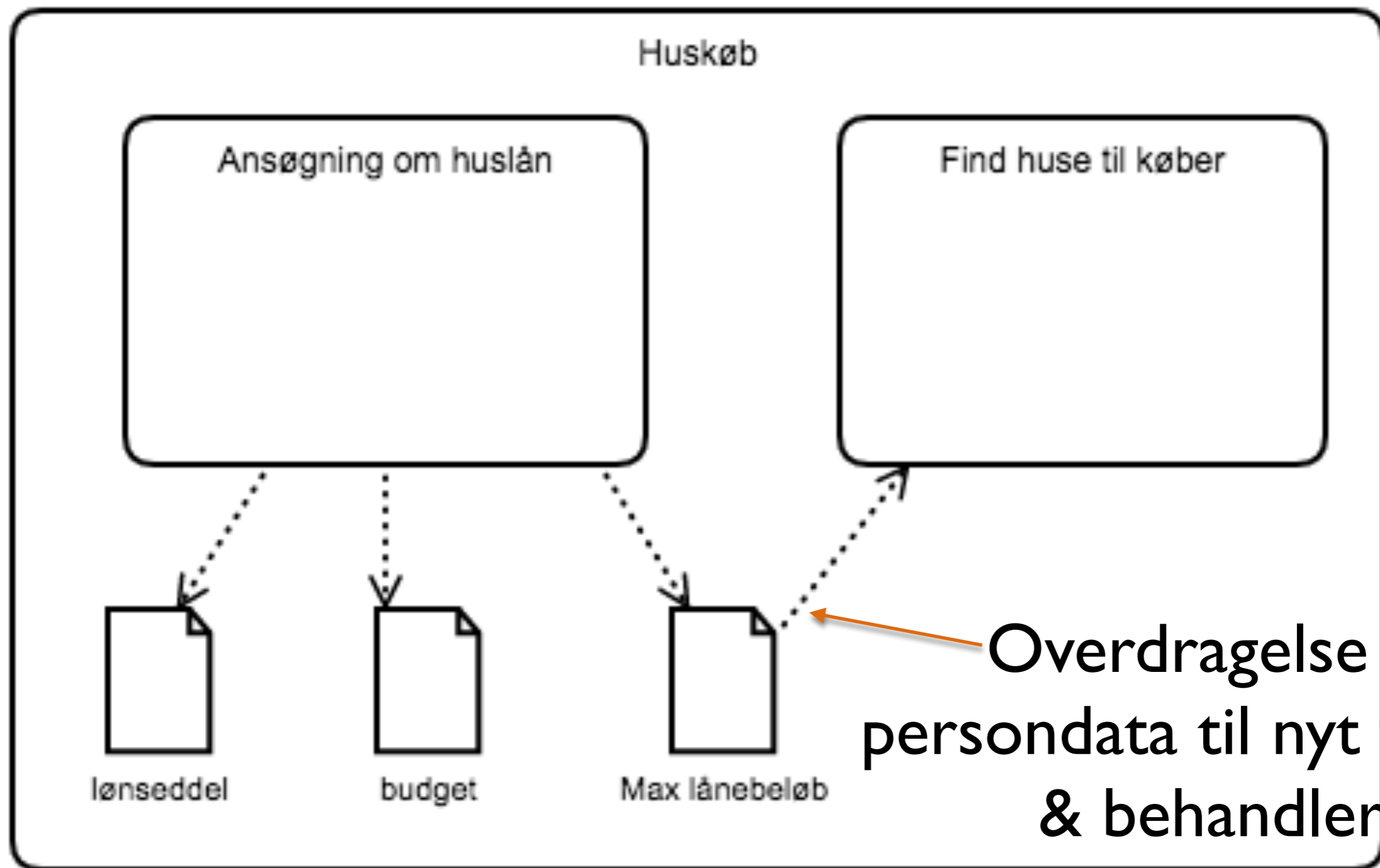
- Kortlæg aktiviteter der *indsamler* persondata og identificer *formålet*, dvs. de forretningsprocesser der *behandler* den indsamlede persondata
- Dokumenter *begrundelse* for at data er nødvendig til formålet. Husk at der kan være anden lovgivning.

Udfordring: Forretningsprocesser kendes bedst af forretningen - og er evigt foranderlige!

