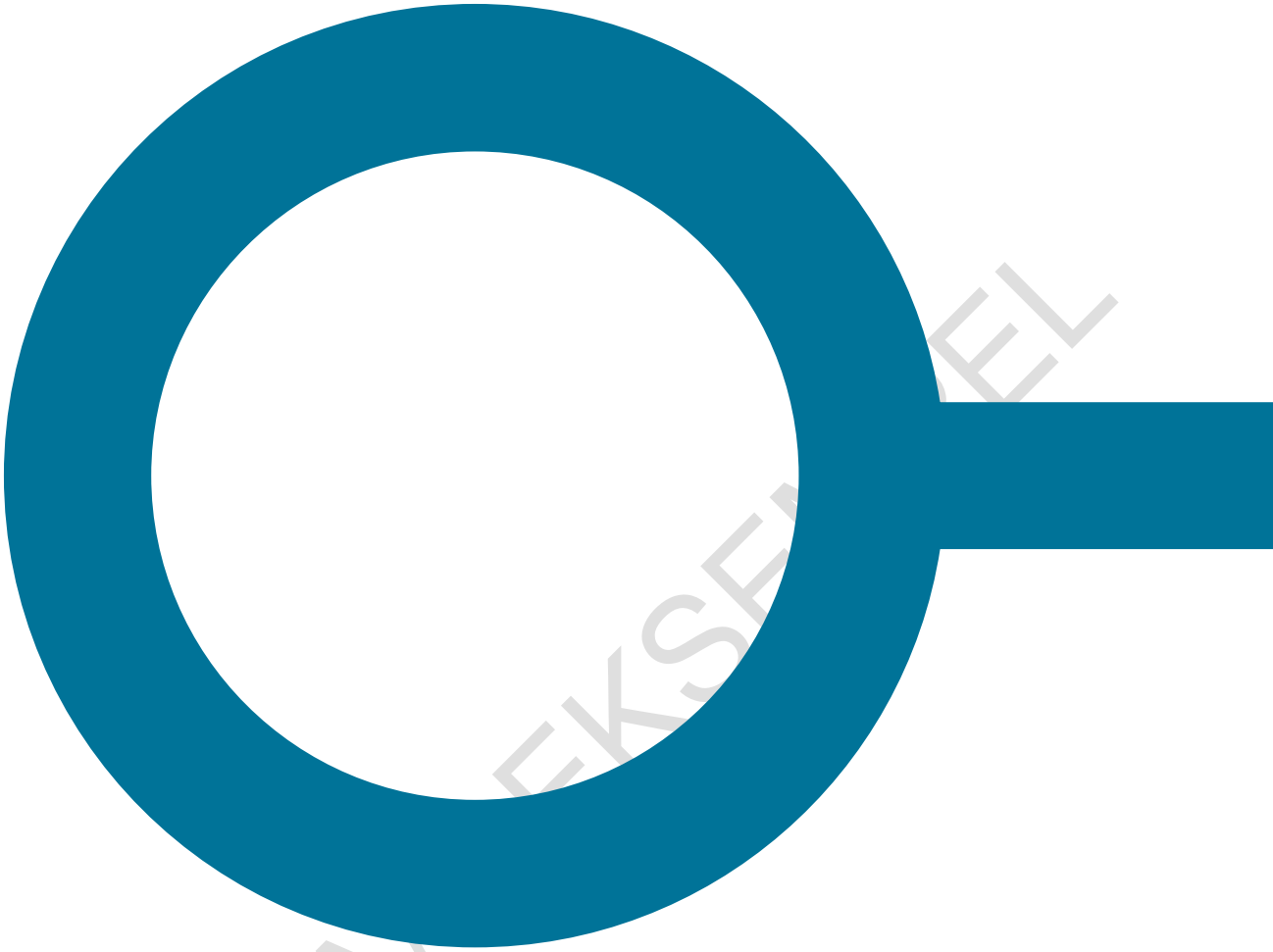


INFORMATIONSSIKKERHED – COMPLIANCE (GDPR & IT-SIKKERHED)

VEJLEDNING DATATYPER & DATASTRØMME

Version 3.0

1 marts 2019

KOMBIT

Kommunernes it-fællesskab

Versions historik

Versions-nummer	Dato	Afsnit der er ændret
1.0	4. august 2017	Gældende version
1.1	24. august 2017	Opdateret afsnit om datatyper jf. input om spørgsmål 12-16. Ikke publiceret på Yammer
2.0	14. september 2017	Tilføjet eksempel med serviceaftaler og Serviceplatformen
2.1	6. februar 2019	Sammenskrevet vejledning og supplerende vejledning. Ikke publiceret.
3.0	1. marts 2019	Gennemskrivning af vejledning. Gældende version.

Ansvarlig i KOMBIT

Indsatsområde	Indsatsansvarlig	Forretningsejer (FE)
Indsatsområde nr. 3		

BEMÆRK!

Denne vejledning er udarbejdet med KOMBIT A/S for øje. Den kan derfor IKKE adopteres i sin nuværende form. Vejledningen er derfor ALENE tænkt som en inspiration til, hvordan GDPR-arbejdet kan brydes ned i mindre og mere forretningsnære størrelser.

KOMBIT A/S fraskriver sig derfor også ethvert ansvar, såfremt andre aktører anvender KOMBITs vejledninger/værktøjer i sin helhed eller brudstykker heraf i deres arbejde med EU's databeskyttelsesforordning.

KOMBIT
Kommunernes it-fællesskab

Indholdsfortegnelse

1 INDLEDNING

Denne vejledning er én ud af en række vejledninger, som hører under indsatsområde 3 (Compliance, styring og kontrol) i KOMBITs informationssikkerhedsstrategi.

Vejledningen handler om den dokumentation, som skal udarbejdes for datatyper og datastrømme, når der er tale om behandling af *personoplysninger* (almindelige, følsomme & fortrolige).

Vejledningen handler også om fastlæggelse af behandlingsgrundlag og rollerne dataansvarlig, databehandler, underdatabehandler, under-underdatabehandler samt databehandleraftaler, hvor dokumentationen for og oversigter over datatyper og datastrømme vil skulle udgøre grundlaget for arbejdet hermed.

I tillæg til denne vejledning er der udarbejdet vejledninger om:

1. Dokumentation for registreredes rettigheder
2. Dokumentation for risikovurdering
3. Dokumentation for risikohåndtering

2 FORMÅL MED KORTLÆGNING

Dokumentationen for datatyper og datastrømme indgår som en ud af flere opgaver i det samlede GDPR compliance arbejde, som alle projekt, speciale eller supportfunktioner, der behandler personoplysninger, har ansvaret for at håndtere.

Oversigter og overblik over datatyper og datastrømme er det grundlag, som bruges i arbejdet med fx udarbejdelse/opdatering af databehandleraftaler, gennemførelse af løbende risikovurderinger samt risikohåndtering og eventuelle mitigerende handlinger til imødegåelse af de risici, der fremgår af risikovurderingen.

Dokumentationen tjener desuden det formål at opfylde dokumentationskravet i databeskyttelsesforordningens artikel 30 om fortegnelse over behandlingsaktiviteter.

Endelig skal dokumentationen udgøre grundlaget for den risikovurdering, som projekt, speciale eller supportfunktioner er forpligtet til at gennemføre og dokumentere for alle løsninger, hvor der behandles personoplysninger.

I arbejdet med at etablere dokumentation for datatyper og datastrømme kan det - alt afhængig af, hvilket projekt, speciale eller supportfunktion, der er tale om – være hensigtsmæssigt at opdele projekt, speciale eller supportfunktion i dataprocesser, som hver for sig indeholder oversigter over datatyper og datastrømme.

En dataproces er således i denne sammenhæng udtryk for en del af den samlede dokumentation af et projekt, speciale eller supportfunktion og en del af løsningen eller systemet, hvor der behandles personoplysninger.

Hvis der fx i en og samme løsning modtages data fra kommunerne, som KOMBIT får ansvaret for at stille til rådighed eller videresende til forskellige eksterne, så kan det være hensigtsmæssigt at udarbejde en oversigt over datatyper og datastrømme for hver af de processer, hvor kommunens data stilles til rådighed eller videresendes til eksterne.

Skemaet over datatyper og datastrømme skal således indeholde de nødvendige oplysninger på et vist overordnet niveau. Det er dermed ikke forventningen, at der skal udfærdiges store tekniske dataflowanalyser og niveauet er således ikke, at skemaet skal indeholde enhver detalje om hver enkelt datatype og dennes datastrømme, men omvendt må niveauet heller ikke være af så generel karakter, at det ikke er muligt at vurdere om den krævede og fornødne sikkerhed for den pågældende behandling af personoplysninger er tilstede. I dokumentationsskemaet vil der fremgå eksempel på niveauet af information.

