Persondataforordningen og digitale forretningsprocesser

ved hjælp af Dynamic Condition Response (DCR) grafer

Thomas T. Hildebrandt
Leder af forskningsgruppen for
Process Intelligens, Modellering og Optimering

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

OpenITU
15. september, 2017

IT UNIVERSITY OF COPENHAGEN

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 infinit.dk, cfir.dk & videndanmark.dk

Hvad slags data ?

Relevant personhenførbar 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

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

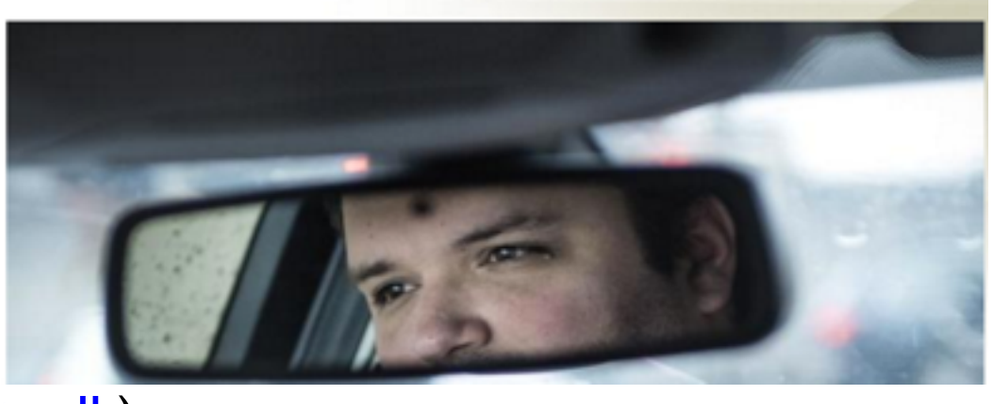
BT

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 version2

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

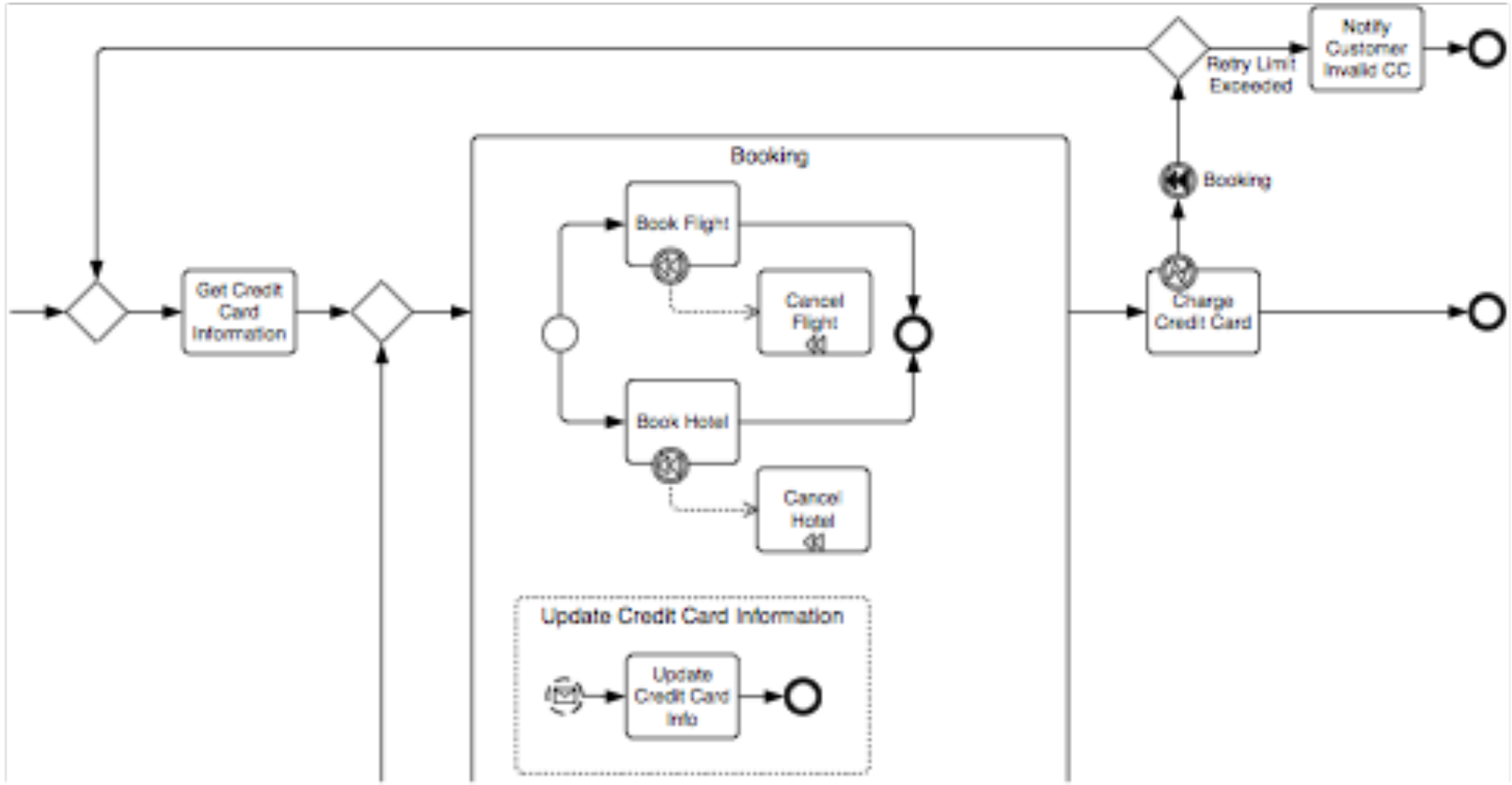
og forpligte tredjeparts behandlere at gøre det samme!

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

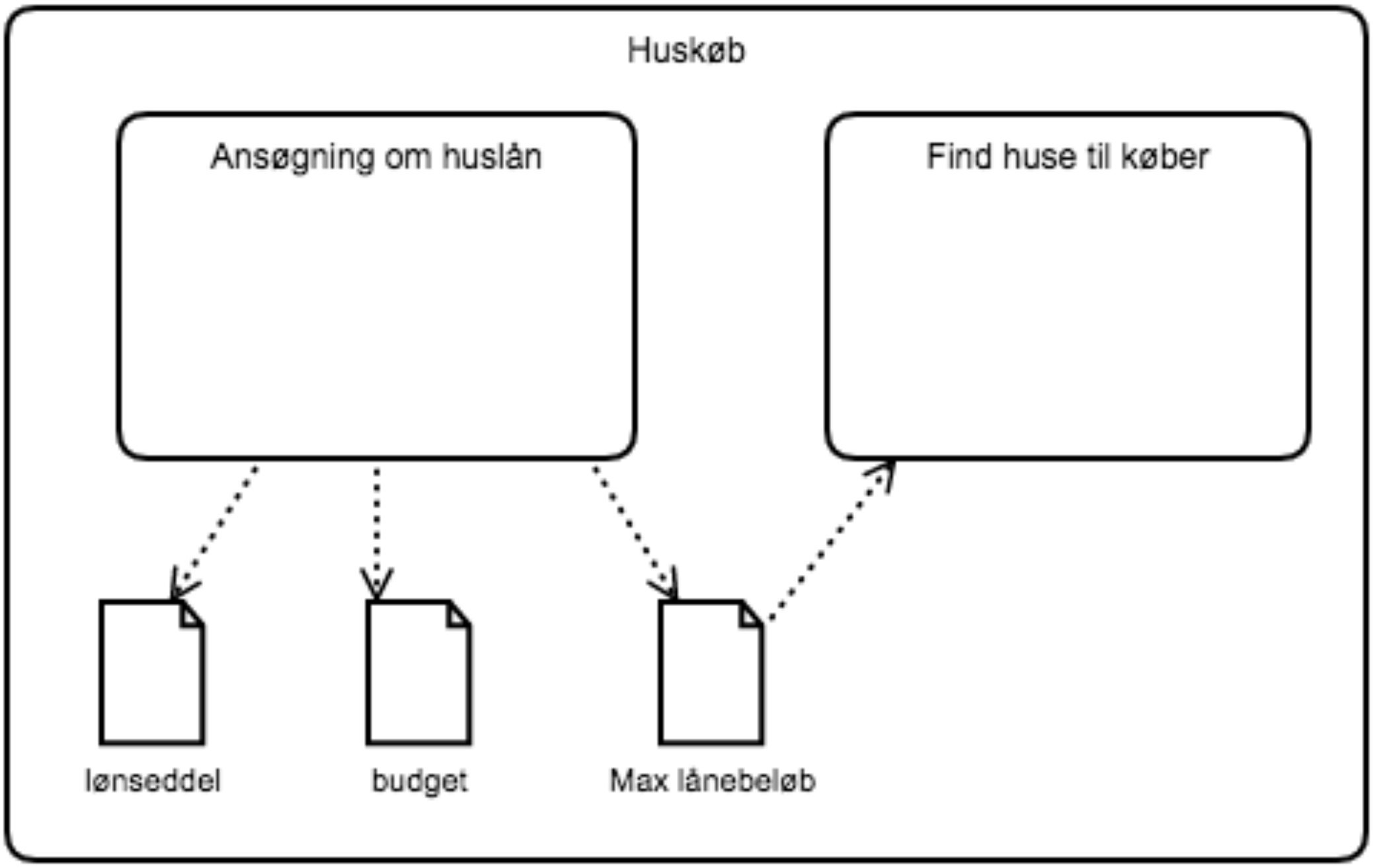
- Kortlæg aktiviteter der *indsamler* persondata og identificer *formålet*, dvs. de forretningsprocesser der *behandler* den indsamlede persondata