Eksempel - huskøb



Eksempel - huskøb



Privacy by design

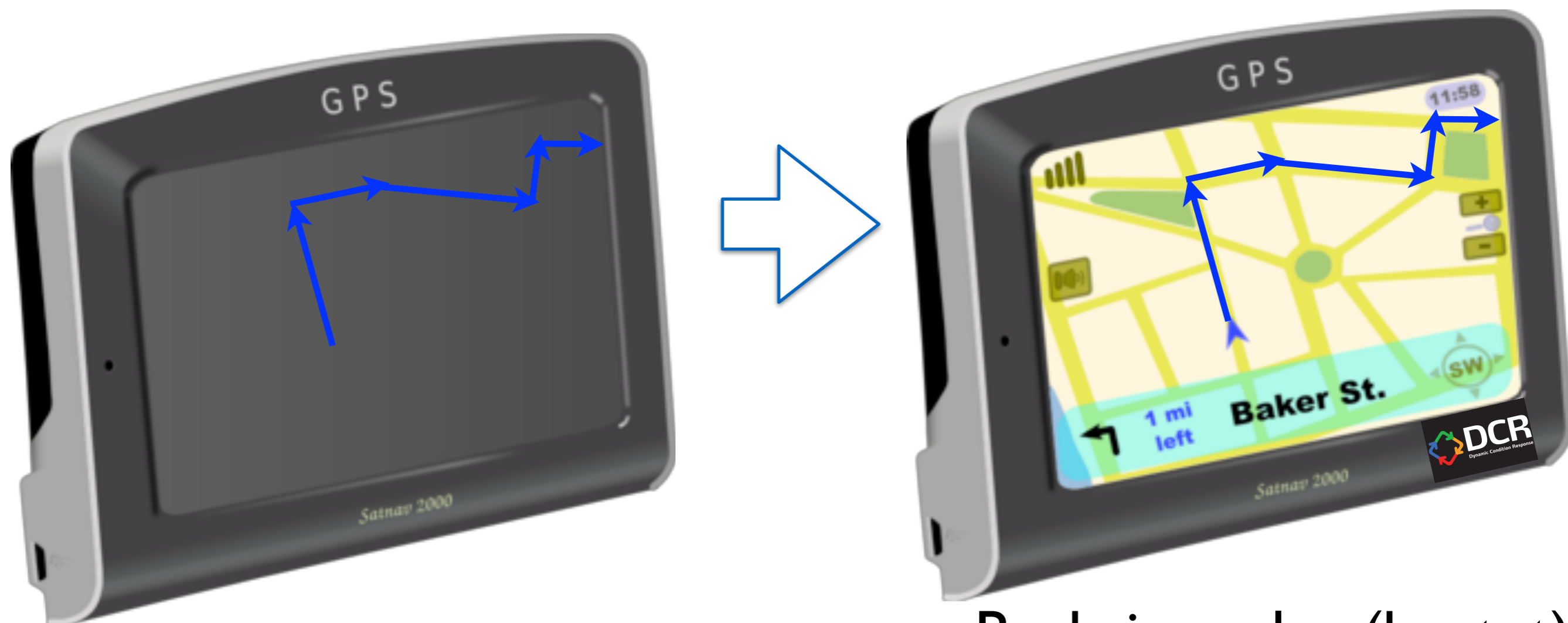
- Etabler mekanismer der sikrer
 - tilsagn om brug af persondata *før* den indsamles
 - brug og adgang begrænset til lovligt formål (proces)
 - sletning/anonymisering af data efter lovligt formål (proces) er ophørt