Det vil i det konkrete projekt, speciale eller supportfunktion bero på en konkret vurdering i hvilket omfang og hvordan der mest hensigtsmæssigt skal ske en nedbrydning af projekt, speciale eller supportfunktionet/løsningen i dataprocesser, der tilgodeser formålet med etableringen af overblik og oversigt over datatyper og datastrømme.

I forhold til specialer og supportfunktioner vil der ligeledes skulle tages stilling til i hvilket omfang, det vil være hensigtsmæssigt at opdele områder i underliggende processer, hvis der skal etableres dokumentation for de datatyper og det datastrømme, der finder sted i forbindelse med behandlingen af personoplysninger i enheden.

A. PRAKTISK

Til brug for arbejdet med etableringen af dokumentation for datatyper og datastrømme er der udarbejdet et skema, som skal benyttes hertil. Skemaet SKAL navngives med unikke identer således, at der sikres den fornødne sammenhæng mellem skemaerne og det enkelte projekt, speciale eller supportfunktion. Den unikke ident, som SKAL fremgå, er projekt, speciale eller supportfunktions nummer i Project Online. I tillæg vil det være muligt at indsætte en ident fra henholdsvis Qualiware og Pactius såfremt projekt, speciale eller supportfunktionet har dette, men det er ikke obligatorisk.

For yderligere præcisering af navngiving af dokumenter henvises til dokumentet "Vejledning opdatering af compliance og udarbejdelse af årsplan": https://share-it.kombit.dk/i/standarderogskabeloner/MetodeMatrix/Vejledning - Opdatering af compliance og udarbejdelse af %C3%A5rsplan - Informationssikkerhed.docx

I skemaet er der en række spørgsmål, hvor der vil være mulighed for at krydse af eller svare ja/nej. Det er vigtigt at understrege, at det er obligatorisk, at alle felter besvares af hensyn til den efterfølgende dokumentation og proces. Det er således væsentligt, at man ved at kigge på besvarelserne kan se, at der er taget aktivt stilling til de fremsatte spørgsmål i projekt, speciale eller supportfunktionerne. Det er muligt at anføre bemærkninger til svar i skemaet såfremt der er usikkerhed omkring svar, eller der efterfølgende kan være behov for dialog, fx med projekt, speciale eller supportfunktionjuristen eller KOMBITs DPO, eller hvor kan konstateres, at der er forhold, som skal håndteres eventuelt indarbejdes i årsplanen og efterfølgende, fx i risikovurderingen eller de sikkerhedstiltag, der skal iværksættes i løsningen.

Det er et vigtigt hensyn, at dokumentationen foreligger i en form, som nemt kan tilgås i forbindelse med henvendelser fra dataansvarlige eller tilsynsmyndigheder, som har ret til at kontrollere KOMBIT's overholdelse af GDPR på og tilhørende persondataretlig og sikkerhedsmæssig lovgivning herom.

B. BEGREBER

I KOMBIT arbejder vi med begreberne datatyper, dataprocesser og datastrømme, som andre steder går under betegnelserne dataflowsanalyser og dataflowsdiagrammer.

Når det er valgt at bruge begreberne "datatyper", "dataprocesser" og "datastrømme" i stedet for begrebet "dataflowsanalyser", sker det ud fra et ønske om at arbejde med begreber, som også anvendes i ISO-27000. Nedenfor gives en uddybende vejledning om begreberne "dataproces" og "datastrøm".

Dataproces

En dataproces (proces) er en velafgrænset forretningsproces, hvori der foregår behandling af personoplysninger med et bestemt forretningsmæssigt formål, som fx i den kommunale verden ofte er lovbundet.

Det enkelte projekt, speciale eller supportfunktion bør starte med at kortlægge dataprocesser ud fra viden om systemet, formålene og de behandlingsaktiviteter, der skal foregå, således at processerne er veldefinerede og afgrænsede, og så behandlingsaktiviteterne vedrører det samme formål / lovgrundlag. For hver dataproces vil der typisk være en eller flere tilhørende datastrømme, som skal kortlægges – se nedenfor.

Ved identifikation af dataprocesser kan man tage udgangspunkt i de hovedformål, hvormed systemet er bygget, de naturlige moduler/delkomponenter i løsningen/systemet eller BPMN-diagrammer.

Når man kortlægger dataprocesser, vil man typisk undlade at fokusere på infrastrukturkomponenter, som ikke har et selvstændigt formål med behandling af personoplysninger, men alene agerer som 'hjælpesystemer' for de mere 'forretningsorienterede' systemer, der driver de egentlige forretningsprocesser. Dette gælder både interne komponenter (fx servicebus, database eller anden middleware) samt eksterne systemer som fx serviceplatformen og støttesystemer. Dette skal dog betragtes som en generel tommelfingerregel, og der kan være undtagelser, hvor støttesystemer behandler data med et selvstændigt formål. Hvis en infrastrukturkomponent er placeret hos en ekstern part (leverandør), er det vigtigt at identificere den tilhørende datastrøm (se nedenfor), idet data så skal være underlagt en databehandleraftale - det vil sige hjælpekomponenten er inden for samme dataproces, men giver anledning til sin egen datastrøm under denne.

Bemærk endvidere, at dataprocesser både kan være manuelle og automatiske, og at alle typer er relevante for kortlægningen. En manuel dataproces kan således finde sted uden for systemer/løsninger.

Datastrøm

En dataproces kan omfatte en eller flere datastrømme, som skal kortlægges. En datastrøm er en logisk strøm af (person)data mellem to juridiske enheder (altså tværorganisatorisk). Når man kigger på datastrømme anlægges et overordnet perspektiv, hvor man hæver sig over de konkrete, tekniske integrationsmekanismer og mere ser på, hvilke data der flyder på tværs af organisationer med henblik på at vurdere, om databehandleraftaler er på plads samt om regler for oplysningspligt (del af registreredes rettigheder), videregivelse mv. er overholdt.

Datastrømmene modelleres efter, hvordan lovgivningen ser på videregivelser og databehandling af personoplysninger og ikke på, hvordan de fysiske overførsler finder sted mellem systemer. Der er altså fundamental forskel på det fysiske og logiske niveau. Man ser endvidere ikke på konkrete dataudvekslinger i en given situation, men mere på hvilke typer af data, der er mulighed for kan blive udvekslet.

Typisk kan der findes inspiration til at afdække datastrømme ved at se på SystemContext diagrammer, i oversigter over integrationer med eksterne parter og via Systemets brugerflader, hvor der også kan ske en logisk strøm af data mellem eksterne brugere (ofte registrerede) og systemet.

Når en løsning har snitflader til en anden løsning, hvor der udveksles personoplysninger (data-ud og data-ind), er der tale om en datastrøm.

Når projekt, speciale eller supportfunktionet skal kortlægge datastrømme er det derfor vigtigt, at projekt, speciale eller supportfunktion får beskrevet alle de snitflader, hvor løsningen udveksler personoplysninger med andre løsninger. Snitfladerne beskrives som enten logiske eller fysiske datastrømme. Som hovedregel er det kun de logiske datastrømme, som skal beskrives, jf. nærmere nedenfor.

For hver strøm skal der blandt andet tages stilling til, hvem der er dataansvarlig og hvem der er databehandler henholdsvis underdatabehandler på den pågældende strøm. I de løsninger som KOMBIT udvikler og forvalter, vil det som hovedregel være kommunerne, der er dataansvarlige og KOMBIT, der er databehandler, mens KOMBITs leverandører vil være underdatabehandlere, og endelig vil leverandørens underleverandør være under-underdatabehandler.

Ved dokumentation af datastrømme er det ikke nødvendigt at se på de enkelte felter eller attributter i informationsmodellen – abstraktionsniveau'et er her mere overordnet og med fokus på naturen og kategoriseringen af data (almindelige personoplysninger, følsomme og fortrolige personlysninger).

Logiske og fysiske datastrømme

Projekt, speciale eller supportfunktioner skal som alt overvejende hovedregel kun dokumentere de logiske datastrømme – altså datastrømme, hvor der udveksles personoplysninger mellem to forskellige juridiske enheder.

Der er ikke tale om en logisk datastrøm, hvis udvekslingen sker mellem kommunens egne løsninger, fx mellem DUBU og kommunens eget ESDH-system. Det skyldes, at personoplysninger i denne situation holdes inden for samme kommune, og der er derfor ikke tale om udveksling mellem to forskellige juridiske enheder. Disse snitflader skal i stedet beskrives som fysiske datastrømme, men kun hvis udvekslingen sker uden for Administrationsmodulet, jf. nærmere nedenfor.

Fysiske datastrømme (løsning til løsning), som finder sted mellem to underdatabehandlere via Administrationsmodulet (fx Serviceplatformen) bliver dokumenteret i regi af GDPR-compliancearbejdet i Adminstrationsmodulet, og projekt, speciale eller supportfunktionerne skal således ikke medtage disse datastrømme i arbejdet med GDPR-compliance.

