

Bilag 1 til Tilmeldingsskemaet til Deltagelse i indkøbsdatasamarbejdet:

Databehandleraftale

Dags dato er indgået nedenstående aftale mellem

_____	<i>[Indsæt kommunens navn]</i>
_____	<i>[Indsæt kommunens CVR-nr.]</i>
_____	<i>[Indsæt adresse]</i>
_____	<i>[Indsæt postnr. og by]</i>

(Herefter benævnt den Dataansvarlige)

og

Staten og Kommunernes Indkøbsservice A/S

CVR nr. 17472437

H. C. Hansens Gade 4

2300 København S

(Herefter benævnt Databehandleren)

om

Drift af et offentligt indkøbsdatasamarbejde
samt udarbejdelse af analyser på baggrund heraf

Indholdsfortegnelse

1. Definitioner.....	3
2. Baggrund.....	3
3. Formål.....	4
4. Personoplysninger omfattet af Databehandleraftalen	5
5. Behandling af personoplysninger	5
6. Informationssikkerhed og databeskyttelse	8
7. Aftaler med en anden databehandler (underdatabehandler)	9
8. Overførsel af oplysninger	11
9. Tavshedspligt	11
10. Ændringer i Databehandleraftalen	12
11. Varighed og ophør af Databehandleraftalen	12
12. Forrang	13
13. Underskrifter	13

[Bilag A til Databehandleraftalen om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles ved Databehandleren](#)

1. Generelle sikkerhedsbestemmelser	14
2. Inddatamateriale som indeholder personoplysninger	15
3. Autorisation og adgangskontrol	15
4. Kontrol med afviste adgangsforsøg.....	16
5. Uddatamateriale som indeholder personoplysninger	16
6. Eksterne kommunikationsforbindelser	16
7. Logning	16

1. Definitioner

Nedenstående definitioner anvendes i Databehandleraftalen.

Ved den Dataansvarlige forstås _____ *[Indsæt kommunens navn]*.

Ved Databehandleren forstås Staten og Kommunernes Indkøbsservice A/S.

Ved Part eller Parterne forstås henholdsvis den Dataansvarlige og/eller Databehandleren.

Ved Databehandleraftalen forstås denne aftale.

Ved Tilmeldingsskemaet forstås Parternes tilmeldingsskema til deltagelse i indkøbssamarbejdet.

Ved databeskyttelsesloven forstås lov nr. 502 af 23. maj 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Ved databeskyttelsesforordningen forstås 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).

2. Baggrund

I regeringens aftale med KL om kommunernes økonomi for 2015 blev parterne enige om, at et vigtigt fokusområde for det offentlige indkøb fremover ville 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.

I kølvandet herpå gennemførte Staten og Kommunernes Indkøbsservice A/S (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 en analyserapport, der sammenlignede den pågældende kommunes indkøb med gennemsnittet af alle deltagende kommuners indkøb.

På grundlag af erfaringerne med indkøbsdataprojektet blev det besluttet at overgå til et egentligt fælleskommunalt indkøbsdatasamarbejde. SKI etablerede en indkøbsdatamodel på baggrund af kommunernes elektroniske fakturadata for kalenderårene 2014, 2015 og 2016. Efterfølgende blev indkøbsdatamodellen udbygget med de efterfølgende års kommunale fakturadata. Således indeholdt indkøbsdatasamarbejdet ved udgangen af 2020 fakturadata for 93 deltagende kommuner for årene 2014-2019.

Med udgangspunkt i data fra det fælleskommunale indkøbssamarbejde blev der udarbejdet en række rapporter til de deltagende kommuner, så hver enkelt kommune kunne sammenligne sin egen indkøbsprofil med de andre deltagende kommuners. Datamodellen har gjort det muligt at se udviklingen af den enkelte kommunes indkøb over tid og sammenholde denne udvikling med andre

kommuners udvikling samme periode. Analyseresultaterne videreformidledes som udgangspunkt i anonymiseret form, bortset fra de analyser, der var udarbejdet til en konkret kommunes eget brug.

Professionshøjskolerne har på samme måde som kommunerne leveret deres fakturadata for årene 2016 og 2017, og på baggrund af dette er der for dem udarbejdet individuelle rapporter. Ligesom der er udarbejdet sammenlignende analyser på tværs af professionshøjskolerne.