Fra *rollebaseret* til *procesbaseret* adgangskontrol

Udfordring: Forretningsprocesser skal kunne *forandres!*

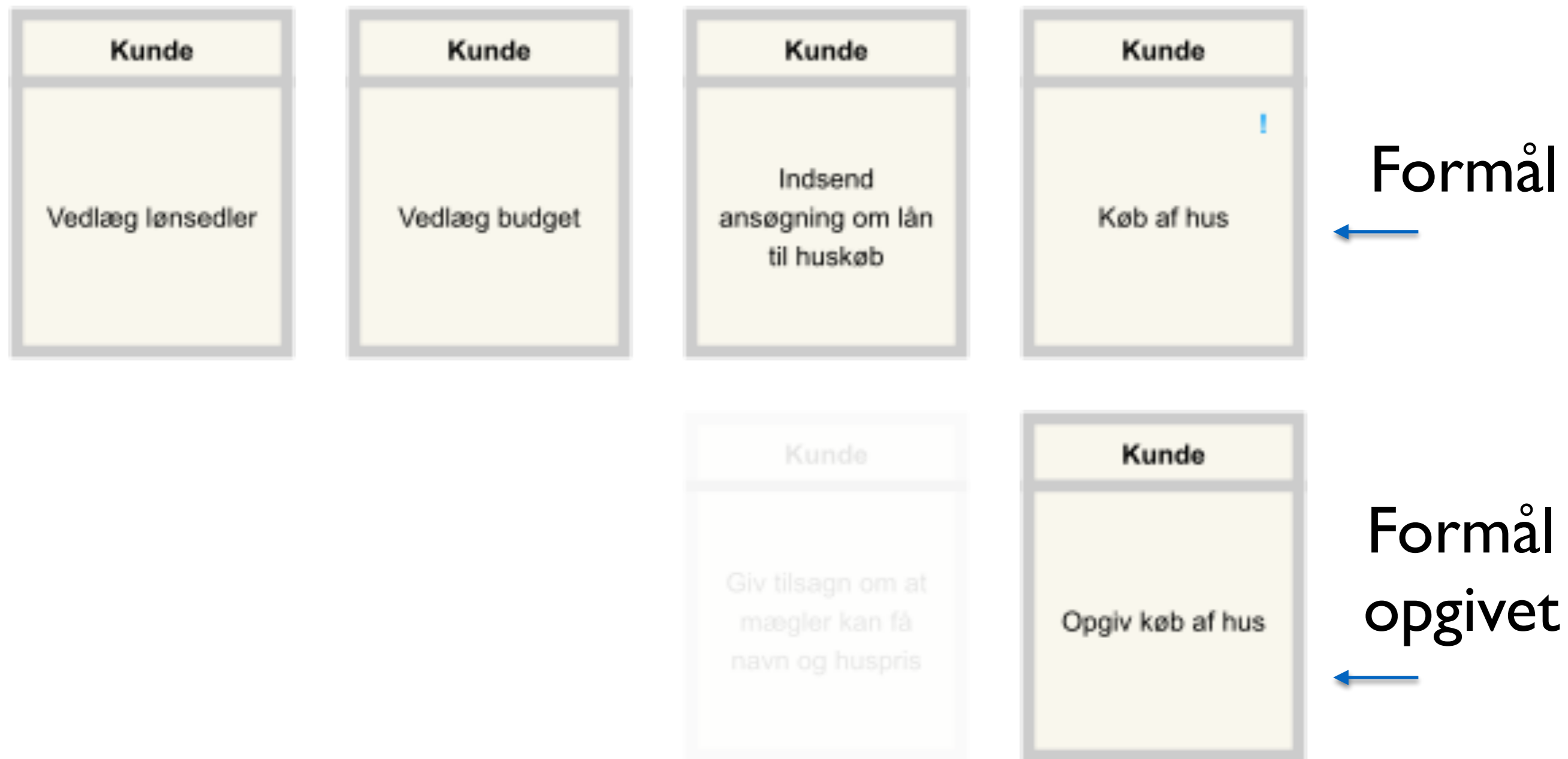
Dynamic Condition Response (DCR) Grafer

Istedet for at beskrive ruter



Beskriv regler (kortet)
simuler og beregn ruter

Eksempel: Lån til huskøb



The screenshot displays the DCR (Digital Case Recorder) interface for a process titled "Lån til huskøb". The interface includes a top navigation bar with the DCR logo, the process name, and a "Simuler" button. Below this is a menu with options like "Fil", "Indsæt", "Rediger", "Simulering", "Apps", "Vindue", and "Hjælp".

The main workspace shows a process flow with several steps, each associated with a role:

- Kunde** (Customer):
 - Vedlæg lønsedler
 - Vedlæg budget
 - Indsend ansøgning om lån til huskøb
 - Køb af hus
 - Opgiv køb af hus
- Bank** (Bank):
 - Beregning af max lånesum
 - Opret lån
 - Afvis lån
- Mægler** (Broker):
 - Find mulige huse

On the right side, there is a "Filtre" (Filter) panel with the following settings:

- Niveauer** (Levels): "Global" is selected.
- Vis alt** (Show all): A green bar indicating all levels are visible.
- 1 Niveau** (1 Level): A list showing the current filter level.
- Roller** (Roles): "Bank", "Kunde", and "Mægler" are listed with checkboxes.
- Grupper** (Groups): "Forretningsproces" (Business process) is selected, and "GDPR" is also listed.

The screenshot displays the DCR software interface for 'Lån til huskøb'. The top navigation bar includes the DCR logo, the title 'Lån til huskøb', a 'Simuler' button, and user controls for language (da), zoom (50%), notifications, and the user 'Tthildebrandt'. Below the navigation bar are menu items: Fil, Indsæt, Rediger, Simulering, Apps, Vindue, and Hjælp.

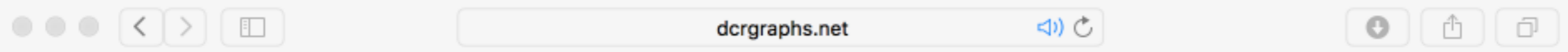
The main workspace shows a process flow with steps categorized by role:

- Kunde (Customer):** Vedlæg lønsedler, Vedlæg budget, Indsend ansøgning om lån til huskøb, Køb af hus, Giv tilsagn om at mægler kan få navn og huspris, Opgiv køb af hus.
- Bank:** Beregning af max lånesum, Opret lån, Anonymiser data, Afvis lån.
- Mægler (Broker):** Find mulige huse, Anonymiser data.

Red boxes highlight specific steps: 'Giv tilsagn om at mægler kan få navn og huspris', 'Anonymiser data' (under Bank), and 'Anonymiser data' (under Mægler).

The right-hand sidebar contains a 'Filtre' panel with the following sections:

- Niveauer:** Nulstil, Global (checked), Vis alt, 1 Niveau.
- Roller:** Nulstil, Vælg Alle, Bank, Kunde, Mægler.
- Grupper:** Nulstil, Vælg Alle, Forretningsproces (checked), GDPR (checked).