Projekt, speciale eller supportfunktionerne skal derimod beskrive de fysiske datastrømme, som finder sted mellem to systemer uden for Administrationsmodulet (fx Serviceplatformen). Disse fysiske datastrømme skal dokumenteres i Excel-arket på samme måde, som de logiske datastrømme beskrives.I skemaet i Excel-arket under datastrømme bliver projekt, speciale eller supportfunktionerne bedt om at angive, hvilken organisation/enhed der overføres fra/til. Hvis der overføres personoplysninger fra projekt, speciale eller supportfunktionets løsning til en anden løsning uden for Administrationsmodulet, vil "organisation/enhed der overføres fra" typisk være leverandøren som underdatabehandler, og "organisation/enhed der overføres til" vil typisk være den dataansvarlige, eksempelvis kommunen eller SKAT.

Det vurderes, at det vil være ganske få fysiske datastrømme, som ikke finder sted via Administrationsmodulet. Det vil derfor være ganske få (hvis nogen) fysiske datastrømme, som projekt, speciale eller supportfunktionerne skal beskrive i Excel-arket.

Hvad skal datastrømme bruges til?

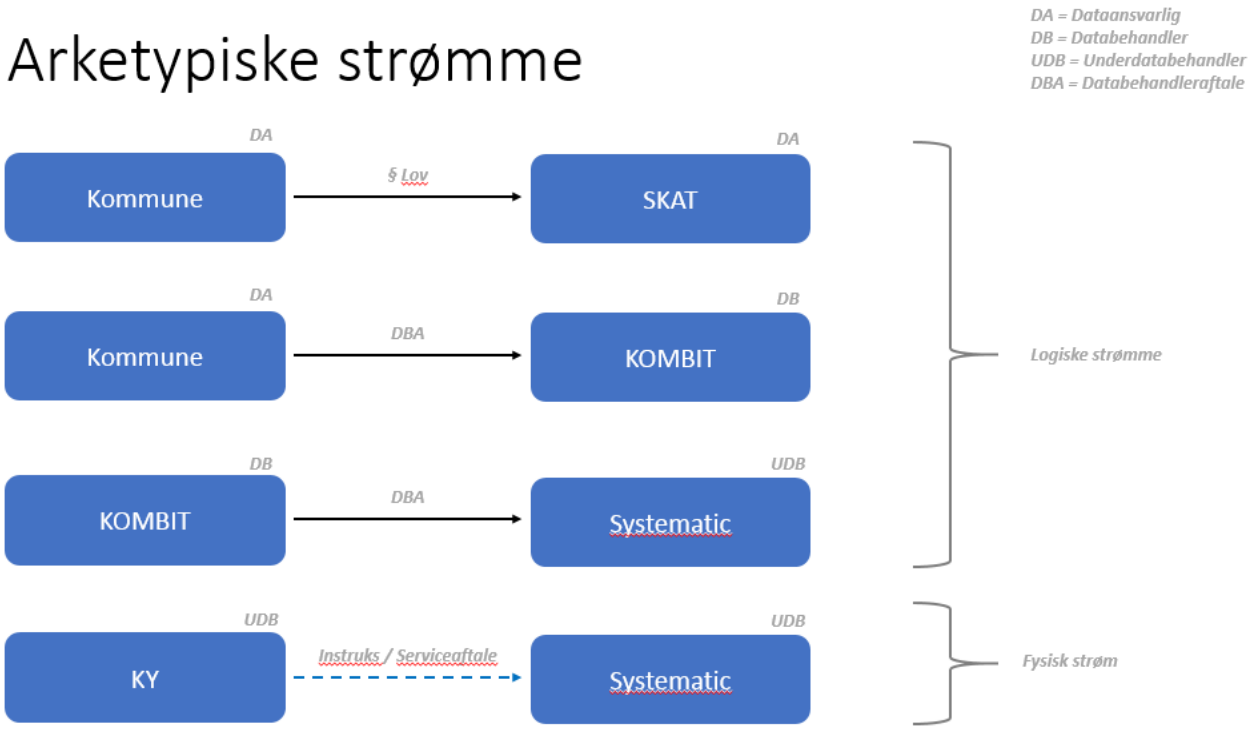
For hver dataproces er det vigtigt at beskrive alle datastrømme, hvor der udveksles personoplysninger i løsningerne, da beskrivelserne af datastrømme skal bruges som grundlag for udarbejdelsen af instrukserne i databehandleraftalerne. Alle datastrømme skal altså være tilknyttet en dataproces. Databehandleraftalen mellem kommunerne og KOMBIT skal således indeholde kommunens instrukser til KOMBIT om at udveksle personoplysninger med andre løsninger.

Når projekt, speciale eller supportfunktionerne har kortlagt alle datastrømme under alle dataprocesser, som er defineret for løsningen, skal de kontrollere, at alle datastrømme indgår som instrukser i databehandleraftalerne, og at de samme instrukser indgår i underdatabehandleraftalen mellem KOMBIT og leverandøren og eventuelle underleverandører.

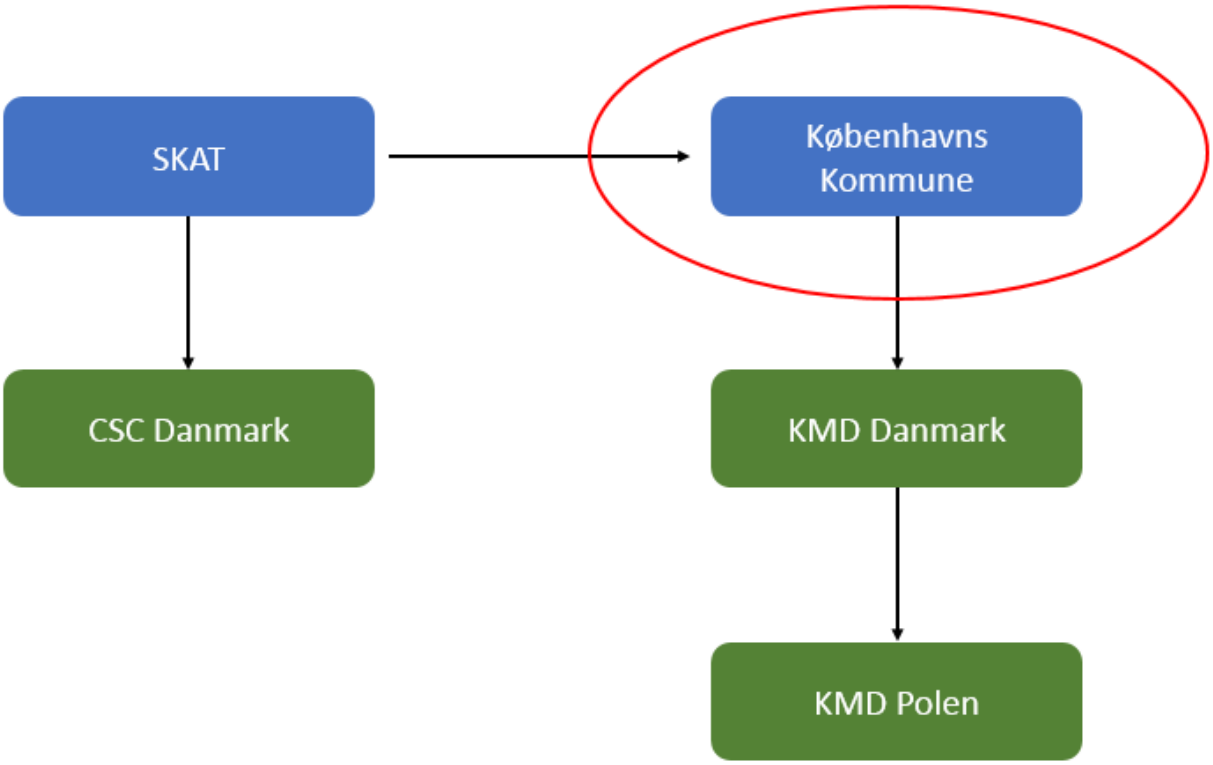
Dokumentationen af datastrømme skal herudover bruges som den fortegnelse, som Databeskyttelsesforordningen stiller krav om, at både dataansvarlig og databehandler udarbejder, når der behandles personoplysninger i løsningen.

Endelig skal dokumentaionen udgøre grundlaget for den risikovurdering, som projekt, speciale eller supportfunktioner er forpligtet til at gennemføre og dokumentere for alle løsninger, hvor der behandles personoplysninger.