Derudover har SKI kunnet anvende data til analyser med henblik på at effektivisere indkøbet for kommunerne, herunder arbejdet med at udvælge og udbyde relevante udbudsområder i form af såvel frivillige som forpligtende rammeaftaler.

SKI's målsætning er at videreføre indkøbsdatasamarbejdet, så såvel kommuner, professionshøjskoler som andre sektorer og organisationer i den offentlige sektor har mulighed for at aflevere fakturadata til SKI, hvorefter SKI vil kunne udarbejde individuelle rapporter på baggrund af de afleverede data samt at anvende data for grundlag til effektivisering af indkøb i den offentlige sektor.

Indkøbssamarbejdet udvides i 2021 med henblik på at bidrage til at fremme klimadagsordenen og bæredygtige indkøb. Det er hensigten, at der skal foretages analyser og beregninger, der skal bidrage til grønne og klimavenlige indkøb. Der foretages bl.a. klimaberegninger om udledningen af CO₂ i forbindelse med offentlige indkøb, og disse beregninger rapporteres løbende for at følge udviklingen, herunder også til KL. Der foretages også 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.

3. Formål

Formålet med behandlingen af personoplysninger er overordnet set at optimere og effektivisere offentlige indkøb, samt at sikre klimavenlige og bæredygtige indkøb, ved bl.a. at udarbejde analyser på baggrund af indkøbsdatasamarbejdet.

Databehandleren vil foretage behandling af elektroniske fakturadata, der i begrænset omfang kan indeholde personoplysninger, på vegne af den Dataansvarlige til opfyldelse af indkøbssamarbejdets målsætninger som beskrevet i afsnit 2. De offentlige organisationer overlader i forbindelse med Databehandleraftalen personoplysninger til Databehandleren for at Databehandleren kan udføre analyser mv. af elektroniske fakturadata. Analyserne kan f.eks. udforme sig i rapporter og statistikker, der bl.a. kan bruges til at vælge den mest optimale udbudsform.

Som den første aktive behandlingsaktivitet anonymiserer Databehandleren personoplysninger i den overleverede fakturadata via en automatiseret proces. Den automatiske anonymiseringsproces sletter og erstatter personoplysninger med en generel kode afhængigt af hvilken type personoplysninger, der bliver slettet.

Selv den bedste automatiske anonymiseringsproces vil ikke kunne forhindre at enkelte personoplysninger stadig vil forefindes i det i øvrigt anonymiserede datasæt. Databehandleren videregiver derfor ikke de overladte personoplysninger fra elektroniske fakturaer til andre, herunder øvrige offentlige organisationer, ligesom Databehandleren ikke anvender oplysninger i personhenførbare

form til samkøring eller fælles analyse med øvrige organisationers oplysninger. Databehandleren har desuden indført en procedure, der manuelt sikrer at data, der ikke automatisk er blevet anonymiseret, efterfølgende bliver anonymiseret. I de tilfælde, hvor den dataansvarlige efterspørger organisationens egne data, foretages der ikke manuel kontrol af persondata. Data sendes til den af organisationen udpegede kontaktperson vedrørende indkøbsdatasamarbejdet.

I udgangspunktet sker videregivelse og samkøring af indkøbsdata således kun i anonymiseret, ikke-personhenførbare form. Dette gælder dog ikke i forhold til leverandørnavne samt kontaktoplysninger på medarbejdere hos disse. Hvis en organisations data indeholder personhenførbare data, vil Databehandleren dog ikke vise eller dele de pågældende data med andre udenfor den pågældende organisation. Heller ikke selvom organisationen har givet en instruks om det. I disse tilfælde vil Databehandleren sende data til den pågældende organisation, der så selv må påtage sig ansvaret med at sende den personhenførbare data videre til tredjepart.

Databehandleraftalen har på den baggrund til formål at sikre overholdelse af den til enhver tid gældende databeskyttelseslovgivning i Danmark, herunder sikre tilvejebringelse af passende garantier med hensyn til beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med, at Databehandleren gives adgang til at behandle de i Databehandleraftalen nævnte personoplysninger på vegne af Dataansvarlig.