DCR Lån til huskøb Simuler

da 100% Tthildebrandt

Fil Indsæt Rediger Simulering Apps Vindue Hjælp

Kunde

Vedlæg lønsedler

Kunde

Vedlæg budget

Kunde

Indsend ansøgning om lån til huskøb

Kunde

Køb af hus

Kunde

Giv tilsagn om at mægler kan få navn og huspris

Kunde

Opgiv køb af hus

Bank

Beregning af max lånesum

Bank

Opret lån

Bank

Anonymiser data

Bank

Afvis lån

Filtre

Niveauer Nulstil Global

Vis alt

1 Niveau

Roller Nulstil Vælg Alle

Bank

Kunde

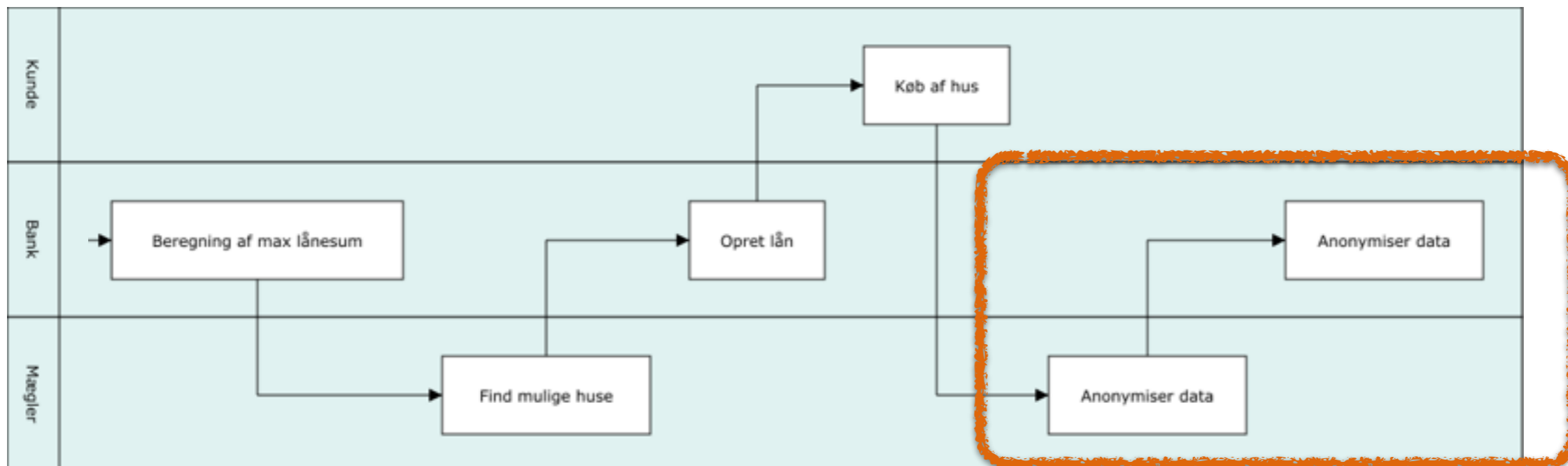
Mægler

Grupper Nulstil Vælg Alle

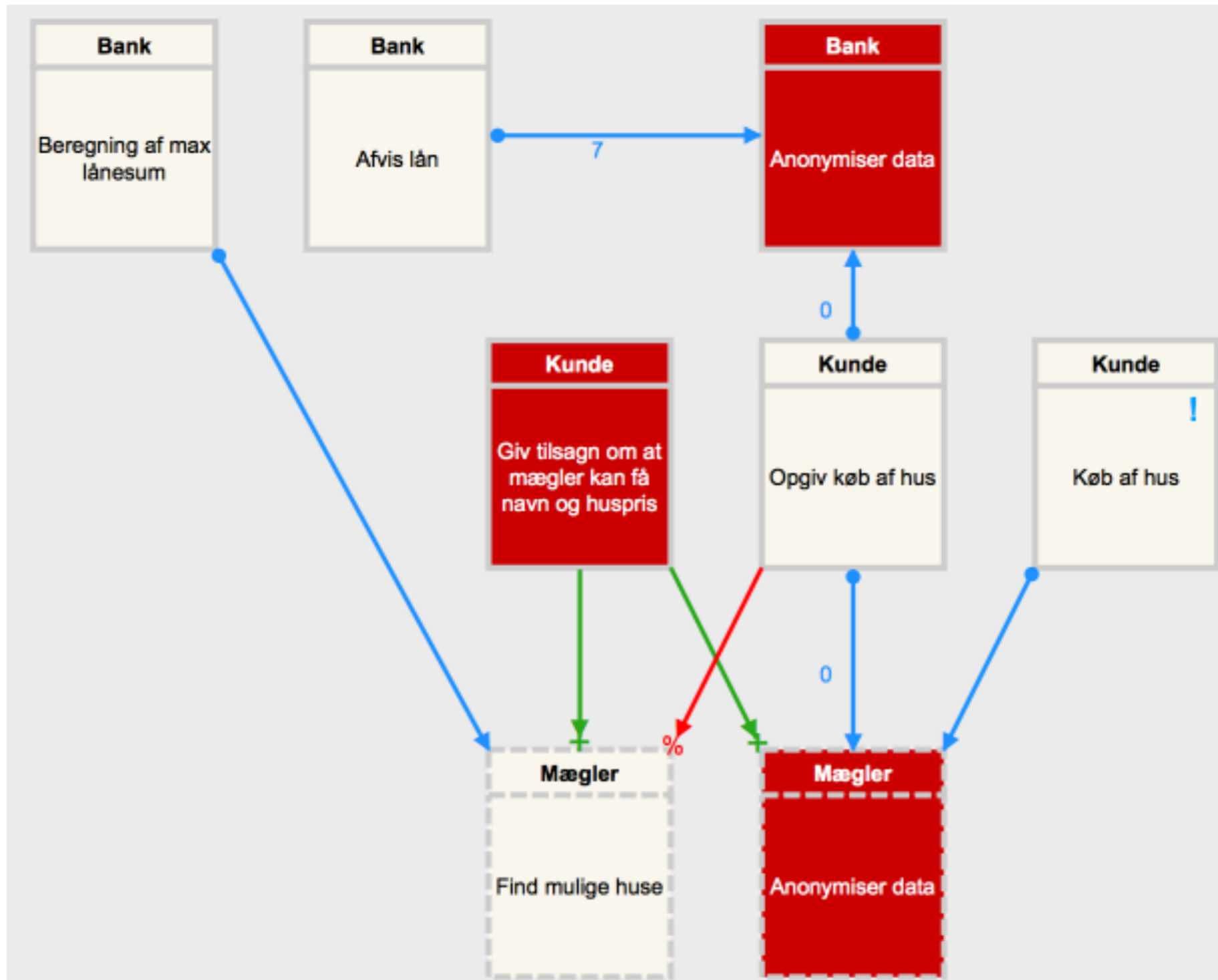