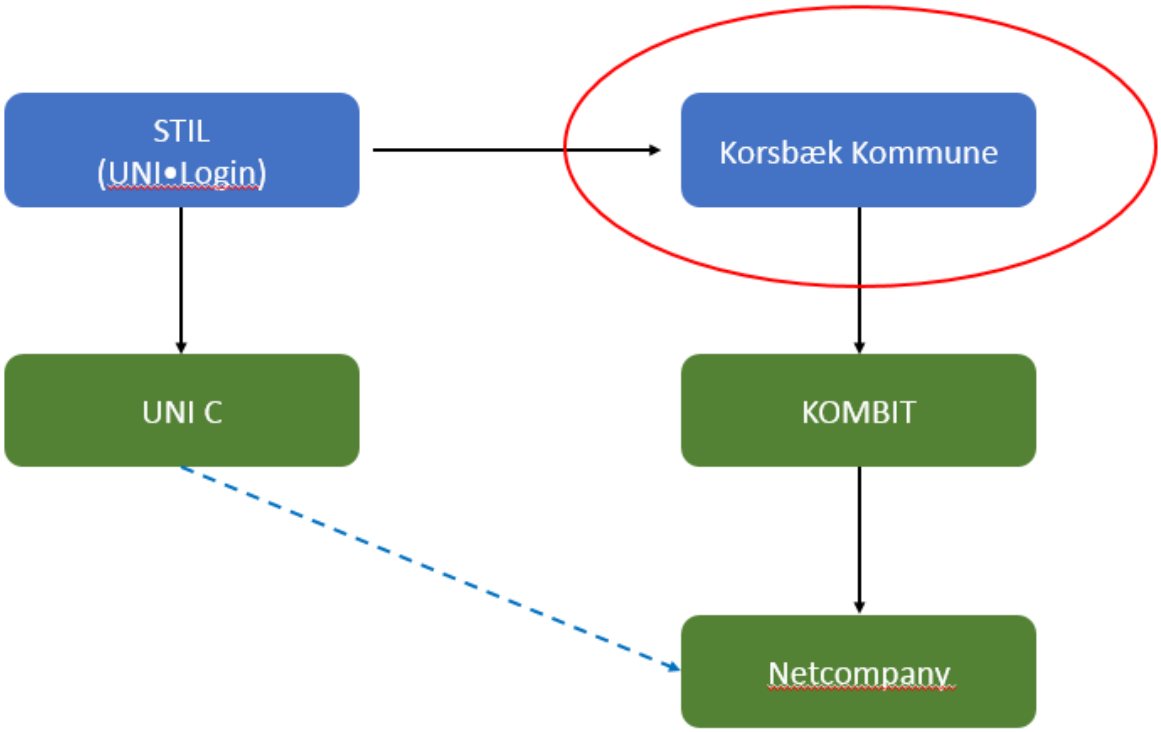
Eksempler på logiske datastrømme (L) og fysiske datastrømme (F)



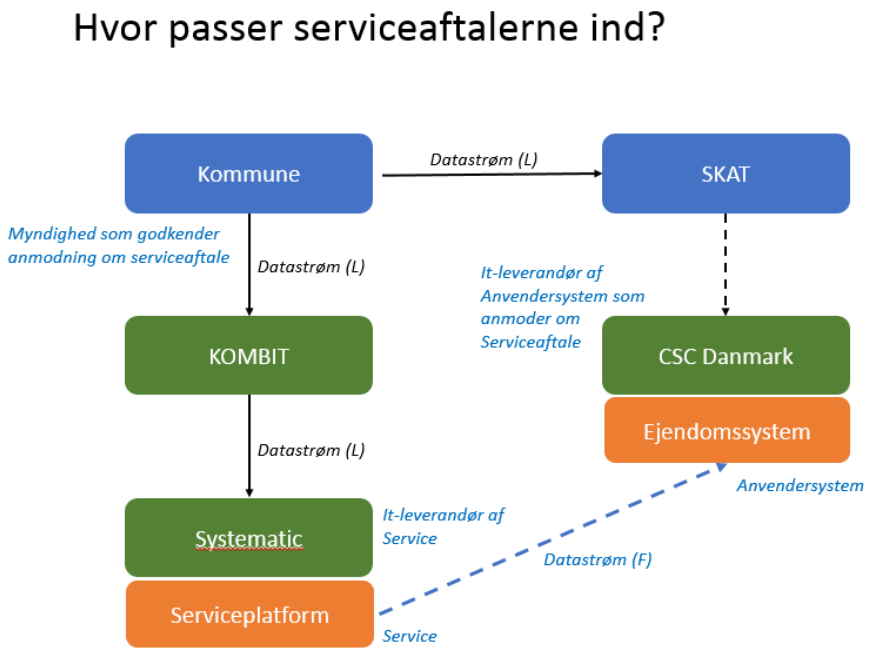
Datastrøm mellem statslig myndighed og kommune



Datastrøm mellem stat, kommune og KOMBIT



Datastrømme via Serviceplatformen



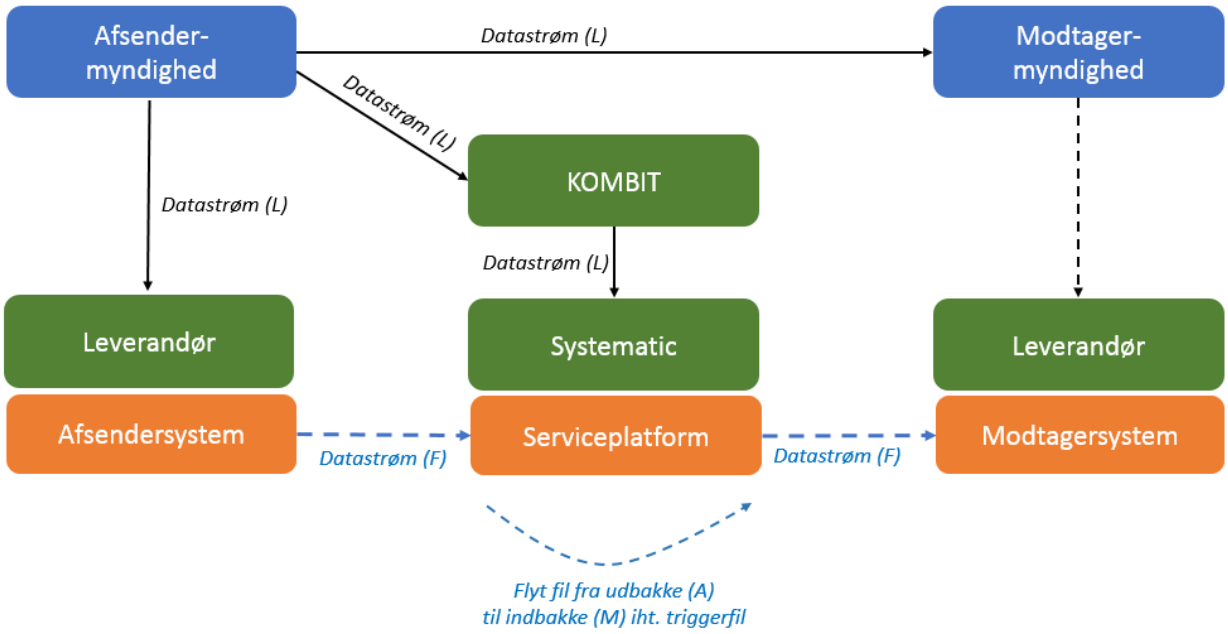
Scenarie:
E&E sender ejendomsoplysninger til SKAT på vegne af en kommune. Sker via Serviceplatformen.

Serviceaftalen åbner for det fysiske flow af data, som ikke er en logisk datastrøm.

I Administrationsmodulet anmoder CSC i rollen som It-leverandør for SKAT's Anvendersystem om en serviceaftale med en E&E service udstillet på Serviceplatformen (Serviceudbyder), som Kommunen herefter godkender som Myndighed. Herefter kan Anvendersystemet hente data via servicen.

Kommunen skal selv have styr på sit grundlag for at videregive data til SKAT, og dette grundlag dokumenteres uden for KOMBIT's systemer!

Datastrømme med SFTP filudveksling via Serviceplatformen

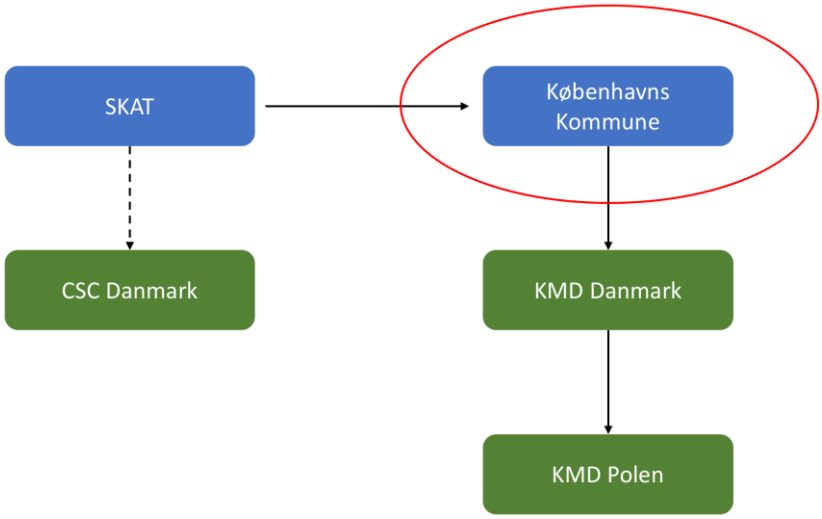


Eksempler:

Nedenfor gives eksempler på, hvordan datastrømme kan beskrives. Fokus er lagt på strukturen og ikke at beskrive alle forhold på de enkelte strømme.