- 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!

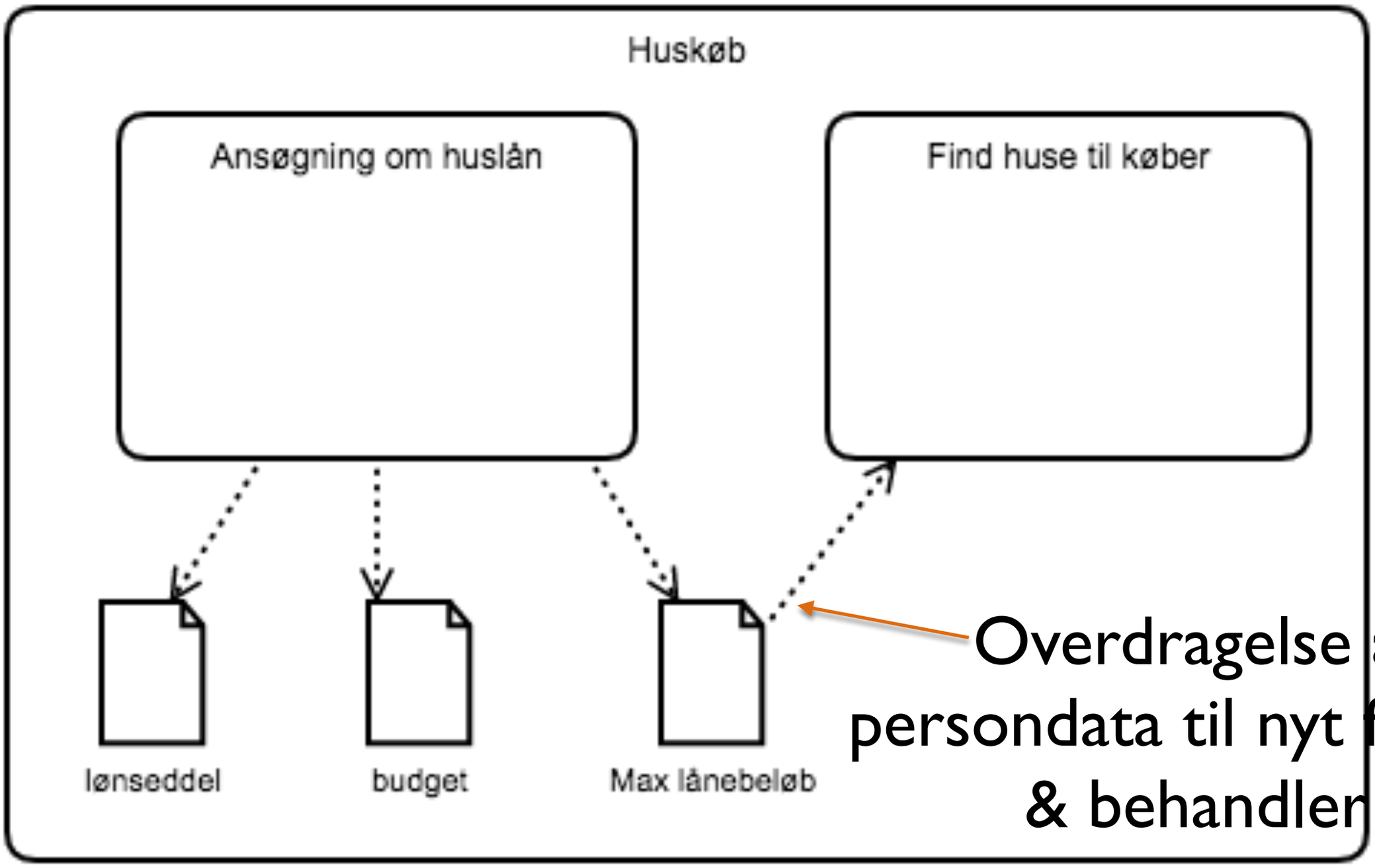
Thomas T. Hildebrandt (hilde@itu.dk)

Eksempel - huskøb



Thomas T. Hildebrandt (hilde@itu.dk)

Eksempel - huskøb



Thomas T. Hildebrandt (hilde@itu.dk)

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

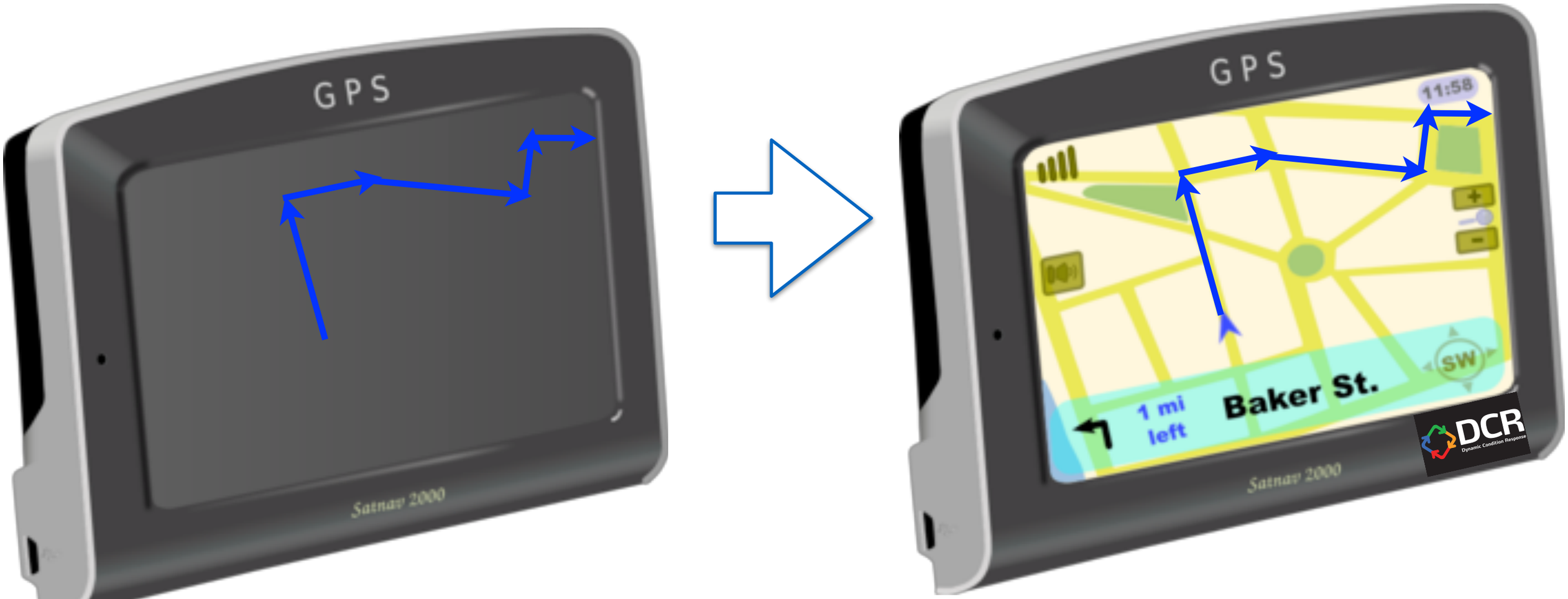
Fra *rollebaseret* til *procesbaseret* adgangskontrol

Udfordring: Forretningsprocesser skal kunne *forandres*!