Forretningsproces

GDPR

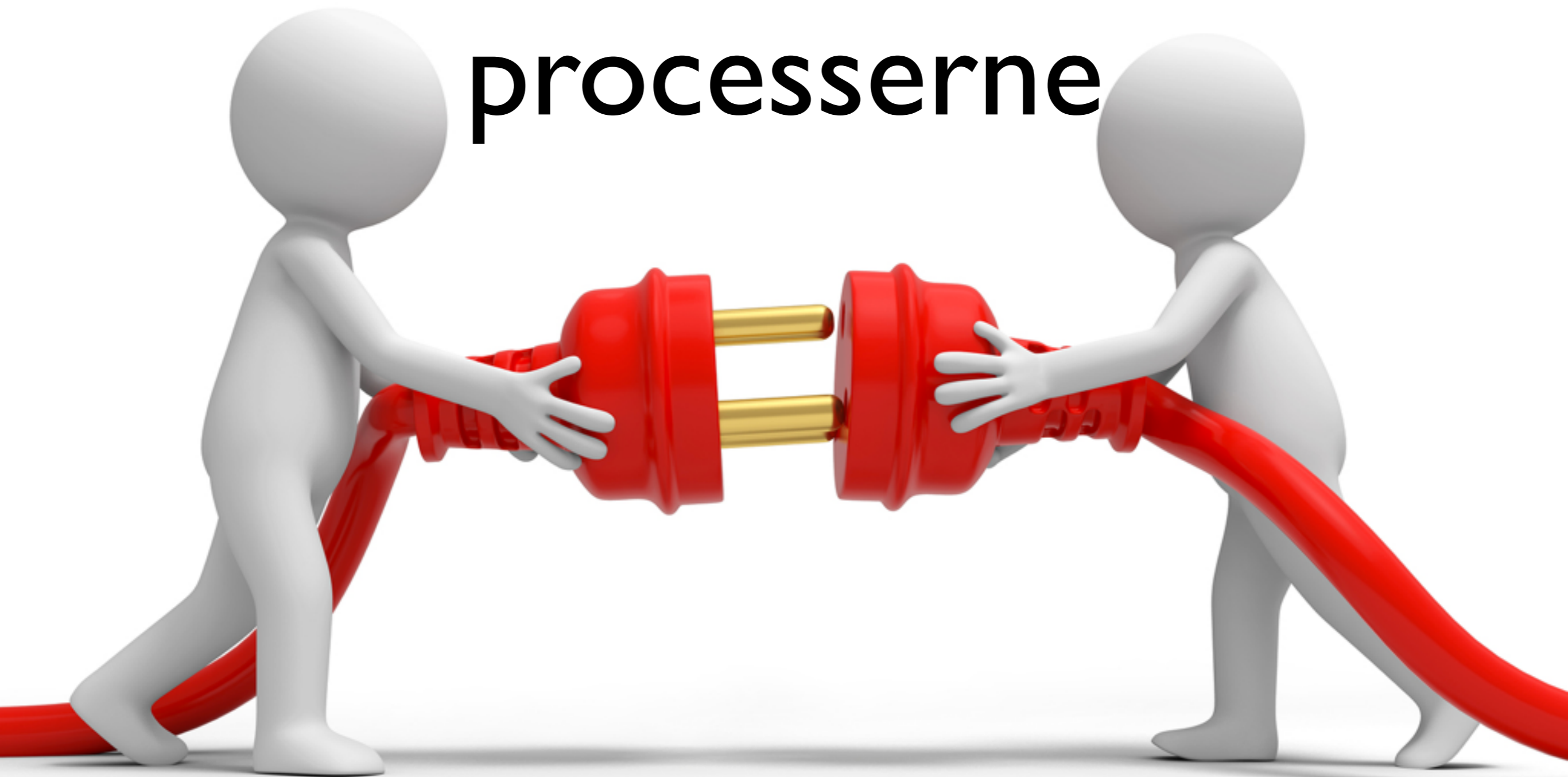
Scenarie med hensyn til GDPR



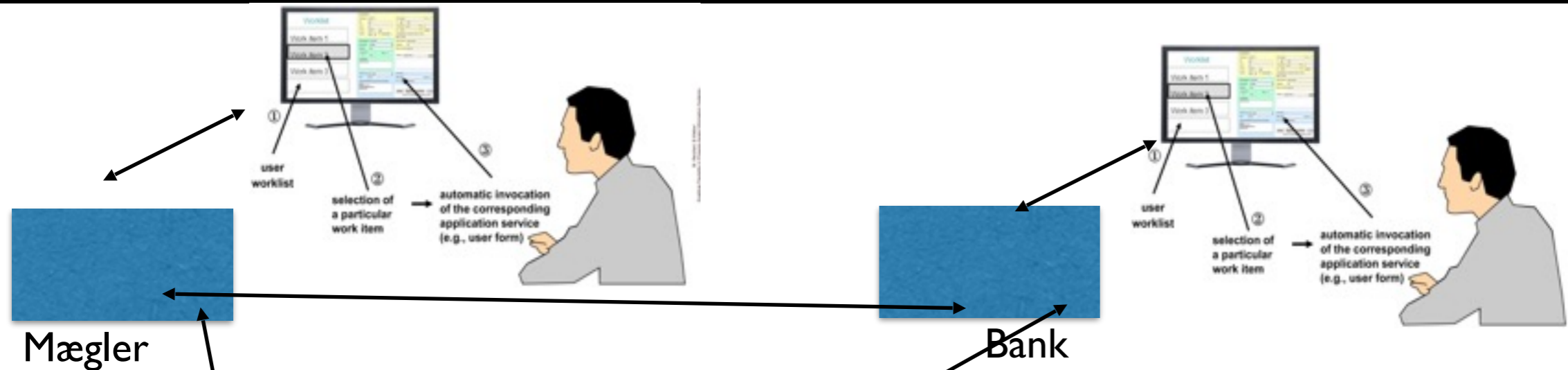
GDPR regler



Sæt strøm til
processerne



Overvågning

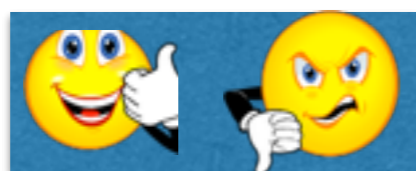
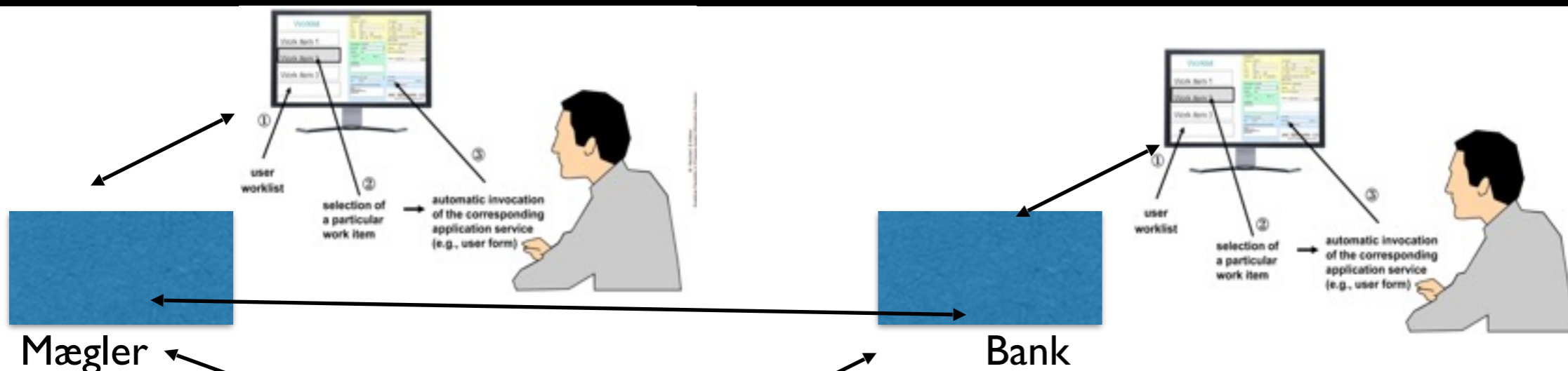


hændelser (events)