4. Personoplysninger omfattet af Databehandleraftalen

Databehandleraftalen omfatter følgende typer af personoplysninger:

- Navn, fødselsdato og CPR-numre,
- Oplysninger om stilling, e-mail, adresser og øvrige kontaktoplysninger,
- Oplysninger om ansættelsesforhold,
- Enkeltstående tilfældighedsprægede oplysninger om de berørte borgere mv., som er genstand for leverancerne. Det kan undtagelsesvis være oplysninger, der indirekte eller direkte omfatter følsomme personoplysninger efter databeskyttelsesforordningens artikel 9 i form af helbredsmæssige oplysninger og personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. Disse behandles alene som led i bortfiltrering hos Databehandleren ved dannelse af analysegrundlaget ud fra fakturaerne.

5. Behandling af personoplysninger

5.1. Behandlingsformer og personkreds

Omfanget af de opgaver, som Databehandleren skal levere og understøtte, betyder, at der vil ske mange forskellige former for behandling af personoplysninger, herunder indsamling, registrering, opbevaring, ændring, søgning, analysering, filtrering, aktiv brug og sletning.

Kredsen af de registrerede personer, som personoplysningerne vedrører, udgør fortrinsvis ansatte hos aftalepartnere, ansatte i de offentlige organisationer, samt i undtagelsestilfælde borgere, som har været genstand for leverancerne, hvis disse oplysninger indgår i fakturaerne.

5.2. Generelle krav til databehandlerens behandlinger

Databehandleren handler alene efter dokumenteret instruks fra den Dataansvarlige.

Databehandleren skal sikre, at de overladte personoplysninger ikke benyttes til andre formål eller behandles på anden måde, end hvad der fremgår af den Dataansvarliges instruks, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, jf. dog punkt 8.

Databehandleren skal behandle personoplysningerne i overensstemmelse med den til enhver tid gældende lovgivning eller anden regulering om personoplysninger eller bestemmelser fastsat i henhold til lov eller anden regulering, herunder men ikke begrænset til databeskyttelsesloven og databeskyttelsesforordningen og bestemmelser fastsat i medfør heraf. Såfremt Databehandleren skønner, at en instruktion er i strid med førnævnte lovgivning, skal Databehandleren omgående orientere den Dataansvarlige herom.

Databehandleren må ikke behandle personoplysningerne til andre formål end dem, der følger af instruks, medmindre Databehandleren er forpligtet hertil efter EU-retten eller lovgivningen i en medlemsstat. I givet fald skal Databehandleren underrette den Dataansvarlige om denne juridiske forpligtelse, forinden behandlingen påbegyndes. Dette gælder dog ikke, såfremt den pågældende lovgivning på baggrund af væsentlige offentlige interesser forbyder en sådan underretning.

5.3. Instruks vedrørende behandling af personoplysninger

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker ved, at Databehandleren udfører følgende:

- Sletter og anonymiserer personoplysninger, der indgår i fakturadata overdraget fra den Dataansvarlige.
- Foretager øvrige behandlingsaktiviteter med henblik på at opfylde sine forpligtelser som anført i Tilmeldingsskemaet, Databehandleraftalen og eventuelle øvrige aftaler med den Dataansvarlige.

5.4 Krav om fortegnelse

Databehandleren skal føre en fortegnelse over alle kategorier af behandlinger, der foretages på vegne af den Dataansvarlige. Fortegnelsen skal indeholde følgende:

- Navn på og kontaktoplysninger for Databehandleren, eventuelle underleverandører, den Dataansvarlige samt databeskyttelsesrådgiveren.
- Kategorierne af de behandlinger Databehandleren eller eventuelle underleverandører foretager for den Dataansvarlige.
- Eventuelle overførsler af personoplysninger til et tredjeland eller en international organisation, herunder angivelse af dette tredjeland eller denne internationale organisation,

samt angivelse af hjemlen for overførslen til tredjelandet eller den internationale organisation.

- En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.

Fortegnelsen skal foreligge skriftligt og elektronisk. Databehandleren skal efter anmodning fra den Dataansvarlige til enhver tid stille fortegnelsen til rådighed for den Dataansvarlige eller Datatilsynet.

5.5. Drøftelser med Datatilsynet

Databehandleren skal deltage i eventuelle drøftelser med Datatilsynet og indarbejde eventuelle anbefalinger og/eller påbud mv. fra tilsynet vedrørende behandling af personoplysninger. Databehandleren skal straks orientere den Dataansvarlige, såfremt Datatilsynet retter henvendelse til Databehandleren vedrørende behandling af personoplysninger omfattet af tilmeldingen efter Tilmeldingsskemaet.