Thomas T. Hildebrandt (hilde@itu.dk)

Dynamic Condition Response (DCR) Grafer

Istedet for at beskrive ruter



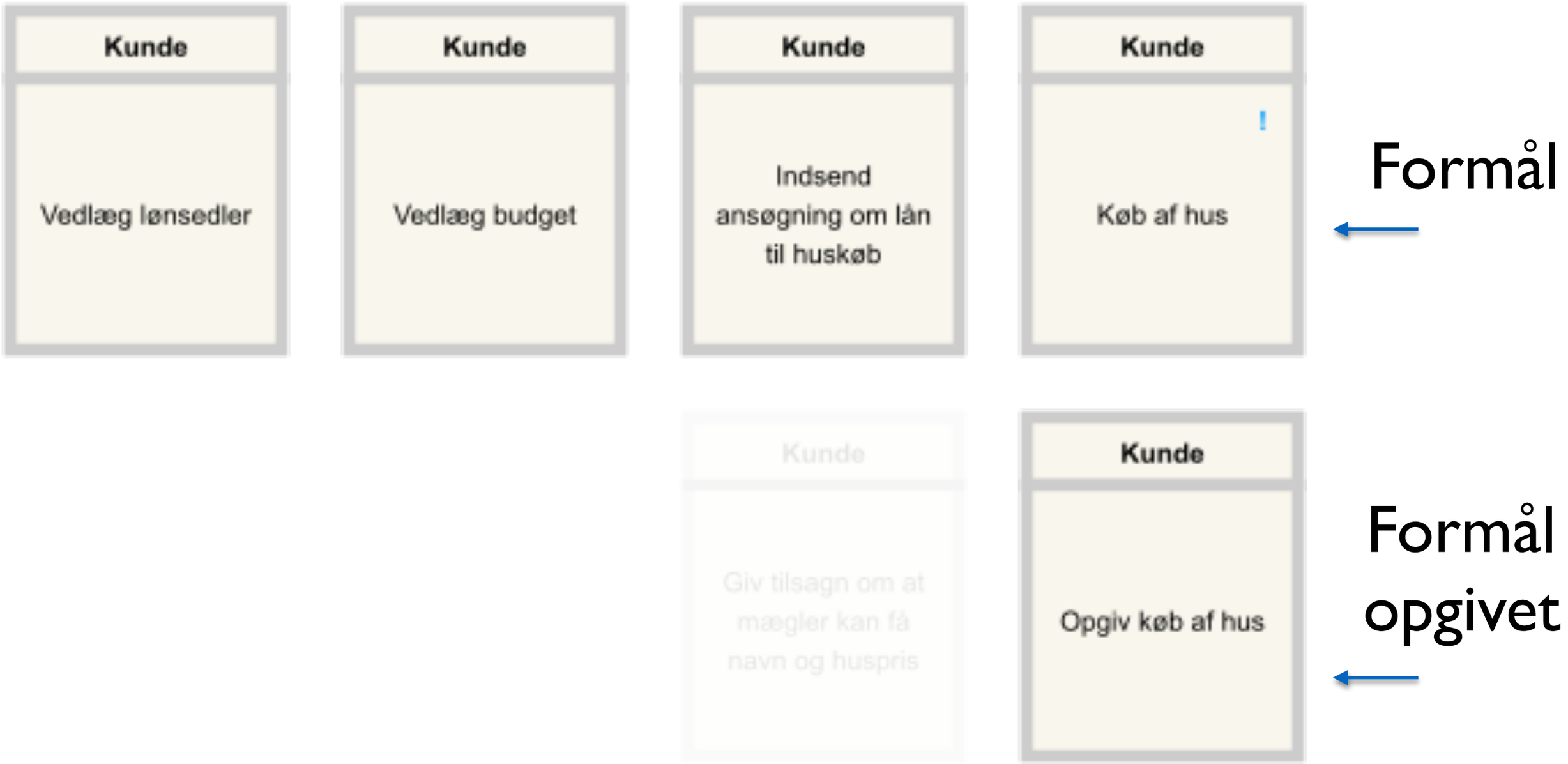
Beskriv regler (kortet) simuler og beregn ruter

Thomas T. Hildebrandt (hilde@itu.dk)

