Notat om behandling af oplysninger fra eFaktura i indkøbsdatasamarbejdet

1. INDLEDNING OG KONKLUSION

1.1 Indledning

Staten og Kommunernes Indkøbsservice A/S (herefter SKI) er på vegne af KL, en række kommuner og andre offentlige organisationer operatør på et indkøbsdatasamarbejde, der blev etableret i 2017. Samarbejdet bygger oven på et fælleskommunalt indkøbsdataprojekt, som fandt sted i 2015 og 2016, og det indebar udviklingen af en såkaldt indkøbsdatamodel.

Formålet med indkøbsdatamodellen og dermed det videreførte samarbejde er overordnet set, at SKI kan udarbejde analyser, der kan bruges til at effektivisere offentlige indkøb på tværs og for den enkelte organisation. Modellen forudsætter anvendelsen af indkøbsdata i form af eFakturadata, som indgår i kommunerne og andre offentlige organisationer fra leverandører i forbindelse med konkrete anskaffelse og ydelser. SKI forestår som operatør på samarbejdet indsamling og analyse af indkøbsdata i samarbejde med deres leverandører.

Uanset, at det følger af retningslinjerne for eFaktura, at disse ikke bør indeholde uvedkommende personoplysninger, er det konstateret, at de i indkøbsdatamodellen anvendte eFakturadata alligevel i begrænset omfang kan indeholde en række personoplysninger om de borgere, hvor ydelsen er leveret eller om f.eks. offentlige kontaktpersoner mv. SKI har på den baggrund anmodet om vores vurdering af, om og i så fald hvordan offentlige organisationer kan overlade eFakturadata til SKI og dennes leverandører under overholdelse af de relevante krav i databeskyttelseslovgivningen.

SKI har bedt Kammeradvokaten om at vurdere, om indkøbsdatasamarbejdet er i overensstemmelse med kravene i databeskyttelsesloven[1] samt databeskyttelsesforordningens[2] almindelige behandlingsregler (databeskyttelseslovens §§ 5 – 11) samt hvordan en databehandleraftale mellem SKI og de deltagende offentlige organisationer skal udformes.

[1] Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

[2] Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

KØBENHAVN
VESTER FARIMAGSGADE 23
DK-1606 KØBENHAVN V

AARHUS
ÅBOULEVARDEN 49
DK-8000 AARHUS C

T +45 33 15 20 10
@ MAIL@POULSCHMITH.DK
W WWW.POULSCHMITH.DK

Kammeradvokaten har således ikke efter aftale med SKI foretaget en gennemgang og vurdering af it-platformen i forhold til databeskyttelsesloven og databeskyttelsesforordningens regler om sikkerhed (herunder logning, identitets- og brugerkontrol, transmissionssikkerhed mv.) og reglerne om den registreredes rettigheder (oplysningspligt over for den registrerede, indsigtsret mv.). SKI har oplyst, at SKI opfylder disse regler og vil forpligte sin leverandør til overholdelse. De sikkerhedsmæssige aspekter ift. den nye infrastruktur-leverandør (cloud-provideren), herunder forholdet til vedkommendes underleverandør, behandles ikke i dette notat, men i SKI's risikovurdering og aftale med den valgte leverandør.

Kammeradvokaten går ud fra, at de offentlige organisationer selv har foretaget en eventuel konsekvensanalyse vedrørende databeskyttelse i overensstemmelse med databeskyttelsesforordningens artikel 35, samt foretaget en eventuel forudgående høring af Datatilsynet som beskrevet i databeskyttelsesforordningens artikel 36.

Kammeradvokaten lægger desuden til grund, at de offentlige organisationer selv gemmer og håndterer modtagne fakturaer uafhængigt af SKI (i et primært fakturasystem), og at overladelsen af fakturaerne – og dermed eventuelle personoplysninger – til behandling hos SKI derfor udgør et supplement hertil i et analysemæssigt øjemed. SKI's indsamling af indkøbsdata udgør således ikke et fakturahåndteringssystem for de offentlige organisationers eFaktura.

1.2 Sammenfatning

Sammenfattende et det vores vurdering, at offentlige organisationer, der indgår i indkøbsdatasamarbejdet, kan overlade eFakturadata til SKI og dennes leverandører uden at bryde databeskyttelseslovgivningens almindelige behandlingsregler (databeskyttelseslovens §§ 5 - 11) eller databeskyttelsesforordningen, hvis følgende forudsætninger er opfyldt:

- Offentlige organisationer overlader kun eFaktura med personoplysninger til SKI, for at SKI som databehandler på den respektive organisations vegne kan udføre analyser, udarbejde aggregerede rapporter, udføre statistik mv. med henblik på at give mulighed for, at organisationen selv – eller øvrige organisationer eller KL – kan udnytte analyseresultaterne til at effektivisere det offentliges indkøb samt bidrage til klimavenlige og bæredygtige indkøb.