5.6. Særlige pligter vedrørende henvendelser fra tredjemand

Databehandleren forpligter sig til straks at orientere den Dataansvarlige om:

- Enhver anmodning om videregivelse af personoplysninger omfattet af Databehandleraftalen fra en myndighed, medmindre orienteringen af den Dataansvarlige er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning.
- Enhver anmodning om indsigt modtaget direkte fra den registrerede eller fra tredjemand, medmindre en sådan handle måde er blevet godkendt af den Dataansvarlige.

5.7. Særlige forpligtelser til at bistå og orientere den Dataansvarlige

Databehandleren skal på den Dataansvarliges anmodning stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i Databehandleraftalen samt gældende databeskyttelsesret, til rådighed for den Dataansvarlige eller dennes repræsentant.

Databehandleren skal straks assistere den Dataansvarlige med håndtering af enhver henvendelse fra en registreret, herunder anmodning om indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af Databehandleren.

Databehandleren skal herudover på den Dataansvarliges anmodning assistere den Dataansvarlige med at overholde øvrige forpligtelser, der måtte påhvile den Dataansvarlige efter den til enhver tid gældende databeskyttelseslovgivning, hvor Databehandlerens assistance er forudsat, samt hvor Databehandlerens assistance er nødvendig for, at den Dataansvarlige kan overholde sine forpligtelser. Databehandleren skal som led heri bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af databeskyttelsesforordningens artikel 32-36.

5.8. Øvrige pligter

Parterne forpligter sig til i hele aftaleperioden at indhente og opretholde de registreringer og tilladelser, som Parten er forpligtet til at indhente og opretholde i overensstemmelse med den til enhver tid gældende lovgivning.

6. Informationssikkerhed og databeskyttelse

6.1. Krav til informationssikkerhed og databeskyttelse

Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med den til enhver tid gældende lovgivning, herunder men ikke begrænset til databeskyttelsesloven og databeskyttelsesforordningen. Dette gælder også, hvis behandlingen af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser.

Fastsættelsen af fornødne tekniske og organisatoriske sikkerhedsforanstaltninger skal ske under iagttagelse af bl.a.:

- a) De i Bilag A fastsatte krav til sikkerhed,
- b) Den Dataansvarliges anvisninger på baggrund af den til enhver tid gældende konsekvensanalyse vedrørende databeskyttelse efter databeskyttelsesforordningens artikel 35 og
- c) Databehandleraftalen.

Hvis Databehandleren etablerer sig i en anden EU-medlemsstat, skal de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den EU-medlemsstat, hvor Databehandleren etablerer sig, derudover gælde for Databehandleren. Hvis Databehandleren etablerer sig i en anden EU-medlemsstat, skal Databehandleren således overholde såvel sikkerhedskrav omfattet af gældende lovgivning i Danmark som sikkerhedskrav i Databehandlerens hjemland.

Databehandleren har pligt til på eget initiativ at søge en eventuel tvivl om sikkerhedskravene og opfyldelsen heraf afklaret, herunder via den Dataansvarlige.

Databehandleren forpligter sig til at gøre sig bekendt med den Dataansvarliges it-sikkerhedsregulativ, it-sikkerhedspolitik og følge de uddybende it-sikkerhedsregler, hvis den Dataansvarlige orienterer Databehandleren om disse forhold. Den Dataansvarlige er samtidigt forpligtet til at holde Databehandleren orienteret i tilfælde af ændringer, ligeledes påhviler det Databehandleren at underrette eventuelle underdatabehandlere.

Databehandleren skal i øvrigt overholde kravene til databehandlere, og den Dataansvarlige skal overholde kravene til dataansvarlige i overensstemmelse med den til enhver tid gældende lovgivning. Databehandleren skal således blandt andet overholde bestemmelserne om behandlingssikkerhed i databeskyttelsesforordningen, herunder iværksætte foranstaltninger som kræves i henhold til artikel 32, samt databeskyttelsesloven.

6.2. Kontrol med informationssikkerhed og databeskyttelse

Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige informationer til, at denne kan påse og dokumentere, at Databehandleren har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger. Herved bl.a. oplysninger om hvor den Dataansvarliges personoplysninger befinder sig, samt fysisk adgang til denne såfremt påkrævet af den Dataansvarlige.