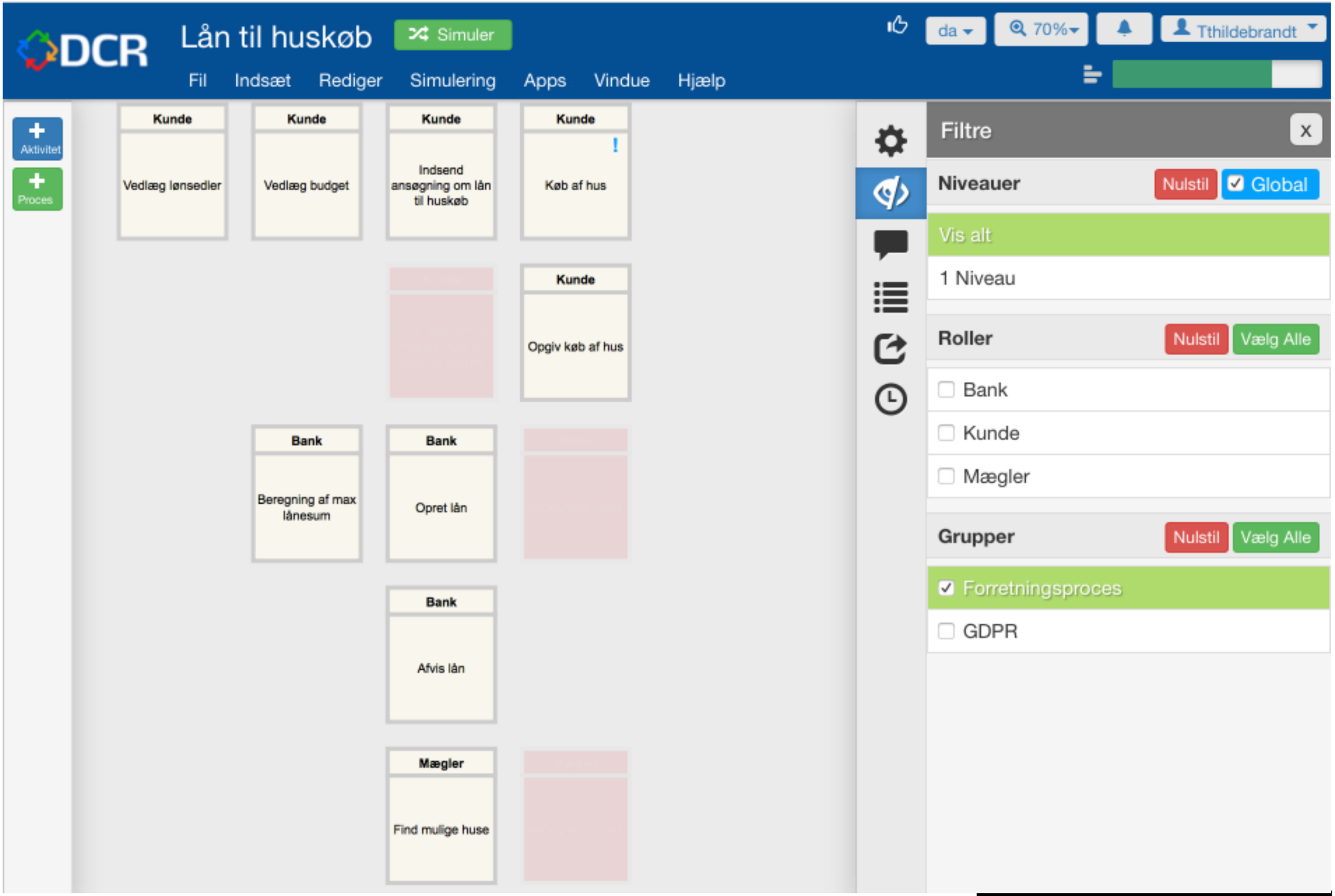
eXformatics

IT UNIVERSITY OF COPENHAGEN

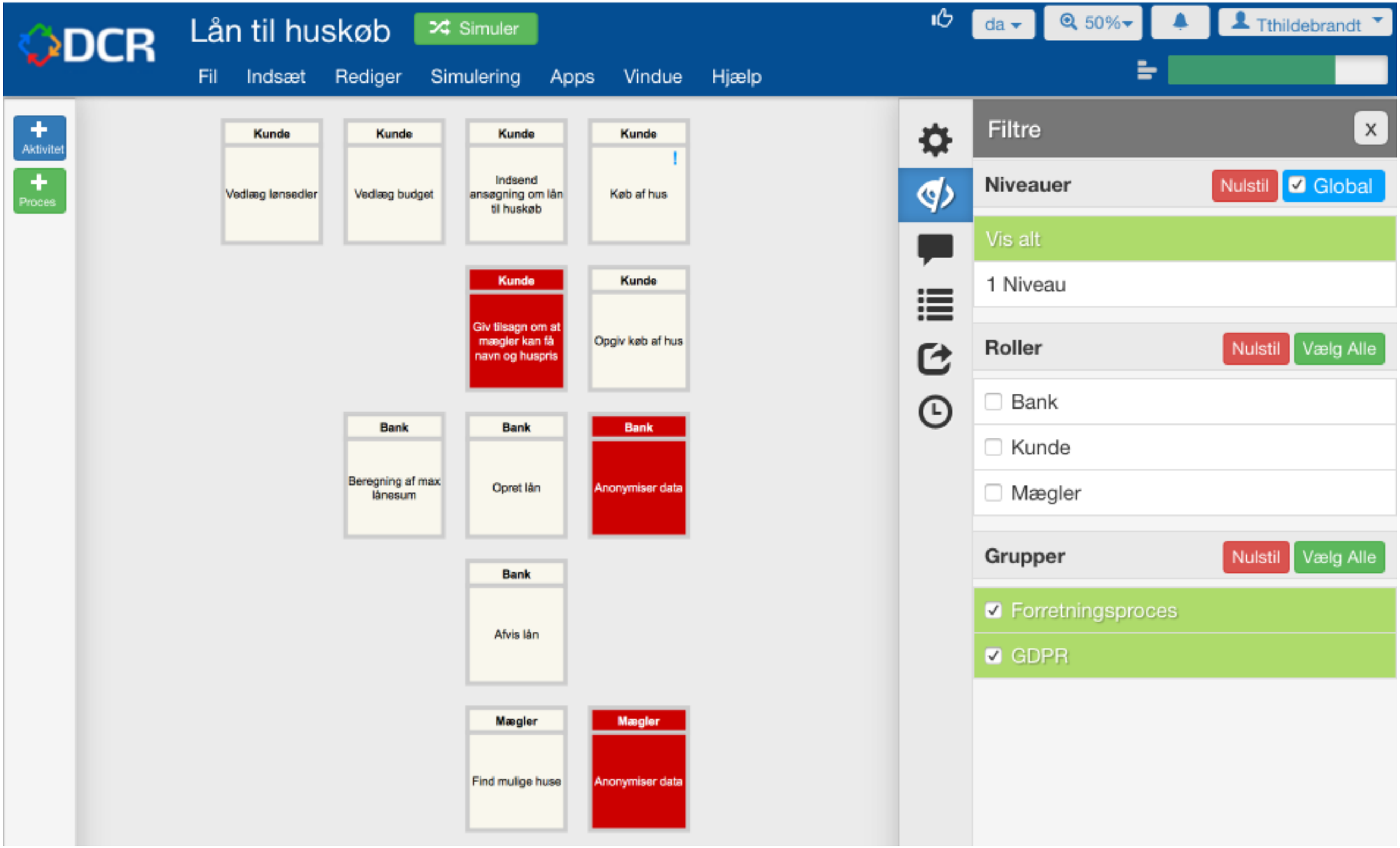
Eksempel: Lån til huskøb



Thomas T. Hildebrandt (hilde@itu.dk)

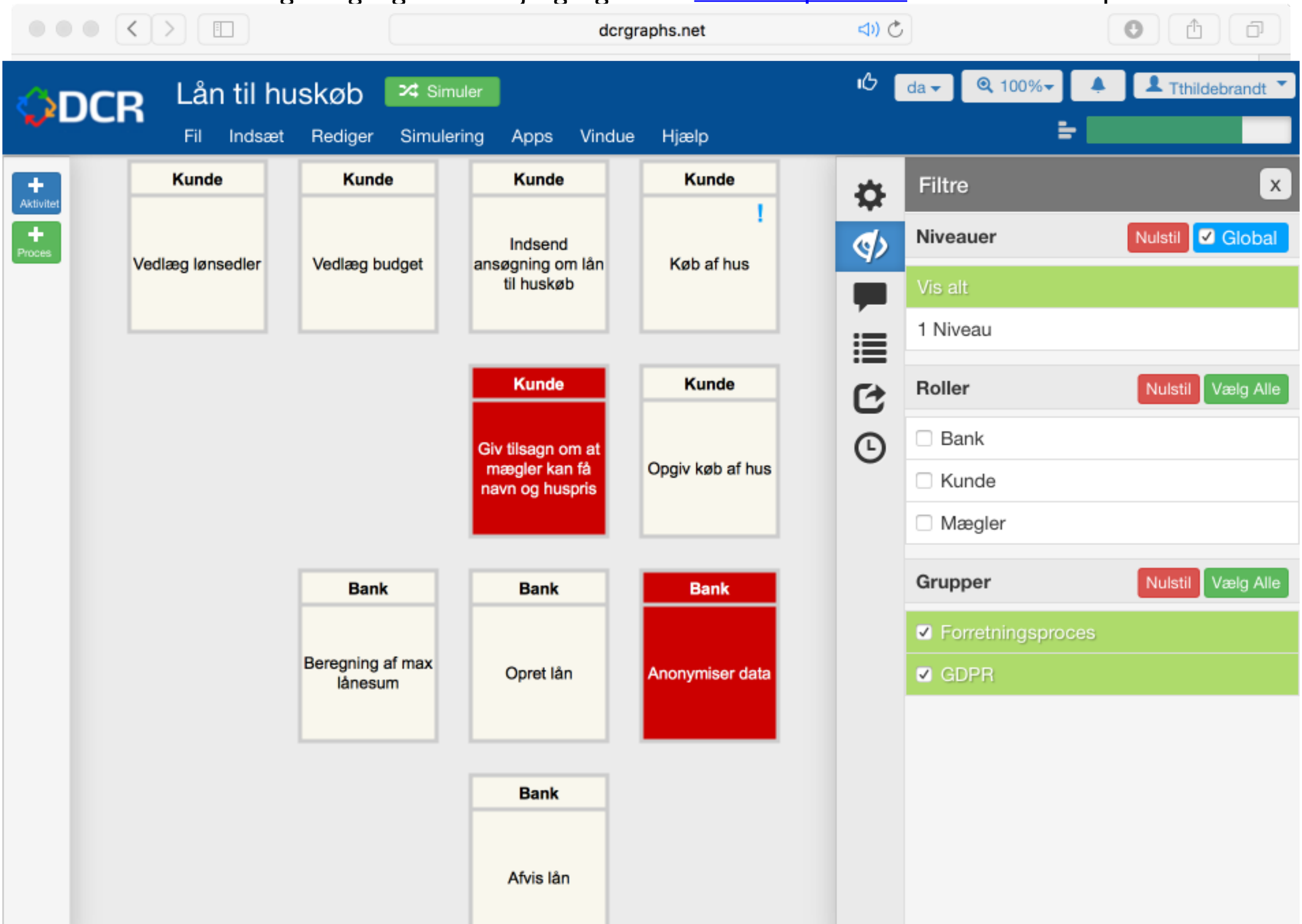


Thomas T. Hildebrandt (hilde@itu.dk)