- Analyserne foretages alene på almindelige personoplysninger (navne, kontaktdata, CPR-numre), og fejlagtigt registrerede følsomme oplysninger frasorteres inden analyserne. SKI tager på vegne af de dataansvarlige nødvendige skridt til at minimere omfanget af unødvendige personoplysninger, som overlades og indirekte indgår i grundlaget for indkøbsanalyserne. Ved unødvendige forstås oplysninger, der er ikke nødvendige for varetagelsen af formålet med indkøbsdatasamarbejdet, f.eks. oplysninger om den borger, som det enkelte indkøb vedrører. Dette kan ske ved en minimering gennem filtrering af mulige personoplysninger i de pågældende fakturaer i videst muligt omfang.

- SKI kan som databehandler overlades en kopi af den originale fakturadata med henblik på at skabe analysegrundlaget, men når analysegrundlaget er tilvejebragt og kopien af originalfaktura

ikke længere er nødvendig, skal kopien slettes. Det samme gælder, når den originale faktura enten arkiveres eller kasseres hos den respektive offentlige organisation. SKI har oplyst, at oplysningerne kan slettes senest efter 5 år fra modtagelse af data.

- Offentlige organisationer skal indgå en gyldig databehandleraftale med SKI, og der indgås en underdatabehandleraftale med SKI's leverandør, hvoraf fremgår at SKI og underdatabehandleren i forhold til de overladte oplysninger alene handler efter instruks fra den pågældende offentlige organisation, og at de øvrige krav til databehandleraftaler er opfyldt. Sikkerhedskrav i databehandleraftale og underdatabehandleraftale skal bero på en risikovurdering efter databeskyttelsesforordningens artikel 32.

- SKI's brug af underdatabehandlere, som tilbyder en cloud-platform, overholder databeskyttelseslovgivningens krav og sker efter en generel eller konkret skriftlig godkendelse fra den offentlige organisation. Det indebærer, at SKI sikrer, at underdatabehandleren er underlagt samme beskyttelseskrav som SKI, og at SKI kontrollerer, at disse krav er overholdt. Det er som nævnt bl.a. en forudsætning for brugen af cloud-løsningen, at der er foretaget en risikovurdering, og at der fastsættes passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som passer til risikovurderingen. Det er ligeledes et krav, at underdatabehandleren ikke overfører personoplysninger til et tredjeland uden et overførselsgrundlag og en forudgående godkendelse fra den dataansvarlige offentlige organisation.

- Medmindre den dataansvarlige offentlige organisation konkret instruerer SKI herom, videregiver eller overfører SKI ikke i nogen sammenhæng eller under nogen omstændigheder de overladte personoplysninger fra fakturadata til andre (KL, øvrige offentlige organisationer mv.) ud over underdatabehandleren i overensstemmelse med aftalen, herunder også de øvrige offentlige organisationer i samarbejdet enten direkte eller indirekte. SKI anvender i den forbindelse heller ikke oplysninger i personhenførbar form til samkøring eller fælles analyse med øvrige offentlige organisationers oplysninger. Videregivelse og samkøring kan således alene ske i anonymiseret, ikke-personhenførbar form. Disse regler gælder dog ikke i forhold til oplysninger om leverandørnavne (hvor disse er personligt ejede virksomheder) samt kontaktoplysninger på medarbejdere hos disse i denne egenskab.

- De dataansvarlige offentlige organisationer skal sikre regeloverholdelse i eget ansvarsområde ift. analyserne. Det gælder f.eks. ift. underretning af de registrerede (databeskyttelsesforordningens artikel 13 og 14) samt pligten til at overveje gennemførelse af en konsekvensanalyse for databeskyttelse (DPIA).

Ud fra, hvad Kammeradvokaten er gjort bekendt med, vil SKI imødekomme ovenstående betingelser.

2. DET FAKTUELLE GRUNDLAG

2.1 Formålet med indkøbsdatasamarbejdet

I regeringens aftale med KL om kommunernes økonomi for 2015 blev parterne enige om, at et vigtigt fokusområde for det offentlige indkøb fremover vil være at sikre en høj anvendelsesgrad af såvel de fælleskommunale aftaler som andre typer af forpligtende aftaler. Af den grund blev det aftalt, at der skulle igangsættes en analyse af, hvordan kommunernes indkøbsdata kunne anvendes til at sikre en høj grad af compliance.

I kølvandet herpå gennemførte SKI i samarbejde med KL i 2015 og 2016 et projekt, hvor der blev indhentet eFakturadata fra 54 kommuner, der frivilligt valgte at indgå i et indkøbsdataprojekt. Alle deltagende kommuner fik i forbindelse med projektet et antal analyserapporter, der sammenlignede den pågældende kommunes indkøb med gennemsnittet af alle deltagende kommuners indkøb.