Databehandleren (og enhver eventuel underleverandør) skal hvert år vederlagsfrit foranledige, at en uafhængig tredjepart afgiver en erklæring til den Dataansvarlige om overholdelse af kravene i Databehandleraftalen, f.eks. en ekstern revisorerklæring efter revisionsstandarden ISAE 3000. Erklæringen skal omfatte en vurdering af Databehandlerens efterlevelse af kravene fastlagt i denne aftale samt de krav, der i øvrigt måtte følge af den til enhver tid gældende databeskyttelsesretlige regulering i Danmark. Erklæringen stilles årligt til rådighed for de offentlige organisationer.

Den Dataansvarlige eller dennes repræsentant har ret til at foretage inspektioner af Databehandleren og underdatabehandleres fysiske faciliteter og systemer, hvor der behandles personoplysninger i medfør af Databehandleraftalen. Den Dataansvarlige skal give den Dataansvarlige et passende varsel på mindst 7 arbejdsdage før inspektioner foretages.

Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den Dataansvarlige og Databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.

6.3. Informationssikkerhedsbrud og brud på persondatasikkerheden

I tilfælde af informationssikkerhedsbrud og brud på persondatasikkerheden, skal Databehandleren straks efter Databehandlerens kendskab hertil orientere den Dataansvarlige herom. Databehandleren skal herefter uden unødigt forsinkelse, dog senest 24 timer efter Databehandlerens kendskab til bruddet, rapportere til den Dataansvarlige. En sådan rapportering skal mindst:

- 1) beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- 2) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- 3) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- 4) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

7. Aftaler med en anden databehandler (underdatabehandler)

7.1. Krav vedrørende aftaler med underdatabehandlere

Databehandleren har den Dataansvarliges generelle forudgående godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre underdatabehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden for 1 måned. En sådan underretning skal gives til den Dataansvarlige minimum 1 måned, før ændringen skal træde i kraft.

Databehandleren skal udarbejde en skriftlig underdatabehandleraftale med en underdatabehandler, såfremt en sådan anvendes. I sin aftale med underdatabehandleren skal Databehandleren sikre

sig, at underdatabehandleren som minimum accepterer de samme databeskyttelsesforpligtelser, som Databehandleren har påtaget sig ved Databehandleraftalen, for så vidt angår den behandling af den Dataansvarliges personoplysninger, der varetages af underdatabehandleren. Den Dataansvarlige skal efter anmodning have adgang til at se aftalen.

Databehandleren indestår for lovligheden af underdatabehandlerens behandling af personoplysninger. Hvis en underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Det forhold, at den Dataansvarlige har meddelt samtykke til Databehandlerens aftaleindgåelse med en underdatabehandler, er uden betydning for Databehandlerens pligt til at efterleve Databehandleraftalen. Ved ophør af en aftale med en underdatabehandler om behandling af personoplysninger omfattet af Databehandleraftalen, skal Databehandleren give den Dataansvarlige meddelelse herom.

Omkostninger forbundet med etablering af aftaleforholdet til en underdatabehandler, herunder omkostninger til udarbejdelse af underdatabehandleraftaler, afholdes af Databehandleren og er således den Dataansvarlige uvedkommende.

7.2. Valg af underdatabehandler

Databehandleren har med den Dataansvarliges samtykke valgt at anvende "Microsofts Azure-platform" til at behandle de elektroniske fakturaer. Endvidere er der indgået en aftale med konsulentfirmaet "Deloitte", der vil bidrage med arbejdet med at kategorisere de indkomne fakturadata i forbindelse med indkøbsdatasamarbejdet. Yderligere er der indgået en aftale med udvikleren "Struct A/S" samt hostingselskabet "Sentia", som omhandler upload og anonymisering af elektroniske fakturaer. Endelig anvender SKI underleverandøren "ProAct" som leverandør af backupservice.

7.3. Beskrivelse af rollefordeling

De offentlige organisationer afleverer elektroniske fakturadata til Databehandleren. Databehandleren står selv for behandlingen af data. Databehandleren beholder en kopi af de ubehandlede elektroniske fakturadata, så organisationerne ikke behøver at genfremsende dem ved en eventuel efterfølgende senere nykategorisering af data. Kopien vil alene kunne tages i anvendelse ved ny-/genkategorisering af de elektroniske fakturadata, samt eventuelt hvis organisationen ønsker en kopi af deres egne data retur fra Databehandleren.