'Klassisk' dataoverførsel mellem myndigheder

Som et første eksempel betragtes en klassisk dataoverførsel mellem to myndigheder. I eksemplet henter Københavns Kommune nogle indkomstoplysninger om sine borgere hos SKAT.



I eksemplet har begge myndigheder en databehandler, som fysisk håndterer data i deres driftcenter (SKAT har CSC Danmark og Københavns Kommune har KMD Danmark). Endelig antager vi for eksemplets skyld, at KMD Danmark benytter en underdatabehandler hos KMD Polen, da polske teknikere via fjerneadgang yder service på driftssystemerne, som er placeret i Ballerup, og at de herigennem kan opnå adgang til data.

Hvis man betragter de relevante datastrømme ud fra Københavns Kommunes synspunkt, kan man identificere følgende datastrømme:

Strøm	Startenhed og rolle	Slutenhed og rolle	Data og kategori
S1	SKAT (dataansvarlig)	Københavns Kommune (dataansvarlig)	Indkomstdata (Alm. personoplysninger)
S2	Københavns Kommune (dataansvarlig)	KMD Danmark (databehandler)	Indkomstdata (Alm. personoplysninger)
S3	KMD Danmark (databehandler)	KMD Polen (underdataansvarlig)	Indkomstoplysninger (Alm. personoplysninger)

Pointer og observationer:

Datastrømme modelleres ud fra en given myndigheds synspunkt – der er forskelle på de relevante strømme afhængigt af, om man tager udgangspunkt i SKAT eller Københavns Kommune. På figuren er det valgte perspektiv angivet med en rød cirkel.

Selvom den fysiske strøm af data reelt sker fra CSC Danmark til KMD Danmark, optræder denne ikke som logisk datastrøm, fordi der ikke er en aftale mellem disse parter1.

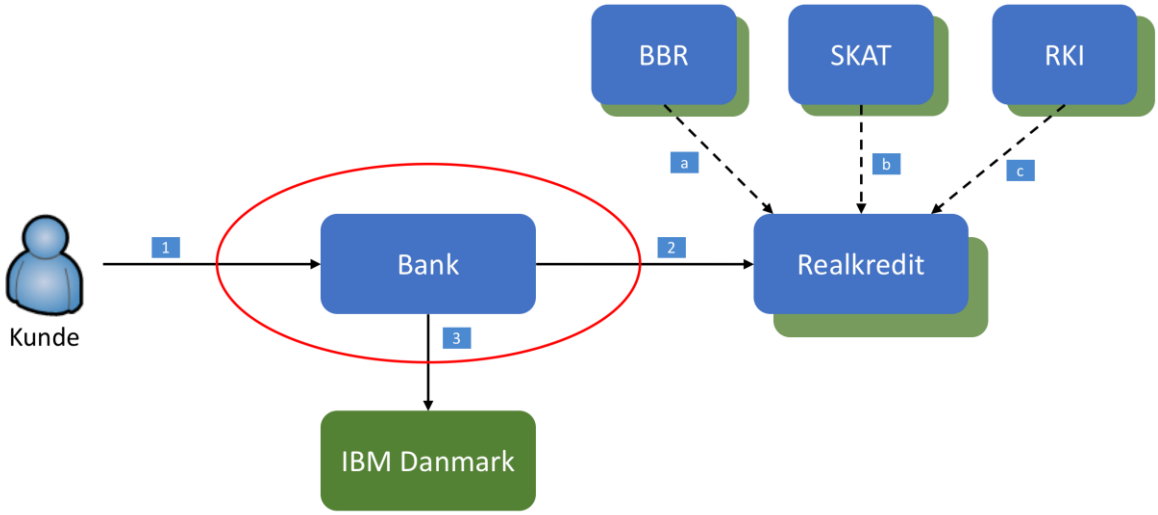
Som Dataansvarlig (København) er andre myndigheders databehandlere ikke relevante i denne sammenhæng. Københavns Kommune opfatter således aftalemæssigt, at de får data fra SKAT, men at de i virkeligheden kommer fra CSC er ikke vigtigt i denne sammenhæng. Her kan henvises til KOMBIT's vejledning om udfyldelses og brug af databehandleraftaler i regi af Videnscentret.

En fjernadgang til data fra et andet land eller en anden organisation betragtes som en overførsel.

Ansøgning om realkreditlån

Denne Dataproces vedrører en digital ansøgning om et realkreditlån udbudt af en bank. Her interagerer brugeren med sin bank i rollen som registreret og indtaster forskellige oplysninger om lånet (fx ønsket størrelse og type). Den første strøm består således i en overførsel af data fra en bruger i rollen som registreret til en bank i rollen som dataansvarlig. Herefter overfører banken oplysninger til et realkreditinstitut (separat organisation), der indhenter oplysninger fra SKAT, BBR, RKI, CPR og andre relevante registre. Realkreditinstituttet agerer i rollen som dataansvarlig for alle de indhentede data og har måske en databehandler, der hoster deres systemer. På baggrund af de indsamlede information laves en kreditvurdering, og kunden modtager et lånetilbud.

[1] Der kan godt være tekniske aftaler, som ikke er relateret til persondatareguleringen, men dette er ikke i fokus her.



De identificerede datastrømme fremgår af nedenstående tabel:

Strøm	Startenhed og rolle	Slutenhed og rolle	Data og kategori
S1	Borger (registreret)	Bank (dataansvarlig)	Stamoplysninger, CPR, lånebeløb, ønsket lånetype (Alm. personoplysninger)
S2	Bank (dataansvarlig)	Realkreditinstitut (dataansvarlig)	Stamoplysninger, CPR, lånebeløb, ønsket lånetype (Alm. personoplysninger)
S3	Bank (dataansvarlig)	Driftsleverandør (databehandler)	Alle ovennævnte oplysninger (Alm. personoplysninger)
a	BBR (dataansvarlig)	Realkreditinstitut (dataansvarlig)	Matrikeloplysninger (Alm. personoplysninger)

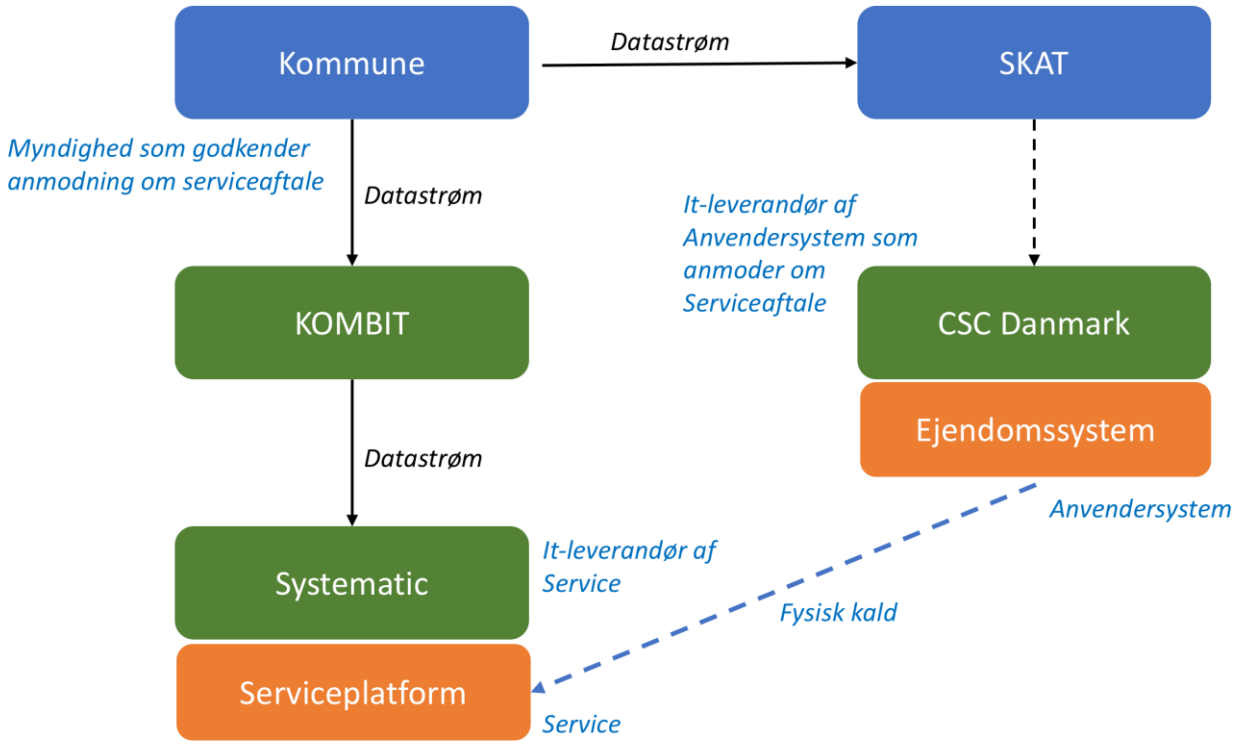
b	SKAT (dataansvarlig)	Realkreditinstitut (dataansvarlig)	Indkomstoplysninger, gæld (Alm. personoplysninger)
c	RKI (dataansvarlig)	Realkreditinstitut (dataansvarlig)	Kreditstatus (Alm. personoplysninger)