Efter afslutningen på dette indkøbsdataprojekt var det et ønske blandt deltagerne, at det skulle overgå til et fælleskommunalt indkøbsdatasamarbejde. SKI har af den grund udviklet en indkøbsdatamodel, som skulle analysere indkøbsdata. Ved udgangen af 2019 indeholder indkøbsdatasamarbejdet fakturadata for 92 deltagende kommuner for årene 2014-2019.

Indkøbsdatasamarbejdet er efterfølgende blevet udvidet til professionshøjskoler. Professionshøjskolerne har leveret fakturadata for årene 2016 og 2017. SKI har på den baggrund lavet individuelle rapporter af den enkelte professionshøjskole og sammenlignende rapporter på tværs af professionshøjskolerne.

SKI ønsker at videreføre indkøbsdatasamarbejdet, så såvel kommuner, professionshøjskoler som andre sektorer og organisationer i den offentlige sektor får mulighed for at indgå i samarbejdet.

Med udgangspunkt i data fra indkøbsdatasamarbejdet udarbejder SKI rapporter m.v. til de deltagende offentlige organisationer, hvorved hver enkelt offentlige organisation kan sammenligne sin egen indkøbsprofil med de tilsvarende offentlige organisationers indkøbsprofiler. I og med at der er indkøbsdata fra flere år, er der være mulighed for at se udviklingen af den enkelte offentlige organisations indkøb over tid og sammenholde denne udvikling med tilsvarende offentlige organisationers udvikling i perioden. Analyseresultaterne videreformidles i anonymiseret form, bortset fra de analyser, der udarbejdes til en konkret offentlige organisations egen brug. Derudover vil SKI også anvende data til at understøtte sin almindelige virksomhed med at effektivisere det offentlige indkøb, herunder arbejdet med at udvælge og udbyde relevante udbudsområder i form af såvel frivillige som forpligtende rammeaftaler.

Disse betragtninger er sammenfattet i afsnittet "Hvad får kommunerne ud af det?" i dokumentet "Det fælleskommunale indkøbsdatasamarbejde". Her oplyser SKI, at:

> *"Kommunerne, der deltager i indkøbssamarbejdet, bidrager til at få udviklet (ny) viden, som kan bruges til at effektivisere det kommunale indkøb. Den viden vil bl.a. kunne ligge til grund for bedre aftaler udarbejdet af den enkelte kommune, indkøbsfællesskaber eller SKI, der bl.a. kan bruge data til at udarbejde bedre forpligtende kommunale aftaler. Derudover vil kommunerne få adgang til*

en række kommunespecifikke rapporter, der især belyser, hvordan kommunen ligger i forhold til andre kommuner på fx compliance og indkøbsmønstre. På den baggrund vil kommunerne kunne se, hvor de hver især måske har et potentiale for forbedringer".

SKI har desuden oplyst, at indkøbssamarbejdet ønskes udvidet i 2021 med henblik på at bidrage til at fremme klimadagsordnen og bæredygtige indkøb. Formålet med indkøbssamarbejdet udbygges herefter til også at omfatte beregninger og analyser af data til at optimere grønne og klimavenlige indkøb. Det er bl.a. hensigten at foretage klimaberegninger, som siger noget om det om udledningen af $C0_2$ i forbindelse med offentlige indkøb, og løbende rapportere om udviklingen, herunder også at rapportere til KL. Det er også hensigten at lave grønne analyser, hvor det f.eks. opgøres antal miljøvenlige biler, strømforbrug og indkøb af økologiske produkter, hvorefter de enkelte deltagere i indkøbssamarbejdet kan sammenlignes og rangeres.

Kammeradvokaten lægger på den baggrund til grund, at det overordnede formål med indkøbsdatasamarbejdet er at opnå viden til at kunne optimere offentlige indkøb.

2.2 Personoplysninger i eFakturadata

SKI har oplyst, at der i eFakturaerne kan indgå personoplysninger. Vi har lagt til grund, at eFakturadata i begrænset omfang kan indeholde almindelige personoplysninger såsom adresse, CPR-numre, navne, adresser mv. SKI kan ikke afvise, at eFakturaerne også enten direkte eller indirekte kan indeholde fejlagtigt registrerede følsomme personoplysninger omfattet af databeskyttelseslovens § 7 og databeskyttelsesforordningens artikel 9.

SKI finder det dog usandsynligt, at de enkelte faktura indeholder oplysninger omfattet af databeskyttelseslovens § 8 og databeskyttelsesforordningens artikel 10, dvs. bl.a. oplysninger om strafbare forhold.

SKI tager på vegne af de dataansvarlige nødvendige skridt til at minimere omfanget af unødvendige personoplysninger, som overlades og indirekte indgår i grundlaget for indkøbsanalyserne. Ved unødvendige forstås oplysninger, der er ikke nødvendige for varetagelsen af formålet med indkøbsdatasamarbejdet – f.eks. oplysninger om den borger, som det enkelte indkøb vedrører. Dette sker ved en minimering gennem filtrering af mulige personoplysninger i de pågældende fakturaer i videst muligt omfang. Personoplysningerne anonymiseres i den forbindelse ved at den enkelte personoplysning bliver erstattet af generiske ord.