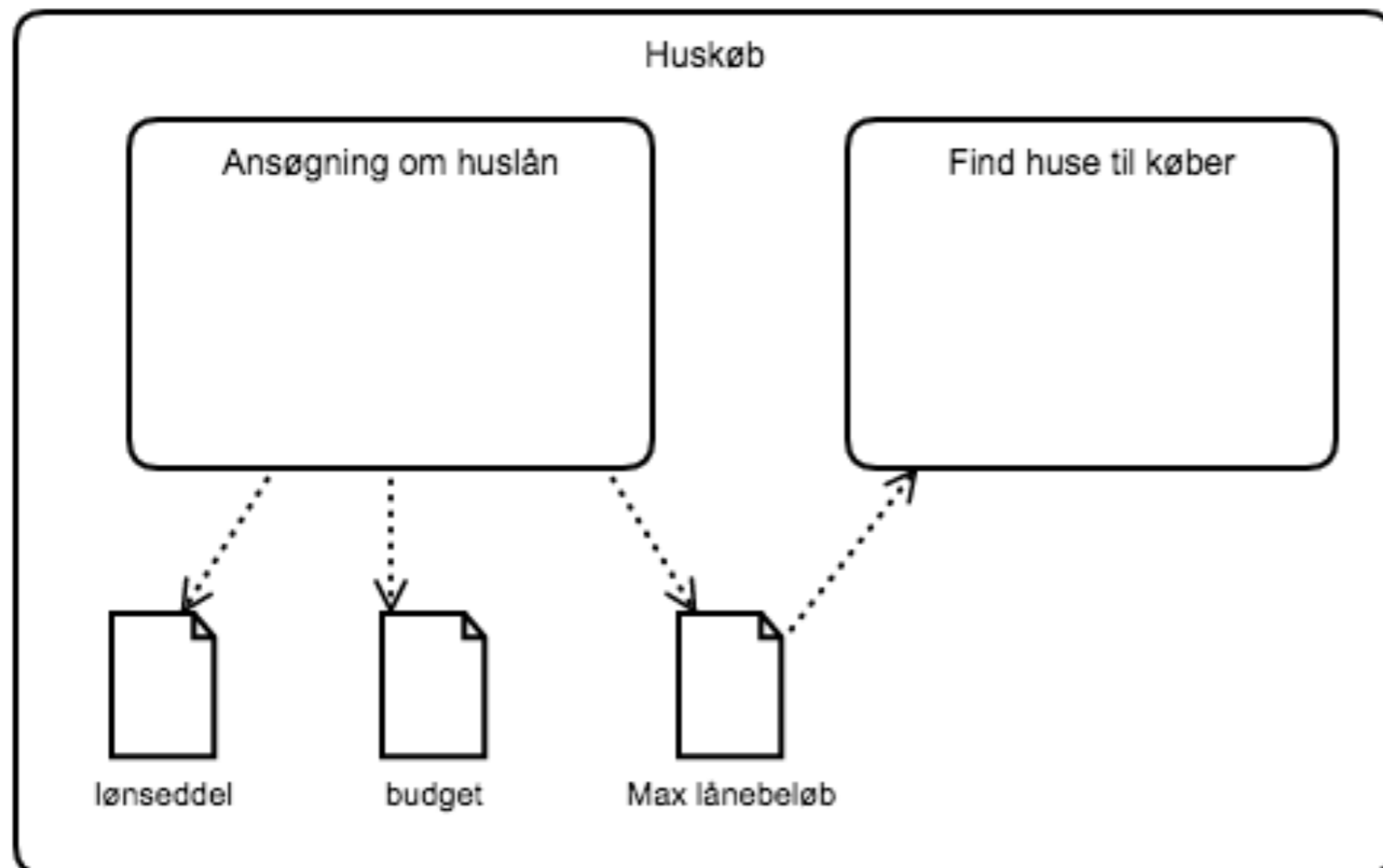
Compliance monitor

Proaktiv compliance



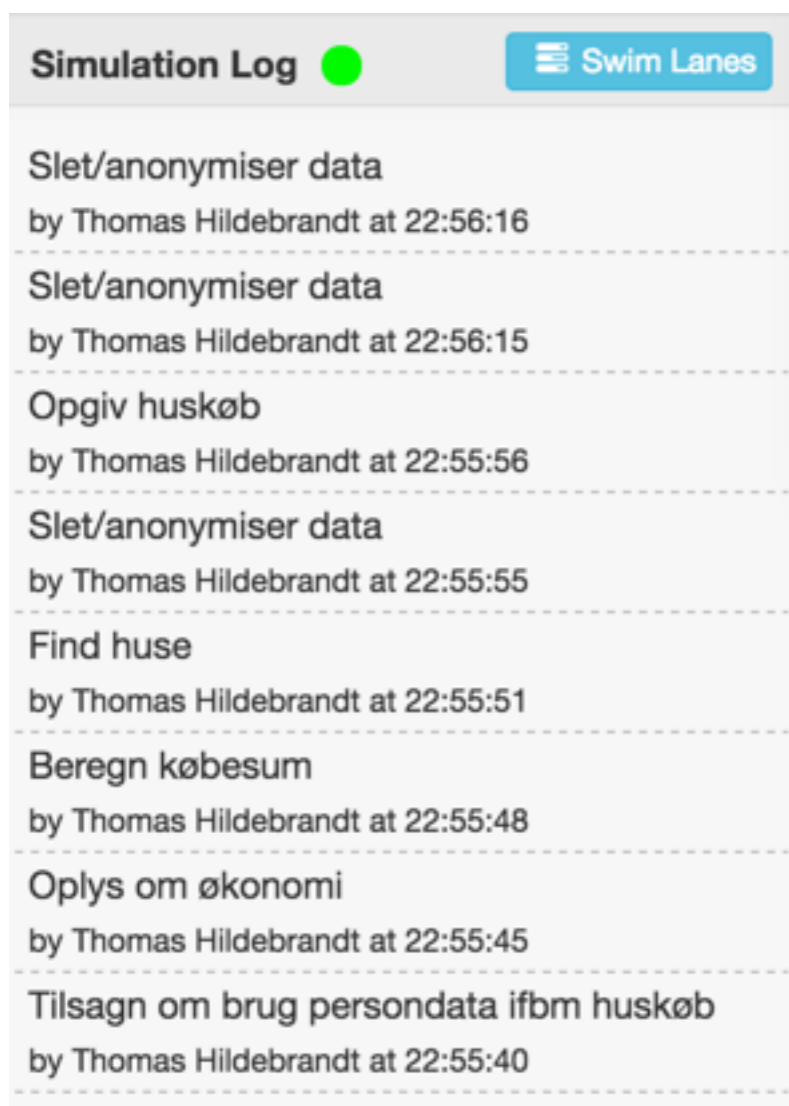
Proactive Policy Enforcement Point
(kan bede om at få udført handlinger om nødvendigt, f.eks. tilsagn eller sletning af data)