Pointer og observationer:

- Strømmene a, b og c er tegnet på for overskuelighedens skyld, men er ikke relevante for bankens perspektiv (banken er ikke part i disse aftaler).
- Alle data er almindelige personoplysninger (ingen følsomme personoplysninger).
- Datastrømmene fra SKAT, RKI, BBR (dataansvarlige) osv. til deres respektive egne driftsleverandører (databehandlere) er ikke relevante her, da disse er dækket af de respektive myndigheders egne databehandleraftaler. Deres driftsleverandører er derfor på figuren indikeret som grønne skygger.
- En strøm hvor der 'svares retur' i naturligvis forlængelse af et kald modelleres blot som én strøm.
- Det er ligegyldigt for analysen af datastrømme, om data er overført på forhånd til et lokalt replika eller hentes via en synkron web services – der er stadig tale om samme datastrøm på logisk niveau.

Anvendelse af serviceplatformen

En lang række systemer i KOMBIT udveksler data via Serviceplatformen, og derfor gives nedenfor et tænkt eksempel på, hvordan denne kan håndteres ved modellering af datastrømme.



I eksemplet ovenfor videregiver en kommune data til SKAT som en datastrøm mellem to dataansvarlige myndigheder. Kommunen anvender KOMBIT som databehandler, og KOMBIT har en underdatabehandleraftale med Systematic vedr. Serviceplatformen. SKAT har på sin side også en databehandler ved CSC Danmark, som driver det system, der fysisk henter data via en snitflade på Serviceplatformen.

KOMBIT styrer adgangen til kommunens data på Serviceplatformen via en serviceaftale, som godkendes af kommunen. På figuren er med blåt angivet rollerne for organisationerne, som de optræder i serviceaftalen. Bemærk at serviceaftalen åbner for det *fysiske* flow af data (den stiplede blå pil viser kaldet), som *ikke* er en logisk datastrøm.

I Administrationsmodulet anmoder CSC i rollen som It-leverandør for SKATs anvendersystem om en serviceaftale med en service udstillet på Serviceplatformen (Serviceudbyder), som kommunen herefter godkender som myndighed. Herefter kan anvendersystemet hente data via servicen.

Kommunen skal selv have styr på sit grundlag for at videregive data til SKAT, og dette grundlag dokumenteres uden for KOMBITs systemer!

C. VEJLEDNING TIL UDFYLDELSE AF SKEMA

Fanen skal indeholde en række stamoplysninger, som identificerer projekt, speciale eller supportfunktionet entydigt, og opmærksomheden henledes særligt på at sikre, at der angives en unik ident jf. det projekt, speciale eller supportfunktionnummer som benyttes i Project Online og i tillæg endvidere anføres reference til Qualiware eller Pactius, hvis et sådant haves.

Fanen Dataprocesser og datastrømme

1. Dataproces

Et projekt, speciale eller supportfunktion kan have flere dataprocesser. En dataproces kan indeholde flere datastrømme. Der skal udfyldes en fane pr. dataproces, hvori datastrømmene til den enkelte proces beskrives. Der kan også oprettes et særskilt excel-skema pr. dataproces.

Formål med dataproces

Der skal udarbejdes en beskrivelse af det grundlæggende formål med løsningen. Behandlingen af personoplysninger kræver i mange tilfælde en lovhjemmel, som bør klarlægges som en del af beskrivelsen af formålet.

Hvis KOMBIT er dataansvarlig, skal der udarbejdes dokumentation for lovligheden. Løsningerne må alene behandle persondata, hvis der enten er indhentet samtykke eller hvis der, alt afhængig af hvilken type data, der er tale om, på anden vis eksisterer et retligt grundlag for behandlingen.

I projekt vil KOMBIT som hovedregel ikke være dataansvarlig, men derimod databehandler. De dataansvarlige (ofte kommunerne) er ansvarlige for, at den behandling af personoplysninger, som bliver foretaget i de løsninger, som KOMBIT stiller til rådighed for kommunerne, er lovlig.

Antal registrerede

Oplysninger om antallet af registerede skal indgå i risikovurderingen af løsningen, og antallet kan således angives indikativit i forhold til at kunne indgå i denne vurdering. Det afgørende er således ikke, om der er 10 eller 20 registrerede men snarere, om der er x-hundrede, x- tusinde eller x-millioner registrerede.

Samtykke

Hvis der ikke eksisterer et andet retligt grundlag for behandlingen af personoplysninger, så skal der indhentes et samtykke fra den registrerede, hvor den dataansvarlige er forpligtet til at kunne dokumentere, at samtykket er givet.

Samtykket til behandling af personoplysninger skal være frit, specifikt, informeret og utvetydigt. Efter GDPR skal samtykket være utvetydig, og hvis der behandles følsomme personoplysninger, skal samtykket tillige være eksplicit.

Samtykket er utvetydigt, når de registrerede foretager en bekræftende handling, som tilkendegiver, at de registrerede accepterer den konkrete behandling af personoplysningerne til det konkrete formål. Eksempler på et sådant samtykke inkluderer, at de registrerede klikker i en boks, vælger indstillinger, afgiver en erklæring eller på anden måde udviser en adfærd, der tilkendegiver samtykket.

Hvis der er tale om samtykke fra børn eller på vegne af børn skal løsningen kunne håndtere, herunder dokumentere dette samtykke på samme måde som almindeligt samtykke.

Sletning

Når personoplysninger ikke længere er nødvendige, skal de som udgangspunkt slettes eller anonymiseres.

Sletning af personoplysninger i et system er en handling, der sikrer, at oplysningerne ikke længere er tilgængelige. Hvis personoplysninger efter sletning fx kan tilgås af systemets administrator, er der ikke tale om en reel sletning.

Det er den dataansvarlige (og i projekt, hvor KOMBIT er databehandler for kommunerne), der – på baggrund af formålene med de behandlinger af personoplysninger der foretages – skal vurdere, hvornår personoplysningerne skal slettes. Det er i den forbindelse vigtigt at den dataansvarlige, for hver af de konkrete behandlinger der foretages, dokumenterer de slettefrister der fastlægges.

Den dataansvarlige (og i projekt, hvor KOMBIT er databehandler for kommuerne) bør sikre sig, at der er taget stilling til hvilke procedurer, der skal følges, når personoplysninger skal slettes fra behandlingssystemerne. En sletteprocedure for et givent system, hvori der behandles personoplysninger, bør tage udgangspunkt i et flow, der følges fra det tidspunkt hvor en personoplysning når sin slettefrist, til sletningen er foretaget og bekræftet i systemet.

Krigsregel

Efter Databeskyttelseslovens § 3, stk. 9, kan Justitsministeren efter forhandling med vedkommende minister fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares her i landet.

Det er ifølge forarbejderne til loven hensigten med den nye udformning af krigsreglen, at IT-systemer - før de tages i brug - af justitsministeren og vedkommende minister kan sættes på en liste, der optages som bilag til bekendtgørelsen i medfør af stk. 9. Endvidere er det hensigten, at IT-systemer alene sættes på denne liste, hvis det vurderes, at det er af hensyn til statens sikkerhed, at det pågældende system skal føres her i landet.

Projekt skal foretage en vurdering af, om personoplysninger i it-løsningen potentielt kan ligge inden for anvendelsesområdet af krigsreglen. Vurderingen skal bruges til at dokumentere, om der er behov for at indlede en dialog med justitsministeriet og vedkommende minister om evt. optagelse af it-løsningen på den ovenfor angivne liste.

1.a Intern overførsel i KOMBIT

Oplysninger om der i det konkrete projekt, speciale eller supportfunktion eller den konkrete enhed er tale om, at de pågældende personoplysninger overføres til andre enheder i KOMBIT (projekt, speciale eller supportfunktioner).