SKI har oplyst, at det fremadrettet er et ønske at overgå til en ny infrastrukturløsning, hvor data opbevares eksternt ved en underleverandør. Data ønskes opbevaret i en cloudplatform, hvor oplysningerne lageres på eksterne servere hos en underleverandør.

3. RETSGRUNDLAGET

3.1 Databeskyttelsesloven og databeskyttelsesforordningens anvendelsesområde

Databeskyttelsesloven og databeskyttelsesforordningen gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk (ikke-automatisk) behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. databeskyttelseslovens § 1, stk. 2 og databeskyttelsesforordningens artikel 2, stk. 1.

Efter databeskyttelsesforordningens artikel 4, nr. 1, forstås ved personoplysninger enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). I databeskyttelsesforordningen fremgår, at der ved en identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Behandling defineres ifølge databeskyttelsesforordningens artikel 4, nr. 2, som enhver operation (aktivitet) eller række af operationer (aktiviteter) med eller uden brug af elektronisk (automatisk) databehandling, som oplysninger (eller en samling af personoplysninger) gøres til genstand for. Omfattet af begrebet er således ikke blot registrering, opbevaring, videregivelse og samkøring af oplysninger, men derimod enhver form for håndtering af oplysninger.

Anonyme oplysninger vil ikke udgøre personoplysninger. Ved afgørelsen af, om en person er identificerbar, og dermed ikke anonym, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende, tages i betragtning. Ombudsmanden har i en sag fra 27. juli 2009 (FOB 2009 5-2) indhentet en udtalelse fra Datatilsynet om anonymisering, hvoraf bl.a. følgende fremgik:

> *"Tilstedeværelsen af en identifikationskode, et løbenummer eller lignende, der et eller andet sted kan oversættes til den oprindelige personoplysning (navn m.v.), medfører efter Datatilsynets opfattelse, at der foreligger personoplysninger omfattet af persondataloven. Det samme gælder for journalnumre, sagsnumre og lignende."*

I udtalelsen anfører Datatilsynet videre, at:

> *"Også de tilfælde, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen. Det er med andre ord tilstrækkeligt, at der i forbindelse med behandlingen er etableret en ordning med et løbenummer eller lignende, f.eks. medlemsnummer eller journalnummer. Er f.eks. navn eller adresse erstattet af en kode, der kan føres tilbage til den oprindelige individuelle personoplysning, vil der stadigvæk være tale om en personoplysning."*

For at databeskyttelsesloven og databeskyttelsesforordningen ikke skal finde anvendelse, kræver det med andre ord, at anonymiseringen skal være effektiv. Hvis anonymiseringen ikke er effektiv, vil regelsættene finde anvendelse, jf. også Peter Blume, Den Nye Persondataret, Persondataforordningen (2016), s. 58.

3.2 Dataansvarlig og databehandler

Det er som udgangspunkt den dataansvarlige (offentlige organisationer i dette tilfælde), som er ansvarlig for overholdelsen af databeskyttelsesloven og databeskyttelsesforordningen, og som har en række pligter i medfør heraf. I databeskyttelsesforordningens artikel 4, nr. 8, defineres den dataansvarlige som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

I databeskyttelsesforordningens artikel 4, nr. 8, defineres en databehandler som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne. En databehandler kendetegnes altså ved kun at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig. Databehandleren behandler således aldrig personoplysninger til egne formål eller bruger de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

Databehandlerens behandling af oplysninger betragtes som en overladelse af de oplysninger, videregivelse, og dataansvaret er dermed overgået til den modtagende part, der betragtes som tredjemand og ny dataansvarlig. Hvis det derimod er en forudsætning mellem parterne, at den oprindelige dataansvarlige ikke længere har rådighed over oplysningerne, og at den modtagende part kan anvende oplysningerne til egne formål, er der tale om videregivelse, og dataansvaret er dermed overgået til den modtagende part, der betragtes som tredjemand og ny dataansvarlig, jf. Waaben og Korfits Nielsen, Lov om behandling af personoplysninger med kommentarer (2015), s. 165.

3.3 Databeskyttelsesloven og databeskyttelsesforordningens behandlingsregler

Enhver behandling af personoplysninger skal have hjemmel i databeskyttelsesloven og databeskyttelsesforordningen. Hjemmelsgrundlaget afhænger af, om der er tale om en almindelig personoplysning (databeskyttelseslovens § 6 og databeskyttelsesforordningens artikel 6) eller følsomme personoplysninger (databeskyttelseslovens §§ 7-10 og databeskyttelsesforordningens artikel 9-10).

Derudover skal enhver behandling ske i overensstemmelse med de grundlæggende principper i databeskyttelsesforordningens artikel 5. Det fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra a, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«).