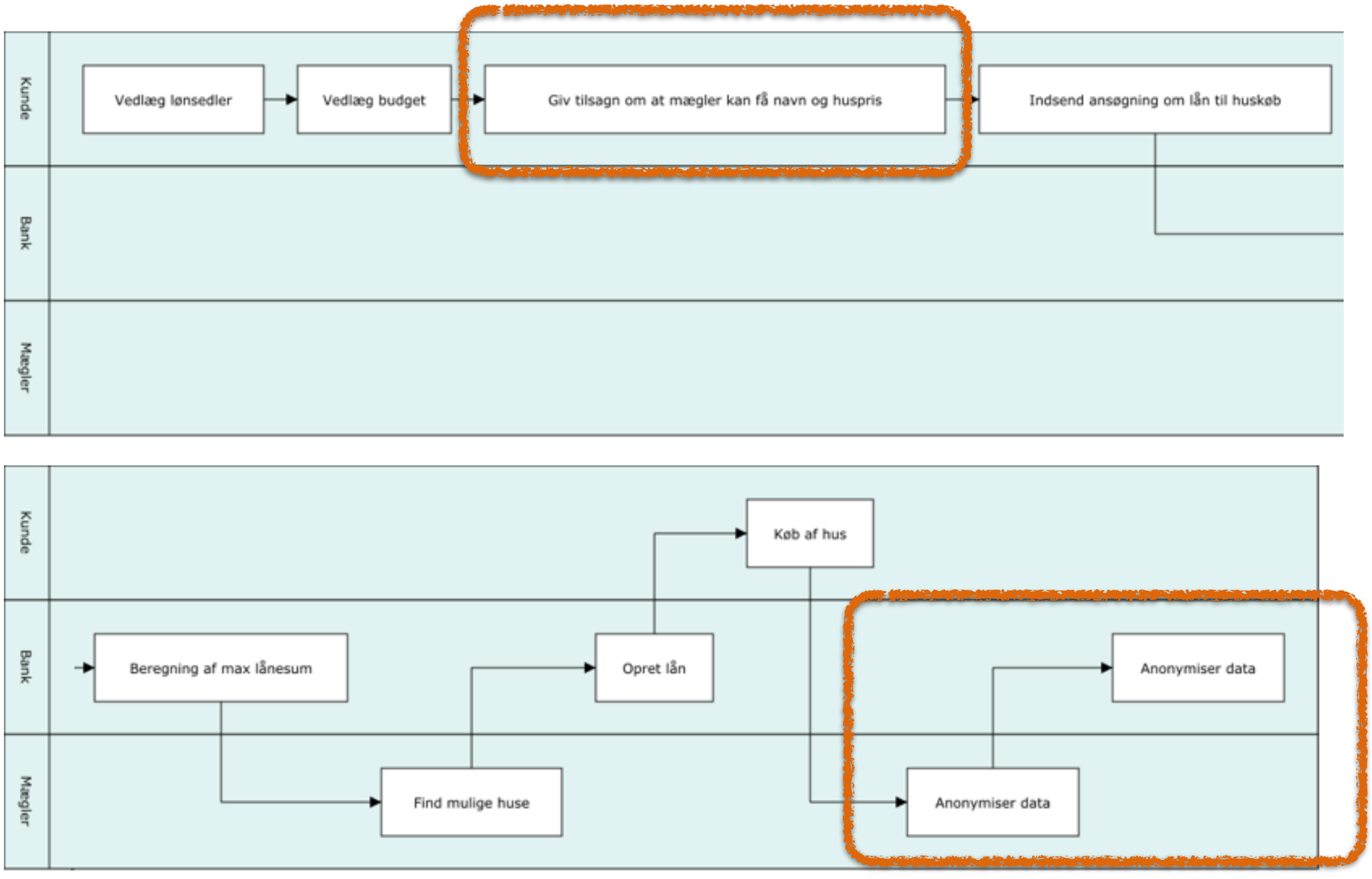


Thomas T. Hildebrandt (hilde@itu.dk)

IT UNIVERSITY OF COPENHAGEN

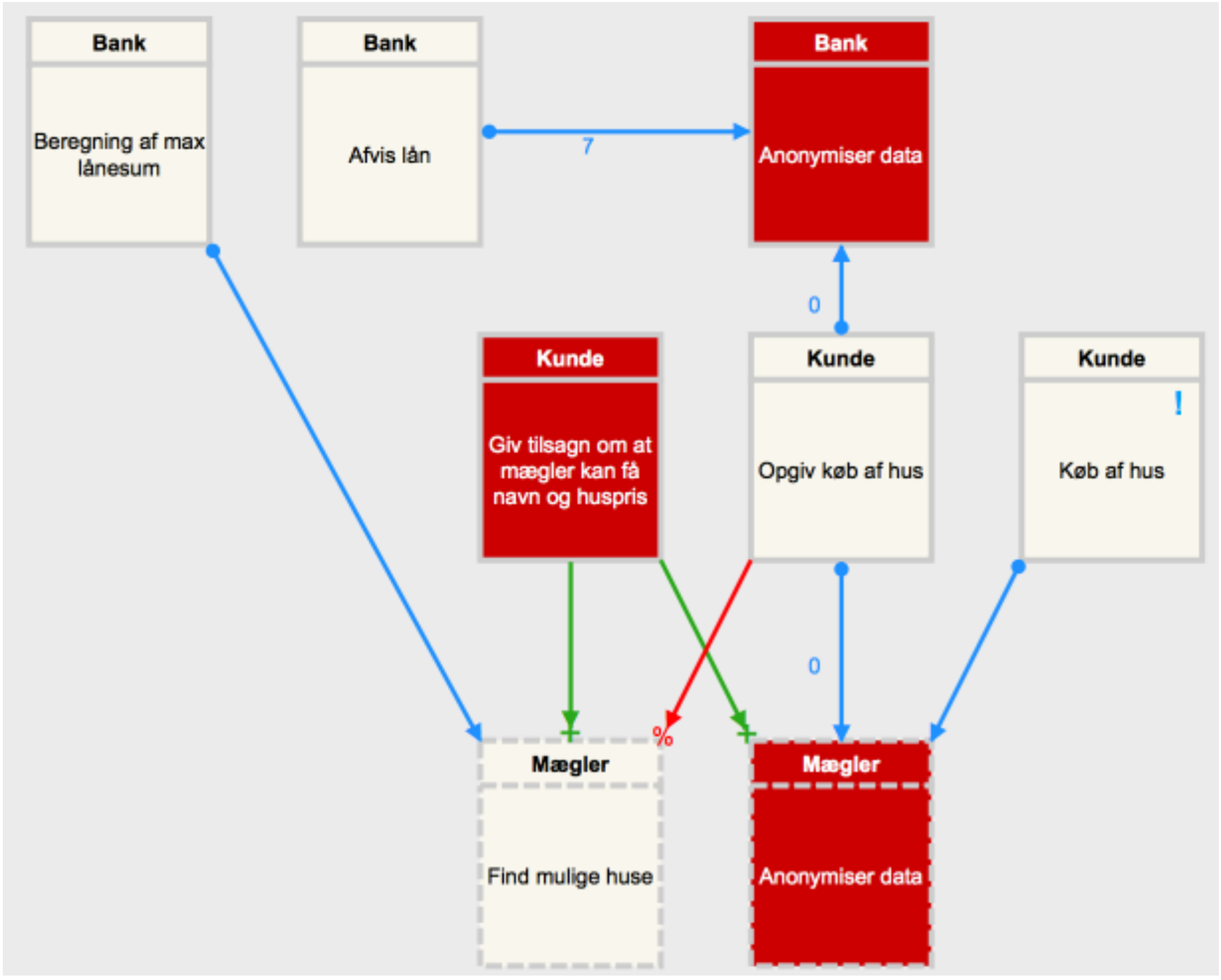

dcrgraphs.net
DCR
Lån til huskøb
Simuler
da
100%
Tthildebrandt
Fil
Indsæt
Rediger
Simulering
Apps
Vindue
Hjælp
Aktivitet
Proces
Kunde
Vedlæg lønsedler
Kunde
Vedlæg budget
Kunde
Indsend ansøgning om lån til huskøb
Kunde
Køb af hus
Kunde
Giv tilsagn om at mægler kan få navn og huspris
Kunde
Opgiv køb af 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