Oplysningerne skal blandt andet bruges som grundlag, når der skal foretages en vurdering af de risici, der er forbundet med behandlingen af personoplysninger samt de dertil hørende organisatoriske og tekniske sikkerhedstiltag, der bliver etableret for behandlingen i interne systemer eller interne processer.

2. Registrerede (datasubjekter)

Oplysninger om hvilke kategorier af registrerede (datasubjekter) skal blandt andet bruges som grundlag, når der skal foretages en vurdering af de risici, der er forbundet med behandlingen af personoplysninger samt de dertil hørende organisatoriske og tekniske sikkerhedstiltag, der bliver etableret for processen eller løsningen.

Derudover skal oplysningerne bruges til identifikation af kategori af registrerede, der skal håndteres under registreredes rettigheder.

3. Kategorier af personoplysninger - datatyper

Forordningen indeholder en opdeling af personoplysninger i forskellige kategorier:

- Almindelige personoplysninger (GDPR artikel 5)
- Følsomme personoplysninger (GDPR artikel 9)
- Personoplysninger om straffedomme & lovovertrædelser (GDPR artikel 10)

Herudover vil der i forhold til kategoriseringen af datatyper være behov for en opdeling af personoplysninger i følgende kategorier:

- Oplysninger om cpr-nummer (Databeskyttelsesforordningens artikel 87 og Databeskyttelseslovens § 11)
- Fortrolige personoplysninger (fx udvalgte almindelige personoplysninger)

Kategoriseringen af personoplysninger og den eventuelle supplerende klassifikation heraf skal indgå i såvel arbejdet med risikovurderinger som fastlæggelsen af de tekniske og organisatoriske sikkerhedstiltag samt kontrollerne heraf.

Almindelige personoplysninger

Almindelige personoplysninger omfatter enhver form for information om en identificeret eller identificerbar fysisk person, herunder fx CPR-nummer, navn, adresse, fødselsdato, email-adresse, uddannelse, stilling, arbejdsområde mm. Behandling af almindelige personoplysninger må finde sted, hvis der er et lovligt formål med behandlingen og der i øvrigt er enten et samtykke eller anden behandlingshjemmel herfor – se mere om dette nedenfor om behandlingsgrundlag.

Følsomme personoplysninger

Følsomme personoplysninger er fx oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Det er som hovedregel forbudt at behandle sådanne følsomme personoplysninger, når de kan henføres eller entydigt identificers med en fysisk person. Behandling af følsomme personoplysninger må dog finde sted, hvis der indhentes samtykke eller i øvrigt er anden hjemmel til at behandle disse – se mere om dette nedenfor om behandlingsgrundlag.

Personoplysninger om straffedomme og lovovertrædelser

Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger, må kun foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder.

Oplysninger om cpr-nummer (Databeskyttelsesforordningens artikel 87 og Databeskyttelseslovens § 11)

Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer. Hvis der i løsningen behandles oplysninger om personnummer (CPR) skal dette registreres i skemaet.

Fortrolige personoplysninger (fx udvalgte almindelige personoplysninger eller CPR-numre)

Spørgsmålet om fortrolighed vil typisk være reguleret i den forvaltningsretlige lovgivning eller anden særlovgivning og derimod ikke direkte reguleret i den databeskyttelsesretlige lovgivning. Det vil imidlertid være relevant at få kortlagt de oplysninger, som skal behandles fortroligt samtidig med kortlægningen af fx almindelige henholdsvis følsomme oplysninger mm i løsningen, idet disse oplysninger også vil få en betydning for dels risikovurderingen og dels i forhold til den organisatoriske og tekniske sikkerhed, der etableres i løsningen.

4. Brug af KOMBIT-interne værktøjer

Oplysninger om der i det konkrete projekt, speciale eller supportfunktion er tale om, at de pågældende personoplysninger behandles i KOMBIT-interne værktøjer (fx email, ShareIT, fildrev) er væsentlig, idet det stiller nogle skærpede krav til især de sikkerhedsmæssige forhold i de værktøjer, som KOMBIT stiller til rådighed herfor.

Oplysningerne skal således blandt andet bruges som grundlag, når der skal foretages en vurdering af de risici, der er forbundet med behandlingen af personoplysninger samt de dertil hørende organisatoriske og tekniske sikkerhedstiltag, der bliver etableret for behandlingen i interne systemer.

4.a Specifikke KOMBIT-interne værktøjer

Se pkt. 4 ovenfor om brug af KOMBIT-interne værktøjer. Her angives oplysninger om, hvorvidt anvendte værktøjer er risikovurderet.

5. Datastrømme

For at kunne fastlægge roller og forpligtelser for henholdsvis dataansvarlig og databehandler i forhold til behandlingen af personoplysninger i løsningen, skal der etableres et overblik over, hvor personoplysningerne kommer fra, hvem der behandler oplysningerne, hvor de opbevares, og hvor de sendes hen (datastrømme).

Overblikket over datastrømme etableres på procesniveau, hvor det for hver proces dokumenteres, hvor data kommer fra (data-ind), opbevares (transit) og hvor data sendes hen (data-ud).

Udgangspunktet for udarbejdelsen af overblik over datastrømme er således på et overordnet niveau, som ikke indeholder meget detaljerede oplysninger, men udarbejdes på et så tilpas overordnet niveau,

at det giver overblikket over især de dele af processen, hvor der fx er tale om skift af snitflader, som fx kan være de steder, hvor der sker ændringer i, hvor data kommer fra og hvor de sendes til.

Formålet med udarbejdelsen af overblik over datastrømme er, at denne fx skal danne baggrund for fastlæggelsen af hvem, der er henholdsvis dataansvarlig, databehandler eller underdatabehandler i forhold til den behandling af personoplysninger, som finder sted inden for den pågældende proces. Niveauet og detaljeringsgraden for de konkrete datastrømme må således bero på en konkret vurdering i det enkelte projekt, speciale eller supportfunktion eller den enkelte proces.

Det anbefales at skrive den juridiske enhed ind og løsningens navn i parentes fx "kommunen (DUBU)" eller Økonomi- og Indenrigsministeriet (CPR) i navnet på datastrømmen.

Dataansvarlig

Det er den dataansvarlige, der bestemmer og har rådigheden over behandlingen af personoplysninger, og det er således den dataansvarlige, der bestemmer om og i hvilket omfang behandlingen skal overlades til en databehandler, der behandler personoplysningerne på vegne af den dataansvarlige.

Databehandleren kan således alene behandle de personoplysninger, som er omfattet af den databehandleraftale og de instrukser, som er aftalt mellem den dataansvarlige og databehandleren.

Hvis databehandleren behandler personoplysninger, som ikke er omfattet af databehandleraftalen eller instruksen, så bliver databehandleren istedet til dataansvarlig for den behandling, der finder sted, og påtager sig dermed ansvaret for, at der fx er hjemmel til at behandle oplysningerne.

Det er derfor vigtigt at faslægge, hvem der er dataansvarlig for behandlingen af personoplysninger i løsningen. Den dataanvarlige har nemlig et omfattende ansvar for både organisatorisk og teknisk at etablere den fornødne sikkerhed for behandlingen af personoplysninger ligesom den dataansvarlige har pligten til at håndtere den registreredes (datasubjektets) rettigheder i forhold til behandlingen af personoplysninger, der finder sted.

Kommunerne er som hovedregel dataansvarlige og KOMBIT er databehandler i de løsninger, som KOMBIT udvikler og forvalter. Dog vil det, idet KOMBIT udvikler og forvalter løsninger på vegne af kommunerne, være nødvendigt, at KOMBIT i tillæg til ansvaret som databehandler også har fokus på det ansvar, der påhviler dataansvarlig, i det omfang ansvaret handler om regler, som implementeres som en del af løsningen.

KOMBIT's løsninger skal således som hovedregel stille funktionalitet til rådighed, der gør det muligt for kommunerne at overholde lovgivningen, og i de tilfælde, hvor lovgivningens krav ikke er understøttet af funktionalitet i løsningen, da skal der udarbejdes dokumentation for, i hvilket omfang og hvordan kravene fx håndteres organisatorisk hos dataansvarlig eller databehandler.

For så vidt angår behandlingen af personoplysninger internt i KOMBIT fx i HR, Økonomi eller Intern It, hvor KOMBIT indsamler og behandler disse, da vil det være KOMBIT, der er dataansvarlig. Og i det

omfang KOMBIT overlader behandlingen af personoplysninger til fx eksterne leverandører fx Enalyzer, EU-supply, KL eller andre, da vil disse leverandører blive databehandlere for KOMBIT.

KOMBIT har derfor ansvaret for at sikre, at der foreligger den fornødne sikkerhed for leverandørens behandling af de personoplysninger, som KOMBIT har ansvaret for, hvilket typisk sker i en databehandleraftale og/eller den hovedaftale, der ligger til grund for behandlingen af de pågældende personoplysninger.