Af databeskyttelseslovens § 5, stk. 1, og databeskyttelsesforordningens artikel 5, stk. 1, litra b, følger, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige (legitime) formål, og at senere behandling (viderebehandling) ikke må være uforenelig med disse formål. Efter databeskyttelsesforordningens artikel 5, stk. 1, nr. 3, skal oplysninger, som behandles, være relevante og tilstrækkelige og ikke

omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysninger indsamles. Med andre ord må der ikke ske indsamling af oplysninger, som ikke er nødvendige eller relevante. Dette følger også af almindelige forvaltningsretlige principper om saglighed og proportionalitet i forbindelse med forvaltningsvirksomhed, jf. f.eks. Folketingets Ombudsmands beretning for 2011, sag nr. 15-1.

Efter databeskyttelsesforordningen artikel 6, stk. 1, litra e, kan personoplysninger behandles, når behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. I databeskyttelsesforordningens præambel nr. 45, fremgår det, at hvis behandlingen er nødvendig for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, bør behandlingen have retsgrundlag i EU-retten eller medlemsstaternes nationale ret. Der kræves dog ikke en specifik lov til hver enkelt behandling, men blot et retsgrundlag, som er klart og forudsigeligt for de berørte personer, jf. præamblens nr. 41. Det kan i almindelighed lægges til grund, at artikel 6, stk. 1, litra e, hjemler store dele af den persondatabehandling, som finder sted i den danske offentlige forvaltning, jf. Peter Blume, Den Nye Persondataret, Persondataforordningen (2016), s. 79.

For så vidt angår følsomme personoplysninger følger det endvidere af databeskyttelseslovens artikel 9, stk. 2, at behandlingen af sådanne følsomme oplysninger kun kan finde sted ved, jf. litra j, arkivering, forskning og statiske formål.

Databeskyttelseslovens § 10, stk. 1, fastslår, at oplysninger som nævnt i databeskyttelsesforordningens artikel 9 og 10 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne. Videre fremgår det af lovens § 10, stk. 2, at de pågældende oplysninger ikke senere må behandles i andet end statistisk eller videnskabeligt øjemed.

Endelig fremgår det af § 10, stk. 3, at de af stk. 1 og 2 omfattede oplysninger kun må videregives til tredjemand efter forudgående tilladelse fra tilsynsmyndigheden, når 1) behandlingen sker uden for forordningens anvendelsesområde, 2) vedrører biologisk materiale, 3) sker med henblik på offentliggørelse i et anerkendt tidsskrift el.lign. Tilsynsmyndighederne kan fastsætte generelle vilkår for videregivelse af oplysninger omfattet af stk. 1 og 2, og sundhedsministeren kan fastsætte regler om, at oplysninger omfattet af stk. 1 og 2, som er behandlet med henblik på at udføre sundhedsfaglige statistiske og videnskabelige undersøgelser, senere kan behandles i andet end statistisk eller videnskabeligt øjemed, hvis behandlingen er nødvendig af hensyn til varetagelse af den registreredes vitale interesser.

Databeskyttelseslovens § 11 fastslår, at offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer, hvorimod private alene kan behandle personoplysninger under særlige betingelser, jf. stk. 2, nr. 1-4.

3.4 Databehandleraftaler

Forholdet mellem en databehandler og dataansvarlig er nærmere reguleret i databeskyttelsesforordningens kapitel IV. Kravet om, at der skal indgås de såkaldte databehandleraftaler, finder man i databeskyttelsesforordningens artikel 28, stk. 3. Indholdet af bestemmelserne er dog i modsætning til ovenstående langt fra identiske.

I databeskyttelsesforordningens artikel 28, stk. 3, fremgår det, at en databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige. Kontrakten eller dette andet retlige dokument skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder.

Kontrakten eller dette andet retlige dokument skal derudover navnlig fastsætte, at databehandleren:

a) kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser
b) sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt,
c) iværksætter alle foranstaltninger, som kræves i henhold til artikel 32 (behandlingssikkerhed),
d) opfylder de betingelser, der er omhandlet i artikel 28, stk. 2 (samtykke) og stk. 4 (underdatabehandleraftale), for at gøre brug af en anden databehandler,
e) under hensyntagen til behandlingens karakter, så vidt muligt bistår den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III
f) bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren
g) efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne
h) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner,

herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Databehandleren underretter derudover omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

I artikel 28, stk. 9, fremgår det, at kontrakten eller det andet retlige dokument skal foreligge skriftligt, herunder i elektronisk form.

4. VURDERING

4.1 Behandlingsgrundlag

Som det fremgår af punkt 2.2, indgår en række personoplysninger i de eFakuradata, som SKI indsamler og dermed behandler. For så vidt angår almindelige personoplysninger omfattet af databeskyttelseslovens § 6 og databeskyttelsesforordningens artikel 6 må det antages, at eFakturaerne med sikkerhed vil kunne indeholde sådanne oplysninger, såsom eksempelvis oplysninger om leverandørers navn og adresse samt CPR-numre. Dertil kommer andre oplysninger om berørte borgere, som ikke udtømmende kan angives, men som har karakter af almindelige personoplysninger.