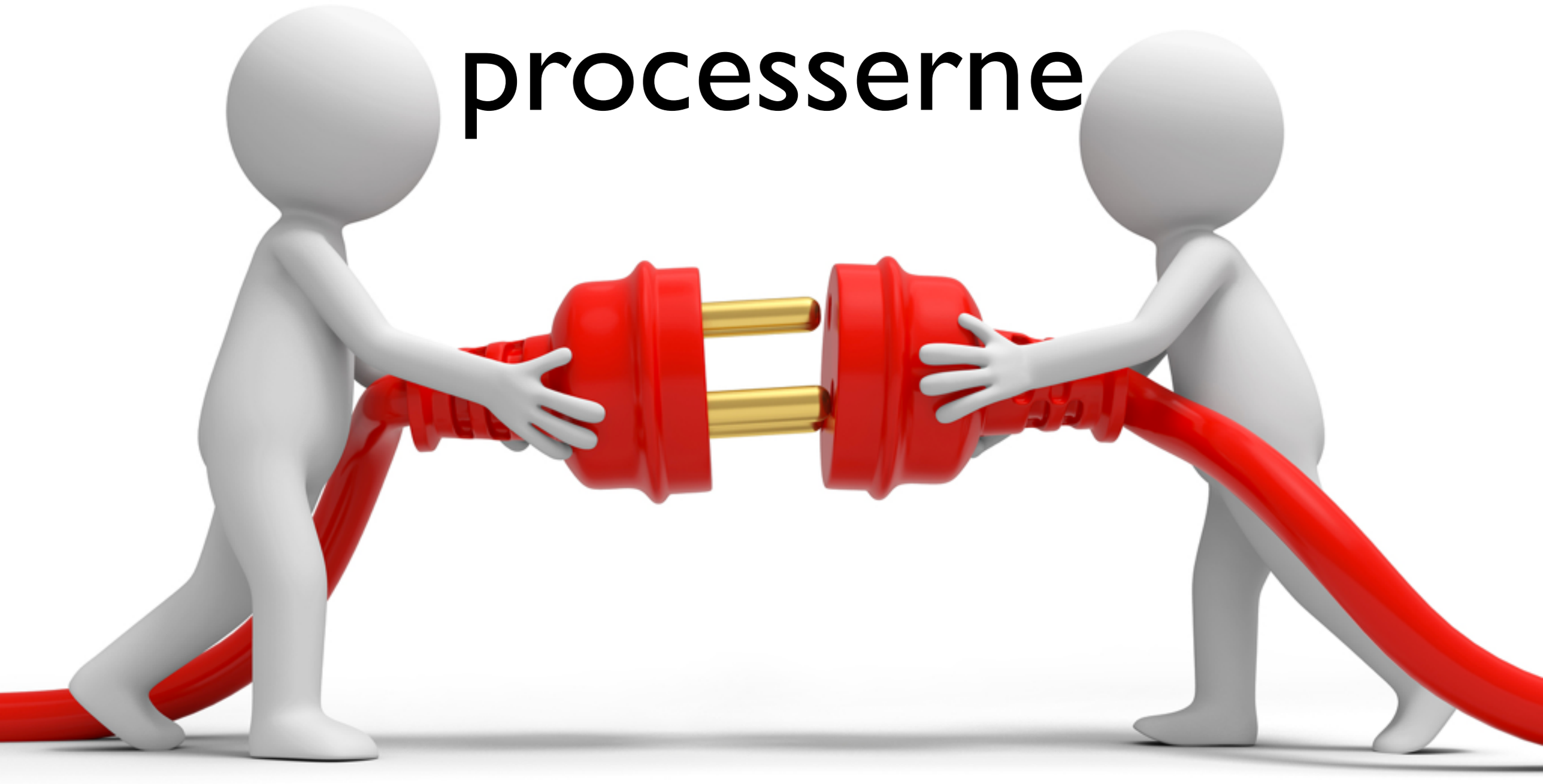
Thomas T. Hildebrandt (hilde@itu.dk)

GDPR regler

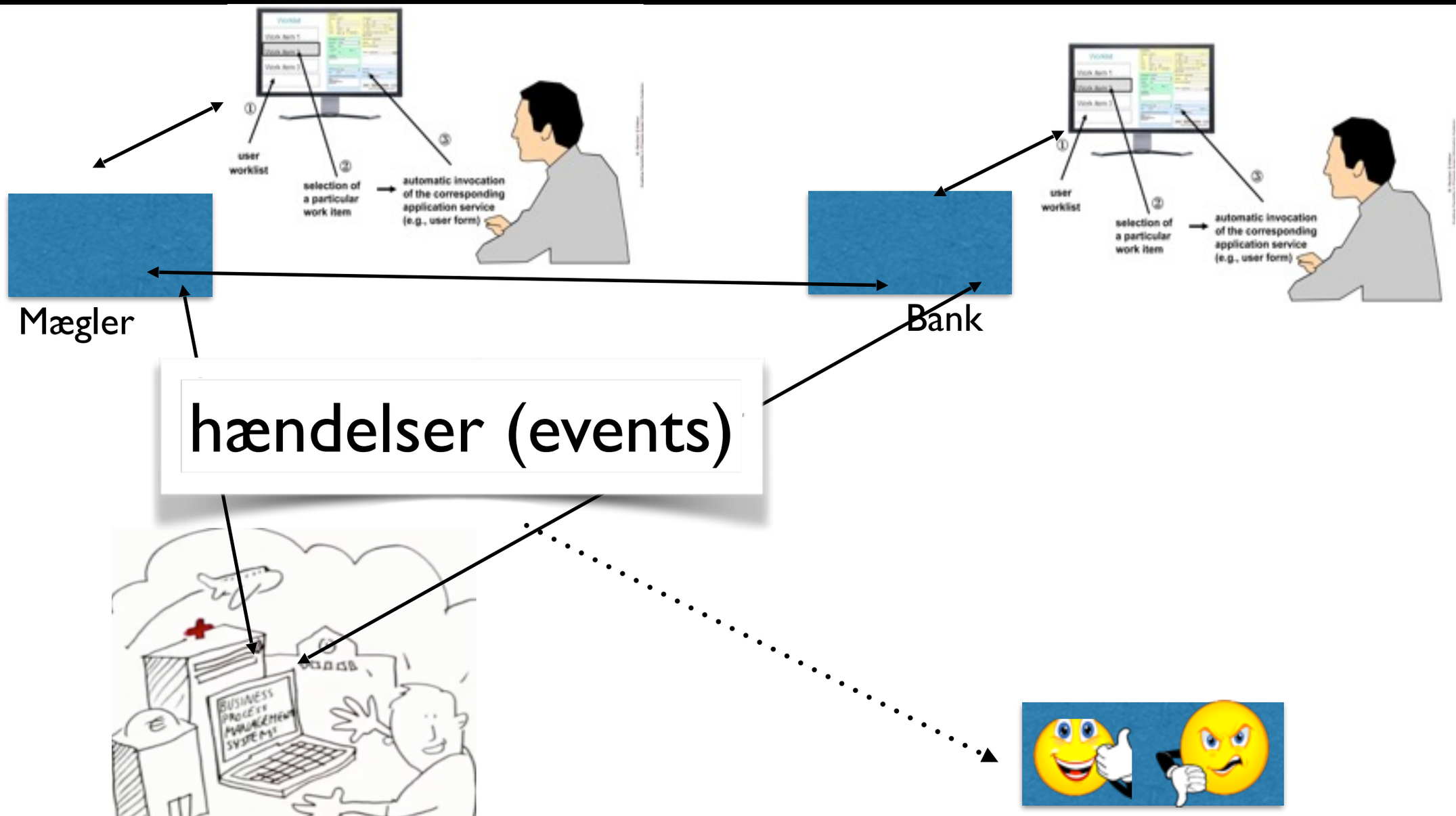


Thomas T. Hildebrandt (hilde@itu.dk)