Perspektiver: Håndtering af tilsagn

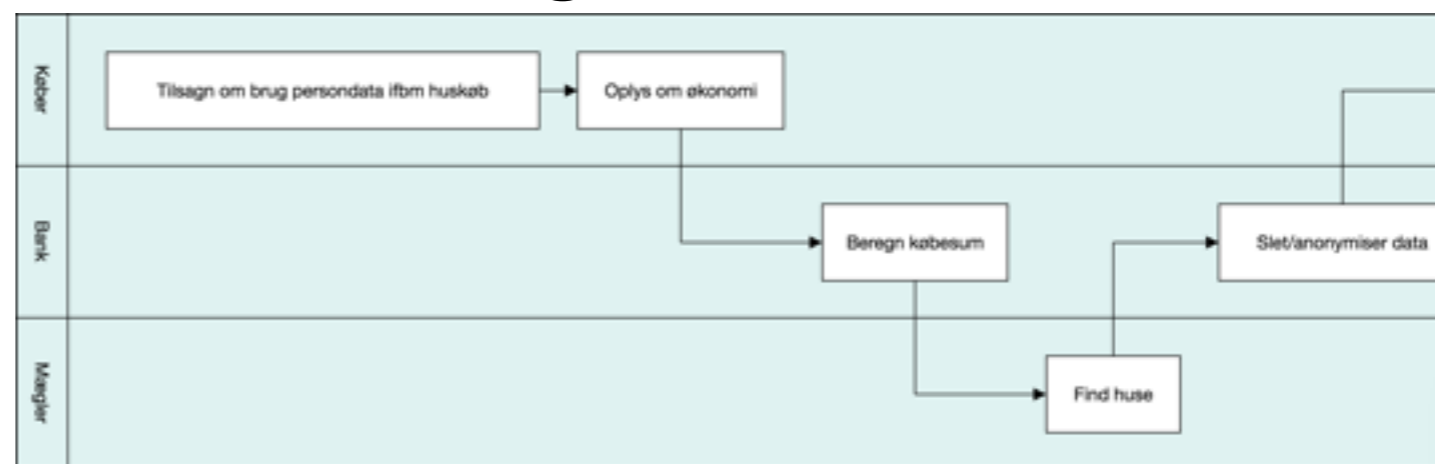


X Giv tilsagn til at Max. lånebeløb benyttes af mægler til at finde huse


Perspektiver: Process Mining



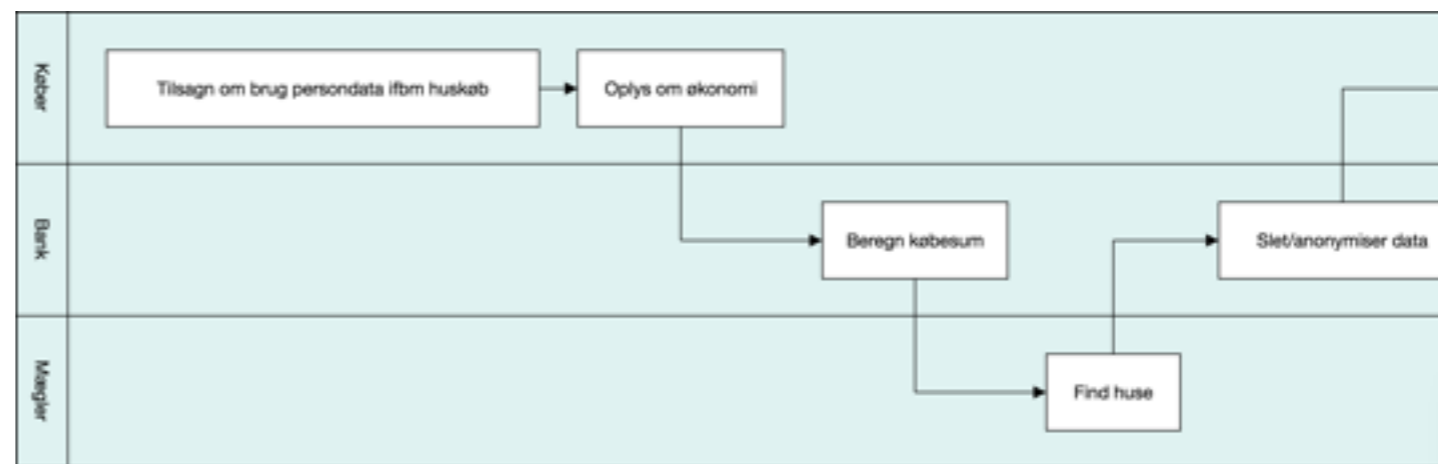
Analyser log-filer og udled ruter og dataflow



Perspektiver: Process Mining

Simulation Log	Swim Lanes
Slet/anonymiser data by Thomas Hildebrandt at 22:56:16	
Slet/anonymiser data by Thomas Hildebrandt at 22:56:15	
Opgiv huskøb by Thomas Hildebrandt at 22:55:56	
Slet/anonymiser data by Thomas Hildebrandt at 22:55:55	
Find huse by Thomas Hildebrandt at 22:55:51	
Beregn købesum by Thomas Hildebrandt at 22:55:48	
Oplys om økonomi by Thomas Hildebrandt at 22:55:45	
Tilsagn om brug persondata ifbm huskøb by Thomas Hildebrandt at 22:55:40	

Analyser log-filer og udled ruter og dataflow



Summa summarum

Nødvendigt med agil kortlægning af de faktiske processer - med fokus på formål og databehandling

Dynamic Condition Response Graphs DCRGraphs.com:
Fleksible proceskort der kan vedligeholdes, simuleres og analyseres

Grundlaget for process-støtte i næste generation af KMD
WorkZone

Regel-baseret tilgang:
Ekstra handlinger f.eks. persondatahåndtering kan flettes ind og ud

Automatisering:
Mulighed for overvågning og proaktiv compliance