Databeskyttelsesloven og databeskyttelsesforordningen finder derfor anvendelse ved behandlingen af disse oplysninger.

Spørgsmålet om, hvorvidt en offentlige organisation lovligt kan overlade fakturaerne og dermed personoplysningerne til SKI med henblik på analyse mv., afhænger i første række af, om en offentlige organisation selv har hjemmel til at foretage behandlingen, dvs. gennemføre analyser med henblik på at optimere sine indkøb. Indsamlingen af data og den forbundne behandling skal efter det oplyste medvirke til at optimere offentlige organisationers indkøb, dvs. en mere effektiv ressourceanvendelse af offentlige midler. Dette er i almindelighed et sagligt formål, som falder inden for databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Efter databeskyttelsesforordningens artikel 5 skal oplysninger, som behandles, kun være de relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles. Det må antages, at de offentlige organisationers eFaktura vil indeholde almindelige personoplysninger, som er nødvendige for varetagelsen af formålet med indkøbsdatasamarbejdet. Det kan eksempelvis være leverandørnavne mv. Omvendt må det også antages, at kommunernes eFaktura vil indeholde både almindelige og følsomme personoplysninger, som ikke er nødvendige for varetagelsen af dette formål, men som overlades til SKI med henblik på analyserne.

Der er efter vores vurdering ikke grundlag i databeskyttelsesforordningens artikel 9, stk. 2, til behandling af følsomme oplysninger fra eFakturaer med det formål at optimere kommunernes indkøb. Det vil

derfor være i strid med databeskyttelsesforordningens artikel 9, stk. 1, hvis kommunerne overlader følsomme oplysninger, der fejlagtigt indgår i eFakturaer, til SKI med henblik på at indgå i grundlaget for analyser i indkøbsanalysesystemet. Jeg har ikke grundlag for at vurdere, om SKI kan anvende databeskyttelseslovens § 10, for at anvende følsomme personoplysninger i analyserne.

Det vil efter min opfattelse være foreneligt med reglerne i databeskyttelsesloven og databeskyttelsesforordningen, hvis SKI på de respektive kommuners vegne overlades og opbevarer en kopi af de modtagne eFaktura i deres original form med henblik på at danne datagrundlaget for analyserne, når de fejlagtige modtagne følsomme personoplysninger aldrig indgår i selve analyserne. Når analysegrundlaget er tilvejebragt og kopien af originalfaktura ikke længere er nødvendig, skal kopien slettes. Det samme gælder, når den originale faktura enten arkiveres eller kasseres.

Uanset, at eFaktura af hensyn til regnskabs- og bogføringsreglerne opbevares lovligt i deres oprindelig form i kommunernes primære fakturasystem, stiller og databeskyttelsesforordningens artikel 5 i den forbindelse efter min mening krav om, at kommunerne – dvs. i praksis SKI – må minimere omfanget af personoplysninger i indkøbsanalyse, der ikke er nødvendige for varetagelsen af formålet med indkøbsdatasamarbejdet og slette de øvrige personhenførbare oplysninger. Dette sker ved en minimering gennem filtrering af mulige personoplysninger i de pågældende fakturaer, så personoplysninger anonymiseres.

4.2 Videregivelse af oplysninger fra analyserne

SKI vil som databehandler alene handle på vegne af og efter instruks fra den dataansvarlige offentlige organisation. Hvis personoplysninger modtaget fra en offentlig organisation stilles til rådighed – direkte eller indirekte – for en andre (andre offentlige organisationer, KL, offentligheden m.v.) vil der foreligge en videregivelse, som kræver, at reglerne herfor i databeskyttelsesforordningen artikel 6-10 er opfyldt. Det samme gælder, hvis SKI anvender oplysningerne til egne formål.

SKI skal således handle inden for instruksen fra den respektive offentlige organisation.

Det er således en forudsætning for lovligheden af indkøbsanalyseplatformen, at SKI ikke i nogen sammenhæng eller under nogen omstændigheder videregiver de overladte personoplysninger fra eFaktura til andre ud over underdatabehandleren, herunder også de øvrige offentlige organisationer i samarbejdet enten direkte eller indirekte. Det betyder bl.a., at SKI ikke må anvende oplysninger i personhenførbar form til samkøring eller fælles analyse med øvrige offentlige organisationers oplysninger. Videregivelse og samkøring skal således alene ske i anonymiseret, ikke-personhenførbar form. Dette gælder dog ikke i forhold til oplysninger om leverandørnavne (hvor disse er personligt ejede virksomheder) samt kontaktoplysninger på medarbejdere hos disse i denne egenskab.

4.3 Databehandleraftale

Det er en forudsætning for dataansvarliges anvendelse af databehandlere, at der bliver indgået en databeskyttelsesforordningens artikel 28, stk. 3.