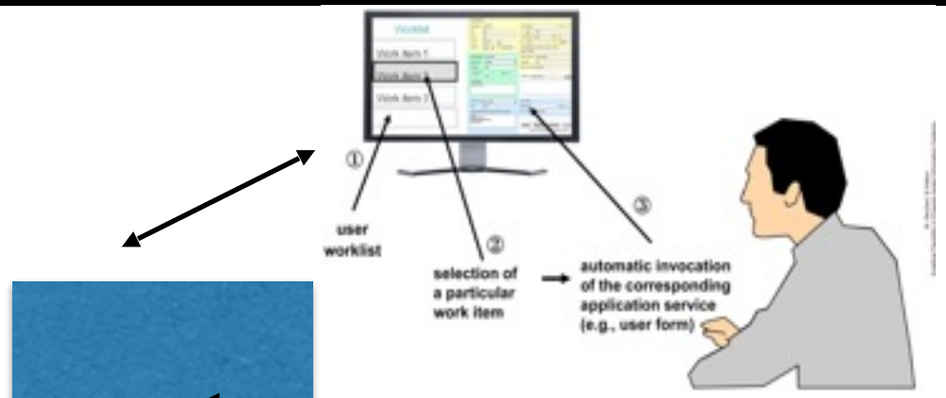
Sæt strøm til processerne



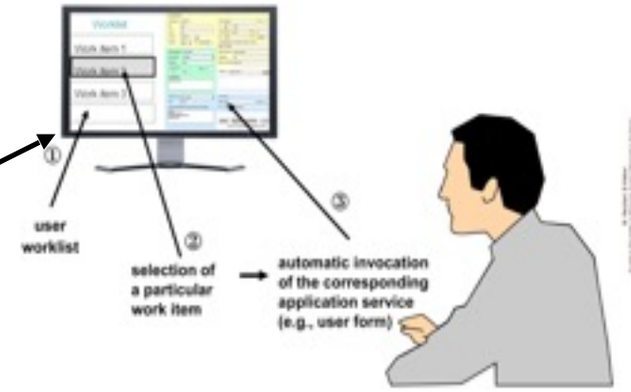
Overvågning



Proaktiv compliance



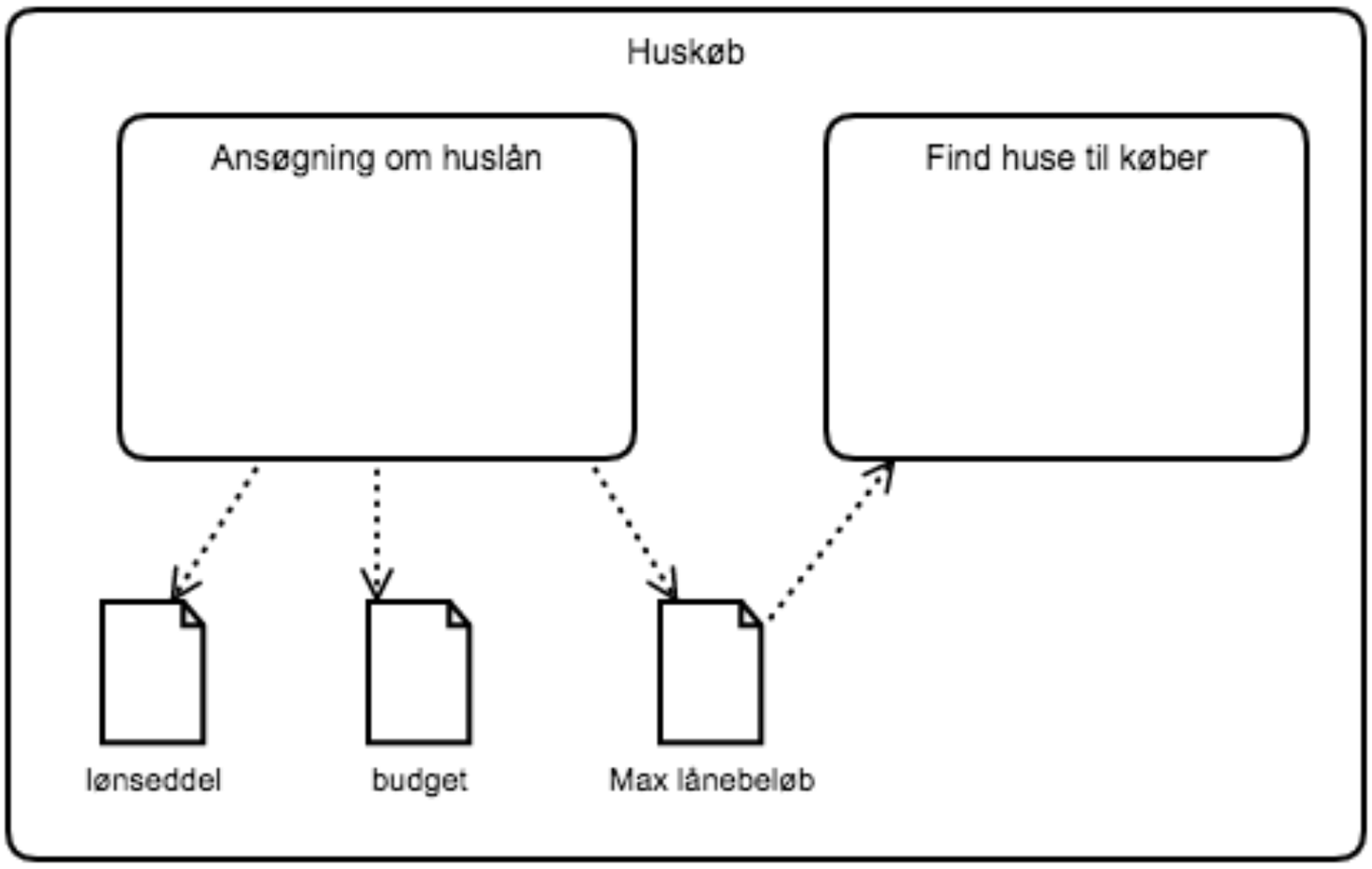
Mægler



Bank

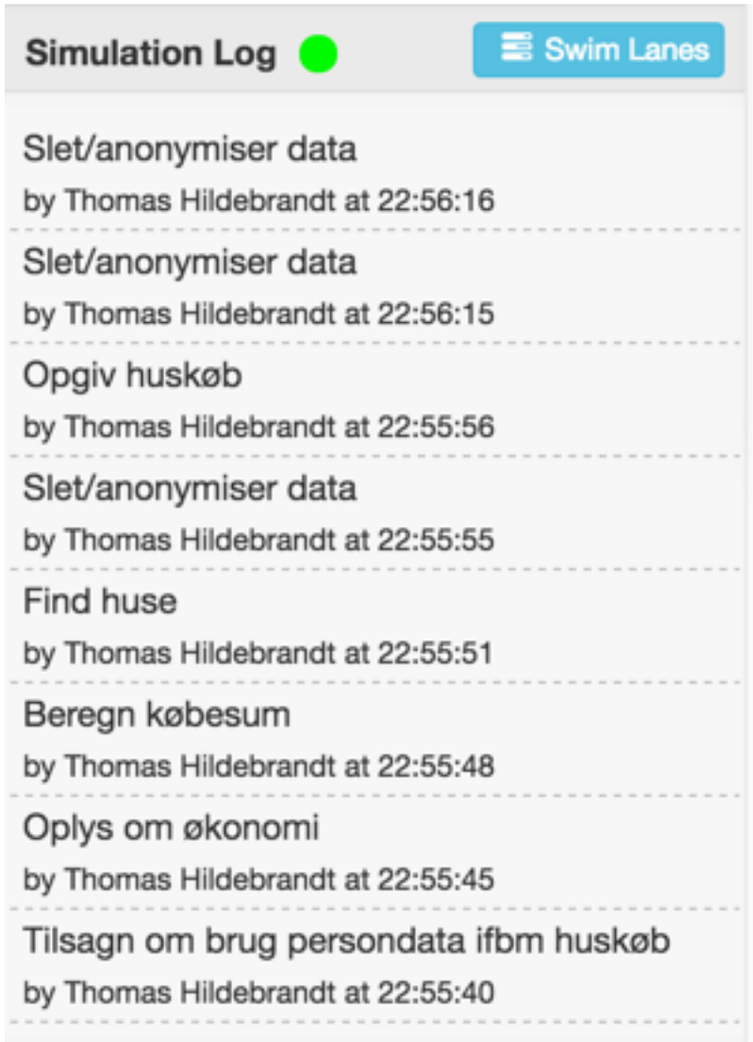
Proactive Policy Enforcement Point (kan bede om at få udført handlinger om nødvendigt, f.eks. tilsagn eller sletning af data)