Databehandler

KOMBIT vil som hovedregel være databehandler i de løsninger, som KOMBIT udvikler og forvalter for kommunerne. Databehandlerens forpligtelser har hidtil alene være reguleret i databehandleraftalen indgået mellem den dataansvarlige og databehandleren, men der introduceres altså nu i forordningen særlige forpligtelser. Væsentligst er det, at databehandleren er forpligtet til at hjælpe den dataansvarlige med at efterleve en række af sine forpligtelser, og at databehandleren har en forpligtelse til at oplyse den dataansvarlige, hvis de vurderer, at fx en instruktion er ulovlig.

En databehandler er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

En databehandler kendetegnes ved altså kun at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig. Databehandleren behandler således aldrig personoplysninger til egne formål og må derfor ikke bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

En databehandler kan fx være en virksomhed, som varetager en anden virksomhed eller en myndigheds it-systemer. Endvidere kan en databehandler være en udbyder af et webhotel, der hoster hjemmesider for andre.

Retsgrundlag

I skemaets rubrik om datastrømme bliver projekt, speciale eller supportfunktionerne bedt om at angive retsgrundlaget for den overførsel af personoplysninger, som finder sted i løsningen i forhold til den konkrete datastrøm. Her er altså ikke tale om, at projekt skal angive den hjemmel, som kommunen har til at behandle personoplysningerne.

Kommunerne har - som dataansvarlig - ansvaret for, at den behandling af personoplysninger, som bliver foretaget i de løsninger, som KOMBIT stiller til rådighed for kommunerne, er lovlig.

KOMBIT har - som databehandler – alene ansvaret for at dokumentere retsgrundlaget for den behandling af personoplysninger, som KOMBIT foretager i løsningerne på vegne af kommunerne.

Projektet skal altså hverken redegøre eller dokumentere den hjemmel, som kommunerne skal have til at behandle personoplysninger, men skal derimod – og det er vigtigt – kunne dokumentere det retsgrundlag,

som KOMBIT har til at behandle personoplysningerne på vegne af kommunerne i den pågældende datastrøm.

KOMBITs hjemmel til at behandle personoplysninger vil oftest være en databehandleraftale med tilhørende instrukser, som udarbejdes med baggrund i netop de datastrømme, som projektet har kortlagt i løsningen.

Databehandleraftale

KOMBIT kan som databehandler alene behandle data, hvis der er indgået en databehandleraftale med den dataanvarlige herom og i den forbindelse modtaget konkrete instrukser, som nærmere regulerer hvad KOMBIT må behandle, og i hviket omfang det behandlede må blive videregivet og til hvem.

Når KOMBIT indgår aftale med en leverandør, der skal udvikle eller forvalte løsningerne, da vil der skulle udarbejdes en underdatabehandleraftale mellem KOMBIT og leverandøren, som svarer til den databehandleraftale, som KOMBIT har med kommunerne (dataansvarlig).

Når leverandøren indgår aftale med en underleverandør, som fx skal forvalte løsningerne, vil der skulle udarbejdes en under-underdatabehandleraftale mellem leverandøren og underleverandøren, som svarer til den databehandleraftale, som KOMBIT har med kommunerne (dataansvarlig).

Kommunerne skal kunne kontrollere, at de data, som de har ansvaret for, behandles i overensstemmelse med reglerne herfor. Kommunerne har således som dataansvarlig indsigts- og indsigelsesret i forhold til de underdatabehandleraftaler og under-underdatabehandleraftaler, som KOMBIT og KOMBIT's underdatabehandlere indgår i forbindelse med udvikling og forvaltning af løsningen. KOMBIT vil have et ansvar overfor kommunerne i forhold til at sikre sig, at underdatabehandler- og under-underdatabehandleraftaler svarer til den databehandleraftale, som KOMBIT har med kommunerne (dataansvarlig).

I vurderingen af behovet for og omfanget af databehandleraftaler kan der med fordel tages afsæt i en oversigt over processer (behandlingsaktiviteter) og datastrømme således, at der i det omfang, der anvendes databehandler, underdatabehandler og eventuelt under-underdatabehandler, da vil der skulle foreligge databehandleraftaler herfor.

Hvis man som databehandler behandler personoplysninger uden at have den fornødne instruks, da vil databehandleren blive dataansvarlig for behandlingen af de konkrete personoplysninger, som behandles uden instruks. Som dataansvarlig vil den oprindelige databehandler således få ansvaret for, at fx behandlingsgrundlaget er tilstede, hvilket kan være ganske problematisk, hvis en hjemmel til behandling af oplysningerne alene er givet til en anden myndighed.

Overførsel til tredjelande

Der gælder en række særlige regler for "overførsel" af personoplysninger til tredjelande, også kaldet tredjelandsoverførsler.

Begrebet "overførsel" dækker både den situation, hvor en dataansvarlig i EU *videregiver* personoplysninger til en dataansvarlig uden for EU og den situation, hvor en dataansvarlig (eller en databehandler) i EU *overlader* en behandling af personoplysninger til en databehandler uden for EU.

En overførsel kan f.eks. bestå i en elektronisk transmission eller i en fremsendelse af en USB nøgle, men en overførsel kan også bestå i, at personer i et tredjeland blot gives "se-adgang" til oplysninger, der befinder sig i EU.

Eksempel 1: En virksomhed etableret i Danmark ønsker at benytte en virksomhed i Indien til IT-support. De indiske medarbejdere har ikke teknisk adgang til at lagre eller printe personoplysninger, men har alene adgang til at se oplysningerne.

Der er tale om en overførsel til et tredjeland, da personoplysninger i Danmark gøres tilgængelige for medarbejderne i den indiske virksomhed. Det gør ingen forskel, at oplysningerne alene kan ses i Indien eller, at medarbejderne ikke forstår dansk.

Reglerne skal sikre, at den databeskyttelse som de registrerede borgere, kunder m.fl. er sikret i EU efter databeskyttelsesforordningens regler ikke bliver udvandet, blot fordi oplysningerne overføres til lande uden for EU's grænser.

Nedenstående er en kort oplistning (ikke udtømmende) af overførselsgrundlag i den forbindelse:

- Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet (sikre tredjelande)
- Overførsler omfattet af fornødne garantier (artikel 46)
- Bindende virksomhedsregler – Binding Corporate Rules (ofte blot kaldet BCR)
- EU-Kommissionens standardkontraktbestemmelser
- EU-U.S. Privacy Shield

Hvis der er behov for at overføre personoplysninger til et tredjeland, er det vigtigt, at projekt, speciale eller supportfunktionet/den interne enhed er opmærksom på også at have et grundlag for at kunne overføre oplysningerne til et tredjeland.

Datastrøm til Digitalpost (e-Boks)

Datastrømmen skal gå mellem dataansvarlig (fx ”Kommune (KY)”) og ”Modtager af Digitalpost”/”Afsender af Digitalpost”. Dvs. Digitalpost (e-Boks) skal ikke angives som ”Afsender” eller ”Modtager” i datastrømmen. I stedet angives enten ”Modtager af Digitalpost” eller ”Afsender af Digitalpost” afhængigt af, hvilken vej datastrømmen går.

Den korte forklaring på, hvorfor vi er nået frem til denne model, er, at borgeren/virksomheden anses som dataansvarlig, så snart kommunen har sendt beskeden til Digitalpost. I den analoge verden svarer det til, at du, som modtager af et fysisk brev, bliver ansvarlig for brevet, når det er lagt i din postkasse, og vil herefter være ansvarlig for eventuelt at reagere på brevet, ligesom du selv bestemmer, om det skal gemmes eller smides ud. Modtageren af et brev i e-Boks bliver således, som med brevet i postkassen, ansvarlig for den post, der afleveres i postkassen.

Datastrøm til fjernprint

Datastrømmen er her mellem dataansvarlig (fx ”Kommune (KY)”) og ”Kommune (fjernprint)”. I GDPR-sammenhæng og i forbindelse med kortlægning af datastrømme er der tale om det, vi anser som en intern overførsel i kommunen, hvilket betyder, at der ikke er tale om en logisk datastrøm (overførsel mellem forskellige juridiske enheder). I stedet er der tale om en fysisk datastrøm. Den fysiske datastrøm skal kun dokumenteres af projekt, speciale eller supportfunktionet, hvis overførslen sker uden for Administrationsmodulet.

I sådanne tilfælde vil datastrømmen gå mellem KOMBITs leverandør (som fysisk sender/modtager) og ”Kommune (fjernprint)”. KDI dokumenterer overførsler, som sker inden for Administrationsmodulet. Modtageren af den post, som kommunen får udskrevet hos fjernprint, bliver i denne situation først dataansvarlig, når posten afleveres hos modtageren, jf. også eksemplet ovenfor om datastrøm til Digital post.