Kammeradvokaten har i 2020 efter anmodning fra SKI haft et udkast til databehandleraftale mellem SKI og de offentlige organisationer til gennemsyn. Kammeradvokaten har revideret aftalen, således at den efter vores overbevisning er i overensstemmelse med kravene i samt databeskyttelsesforordningens artikel 28. Hertil forudsættes det dog bl.a., at de nødvendige sikkerhedskrav implementeres og efterleves på baggrund af en risikovurdering efter databeskyttelsesforordningens artikel 32.

SKI kan benytte sig af underdatabehandlere, som f.eks. tilbyder en cloud-platform. Det forudsætter dog, at SKI overholder databeskyttelseslovgivningens krav, herunder at der indgås en underdatabehandleraftale samt sker efter en generel eller konkret skriftlig godkendelse af den offentlige organisation. Det er tillige et krav, at underdatabehandleren er underlagt samme beskyttelseskrav som SKI, og at SKI kontrollerer, at disse krav er overholdt. Det er også et krav, at der er foretaget en risikovurdering, og at der fastsættes passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som passer til risikovurderingen. Underdatabehandleren må ikke overføre personoplysninger til et tredjeland uden et overførselsgrundlag og forudgående godkendelse fra den dataansvarlige offentlige organisation.

Vi har i 2021 revideret skabelonen for databehandleraftale mellem SKI og de offentlige organisationer. Som beskrevet i afsnit 2.1 er det hensigten, at indkøbssamarbejdet fremadrettet også skal benyttes til at lave beregninger og analyser, der kan bidrage til klimavenlige og bæredygtige indkøb. Som følge heraf er formålet med behandlingen af personoplysninger blevet udvidet med henblik på at kunne rumme de ønskede ændringer.

4.4 Konsekvensanalyse vedrørende databeskyttelse

Kravet i databeskyttelsesforordningens artikel 35 om en konsekvensanalyse vedrørende databeskyttelse bliver udløst, når en behandlingsaktivitets potentielle konsekvenser for de registrerede overskrider en vis tærskel, nemlig når behandlingsaktiviteten sandsynligvis apriori indebærer en *høj* risiko for de registreredes rettigheder og frihedsrettigheder.

En konsekvensanalyse vedrørende databeskyttelse er en proces – herunder et sæt af konkrete produkter, som skabes ved processen – der har til formål at vurdere risici og fastlægge foranstaltninger til at afhjælpe disse risici. Analysen skal beskrive, hvilken behandling der foretages, vurdere behandlingens nødvendighed og proportionalitet og bidrage til at håndtere de risici, som behandlingen af personoplysninger medfører.

Det er den dataansvarliges pligt at foretage konsekvensanalysen vedrørende databeskyttelse, når behandlingen sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Som en del af indkøbsdatasamarbejdet stiller SKI et værktøj til rådighed for de dataansvarlige offentlige organisationer, der har til formål at foretage en tærskelanalyse og en konsekvensanalyse vedrørende databeskyttelse. SKI har i et vist omfang udfyldt værktøjet med relevante oplysninger. Det er den dataansvarliges forpligtelse at overholde databeskyttelsesforordningens artikel 35, og de offentlige organisationer opfordres derfor til at færdiggøre tærskelanalysen og en eventuel konsekvensanalyse vedrørende databeskyttelse.

Det er dog vores umiddelbare opfattelse, at de beskrevne behandlingsaktiviteter ikke medfører en sandsynligvis høj risiko for fysiske personers rettigheder og frihedsrettigheder, og dermed et krav om en konsekvensanalyse vedrørende databeskyttelse. Det skyldes navnlig, at 1) SKI's primære behandlingsaktivitet består i at anonymisere personoplysninger i fakturaer, 2) at følsomme personoplysninger ikke skal indgå i overladte fakturaoplysninger samt 3) at formålet med at optimere offentlige indkøb ikke har vidtrækkende konsekvenser for den registrerede.

Det er nødvendigt løbende at opdatere tærskelanalysen og en eventuel konsekvensanalyse vedrørende databeskyttelse for sikre, at analyserne er retvisende. Hvis behandlingsaktiviteten ændres (f.eks. inddragelse af nye kategorier af oplysninger), og risikobilledet forandrer sig, skal der således tages højde for disse ændringer. Det anbefales derfor, at analyserne periodevist gennemgås for at databeskyttelsesforordningens krav overholdes.

Værktøjet til at gennemføre en tærskelanalyse og en konsekvensanalyse vedrørende databeskyttelse er vedlagt som et bilag.

4.5 Kommunalfuldmagten

Det er vores vurdering, at det er foreneligt med kommunalfuldmagten, der giver kommunerne mulighed for at varetage opgaver og foretage visse økonomiske dispositioner af økonomisk karakter uden lovhjemmel, at indkøbssamarbejdet fra 2021 udvides til også at vedrøre beregninger og analyser, der kan bidrage til klimavenlige og bæredygtige indkøb. Det skyldes navnlig, at disse beregninger har accessoriske karakter i forhold til indkøbssamarbejdets oprindelige formål, samt at kommuner ifølge praksis i vidt omfang kan varetage klimahensyn.