Perspektiver: Håndtering af tilsagn

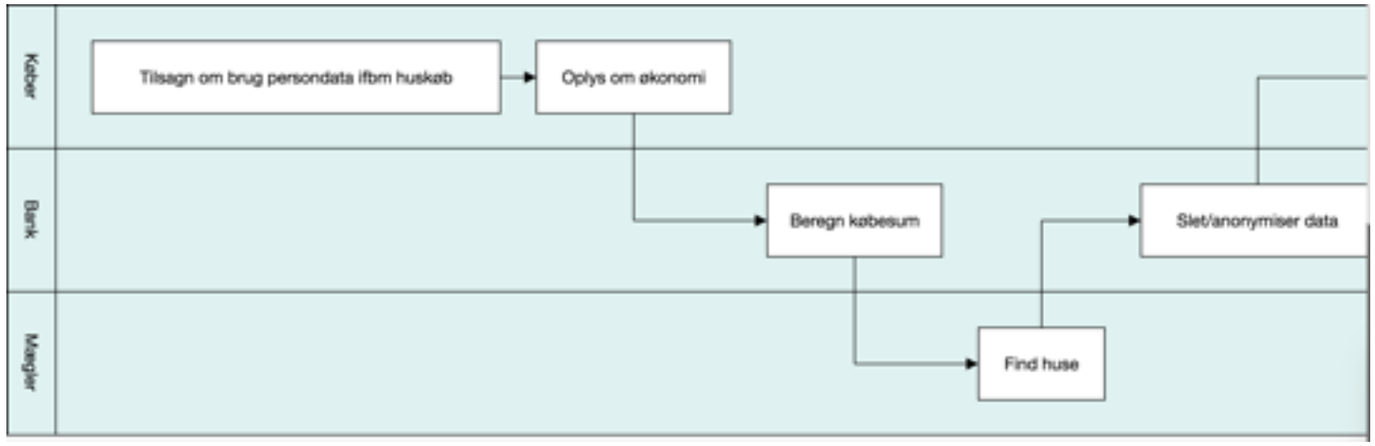


x Giv tilsagn til at Max. lånebeløb benyttes af mægler til at finde huse

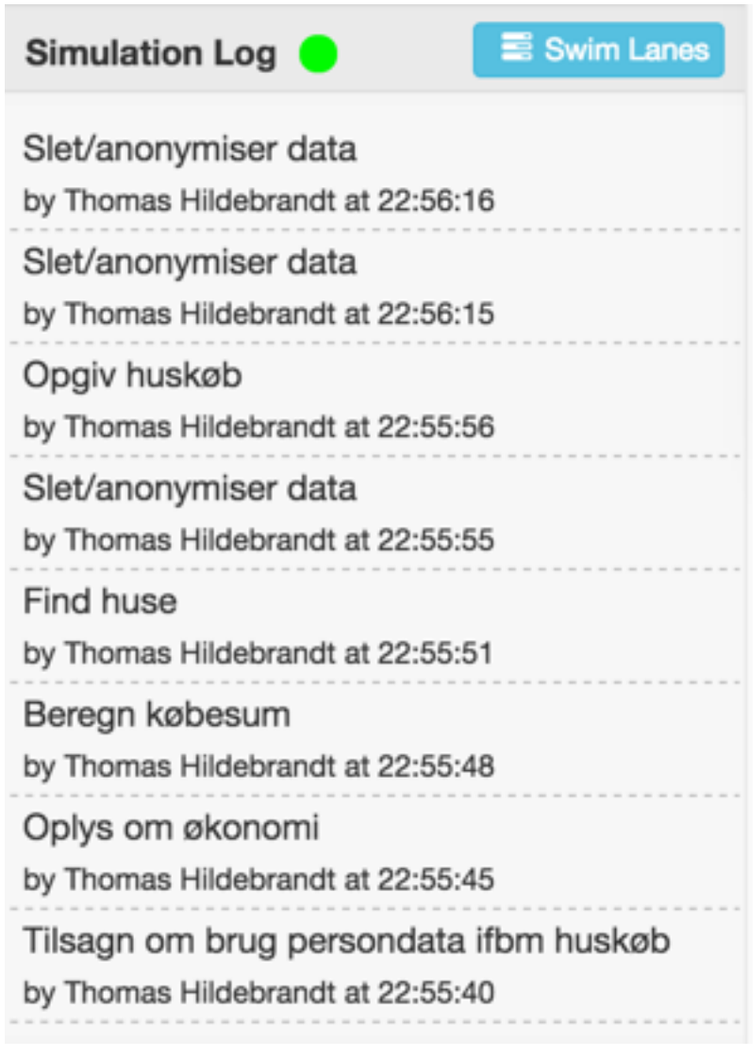
Perspektiver: Process Mining



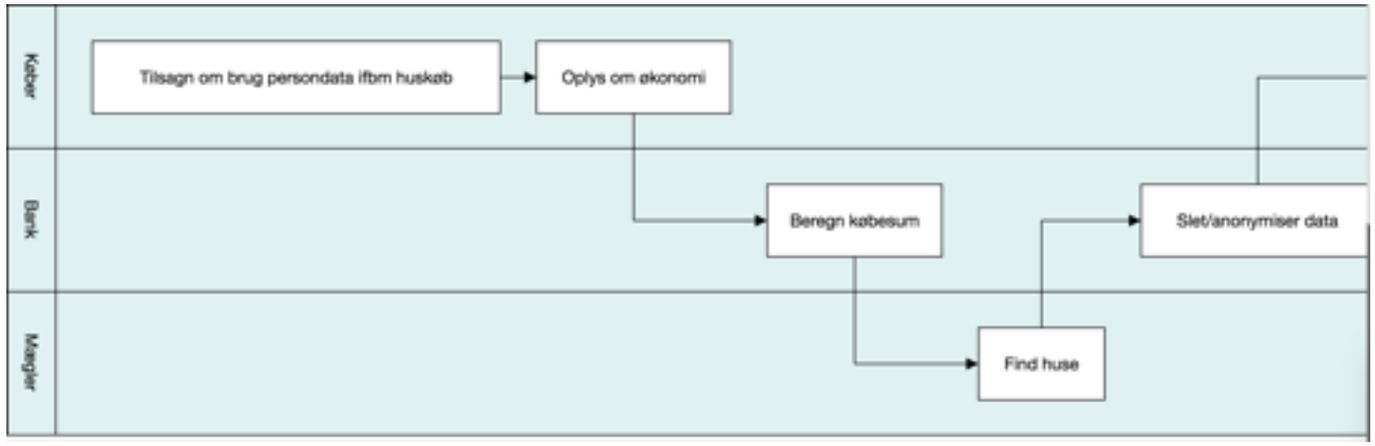
Analyser log-filer og udled ruter og dataflow



Perspektiver: Process Mining



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