5. KONKLUSION

Sammenfattende et det Kammeradvokatens vurdering, at de offentlige organisationer, der indgår i indkøbsdatasamarbejdet, kan overlade eFakturadata fra deres respektive primære fakturasystemer til SKI og dennes leverandører uden at bryde databeskyttelseslovgivningens almindelige behandlingsregler (databeskyttelseslovens §§ 5 - 11), hvis følgende forudsætninger er opfyldt:

- Offentlige organisationer overlader kun eFaktura med personoplysninger til SKI, for at SKI på den offentlige organisations vegne kan udføre analyser, udarbejde aggregerede rapporter, udføre statistik mv. med henblik på at give mulighed for, at offentlige organisationer selv – eller øvrige organisationer eller KL – kan effektivisere det offentliges indkøb, herunder arbejdet med at udvælge og udbyde relevante udbudsområder i form af såvel frivillige som forpligtende rammeaftaler, samt bidrage til klimavenlige og bæredygtige indkøb.

- Analyserne foretages alene på almindelige personoplysninger (navne, kontaktdata, CVR-numre), og fejlagtigt registrerede følsomme oplysninger frasorteres inden analyserne. SKI tager på vegne af de dataansvarlige nødvendige skridt til at minimere omfanget af unødvendige personoplysninger, som overlades og indirekte indgår i grundlaget for indkøbsanalyserne. Ved unødvendige forstås oplysninger, der er ikke nødvendige for varetagelsen af formålet med indkøbsdatasamarbejdet – f.eks. oplysninger om den borger, som det enkelte indkøb vedrører. Dette sker ved en minimering gennem filtrering af mulige personoplysninger i de pågældende fakturaer i videst muligt omfang.

- SKI kan som databehandler overlades en kopi af den originale fakturadata med henblik på at skabe analysegrundlaget, men når analysegrundlaget er tilvejebragt og kopien af originalfaktura ikke længere er nødvendig, skal kopien slettes. Det samme gælder, når den originale faktura enten arkiveres eller kasseres hos den respektive offentlige organisation, jf. databeskyttelsesforordningens artikel 5, stk. 2. SKI har oplyst, at oplysningerne kan slettes senest efter 5 år fra modtagelse af data. Offentlige organisationer skal indgå en gyldig databehandleraftale med SKI, og der indgås en underdatabehandleraftale med SKI's leverandør, hvoraf fremgår at SKI og underdatabehandleren i forhold til de overladte oplysninger alene handler efter instruks fra den pågældende offentlige organisation, og at de øvrige krav til databehandleraftaler er opfyldt. Sikkerhedskrav i databehandleraftale og underdatabehandleraftale skal bero på en risikovurdering efter databeskyttelsesforordningens artikel 32.

- SKI's brug af underdatabehandlere, som tilbyder en cloud-platform, overholder databeskyttelseslovgivningens krav og sker efter en generel eller konkret skriftlig godkendelse fra den offentlige organisation. Det indebærer, at SKI sikrer, at underdatabehandleren er underlagt samme beskyttelseskrav som SKI, og at SKI kontrollerer, at disse krav er overholdt. Det er som nævnt bl.a. en forudsætning for brugen af cloud-løsningen, at der er foretaget en risikovurdering, og at

der fastsættes passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som passer til risikovurderingen. Det er ligeledes et krav, at underdatabehandleren ikke overfører personoplysninger til et tredjeland uden et overførselsgrundlag og en forudgående godkendelse fra den dataansvarlige offentlige organisation.

- Medmindre den dataansvarlige offentlige organisation konkret instruerer SKI herom, videregiver eller overfører SKI ikke i nogen sammenhæng eller under nogen omstændigheder de overladte personoplysninger fra fakturadata til andre (KL, øvrige offentlige organisationer mv.) ud over underdatabehandleren i overensstemmelse med aftalen, herunder også de øvrige offentlige organisationer i samarbejdet enten direkte eller indirekte. SKI anvender i den forbindelse heller ikke oplysninger i personhenførbar form til samkøring eller fælles analyse med øvrige offentlige organisationers oplysninger. Videregivelse og samkøring kan således alene ske i anonymiseret, ikke-personhenførbar form. Disse regler gælder dog ikke i forhold til oplysninger om leverandørnavne (hvor disse er personligt ejede virksomheder) samt kontaktoplysninger på medarbejdere hos disse i denne egenskab. De dataansvarlige offentlige organisationer skal sikre regeloverholdelse i eget ansvarsområde ift. analyserne. Det gælder f.eks. ift. underretning af de registrerede (artikel 13 og 14) samt pligten til at overveje gennemførelse af en konsekvensanalyse for databeskyttelse (DPIA).

København, den 20. februar 2021
Kammeradvokaten

v/ Jakob Kamby
– Partner, Advokat (L)