Databehandleren foretager en behandling af den elektroniske fakturadata, hvorved det samlede indkøb kategoriseres til brug for indkøbsdatamodellen. Først tilstræbes imidlertid en rensning af data således, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger.

Databehandleren opbevarer den behandlede og anonymiserede elektroniske fakturadata i en cloud-baseret løsning, Microsoft Azure, der kun kan tilgås af de til projektet tilknyttede betroede medarbejdere og anvendes til behandlingsformål.

Hverken de oprindelige elektroniske fakturadata eller de rensede data udleveres til tredjepart. De analyser og rapporter, der udarbejdes på baggrund af data, videreformidles som udgangspunkt i

anonymiseret form, bortset fra de analyser der udarbejdes til en konkret organisations eget brug. Dog har KL mulighed for at bestille kommunespecifikke oplysninger til brug for KL's interessevaretagelse og opfølgning på den fælleskommunale indkøbsstrategi, herunder anvendelse af kommunespecifikke nøgletal i forbindelse med KL's dialogmøder med kommunerne. Tilsvarende har staten/Moderniseringsstyrelsen alene adgang til statslige organisationers oplysninger til brug for statens opfølgning på indkøbsområdet.

Leverandørers enhedspriser vil alene fremgå af analyser og rapporter i fuldt anonymiseret form, bortset fra de tilfælde hvor analyserne er afgrænset til en konkret offentlig organisation køb hos egne leverandører.

8. Overførsel af oplysninger

Oplysningerne samt analyser og rapporter på baggrund heraf må alene videregives til tredjemand i anonymiseret ikke-personhenførbart form, medmindre dette følger af gældende lovgivning eller efter instruks fra den Dataansvarlige. Dog har KL adgang til kommunespecifikke oplysninger til brug for KL's interessevaretagelse og opfølgning på den fælleskommunale indkøbsstrategi, herunder anvendelse af kommunespecifikke nøgletal i forbindelse med KL's dialogmøder med kommunerne. Tilsvarende har staten/Moderniseringsstyrelsen adgang til statslige organisationers oplysninger til brug for statens opfølgning på indkøbsområdet. Leverandørers enhedspriser vil alene fremgå af analyser og rapporter i fuldt anonymiseret form, bortset fra de tilfælde hvor analyserne er afgrænset til en konkret organisations køb hos egne leverandører. Eventuelle ændringer i forhold til dette afsnit, se punkt 10.

Databehandleren må ikke overføre eller tillade overførsel af personoplysninger til tredjemand, dvs. lande uden for EU og det Europæiske Økonomiske Samarbejdsområde, uden den Dataansvarliges forudgående skriftlige godkendelse.

Såfremt der skal ske en sådan overførsel, påhviler det Databehandleren at sikre det fornødne overførselsgrundlag, f.eks. brug af EU-Kommissionen godkendte standardbestemmelser om databeskyttelse. Overførselsgrundlaget skal forelægges den Dataansvarlige forud for den Dataansvarliges specifikke godkendelse af overførslen. Databehandleren afholder omkostninger forbundet med etablering af det fornødne overførselsgrundlag.

9. Tavshedspligt

Databehandleren skal holde personoplysningerne fortrolige og er således alene berettiget til at anvende personoplysningerne som led i opfyldelsen af sine forpligtelser i henhold til Tilmeldingsskemaet, herunder Databehandleraftalen.

Databehandleren skal sikre, at de medarbejdere og eventuelle andre databehandlere, der er autoriseret til at behandle de pågældende personoplysninger, har forpligtet sig til tavshedspligt eller underlagt en passende lovbestemt tavshedspligt for så vidt angår de personoplysninger, som de får kendskab til i forbindelse med opfyldelse af formålene med Tilmeldingsskemaet.

10. Ændringer i Databehandleraftalen

Parterne kan til enhver tid aftale at ændre Databehandleraftalen. Ændringer skal være skriftlige.

Den Dataansvarlige er berettiget til med et varsel på 30 dage at ændre i Databehandleraftalen uden forudgående accept fra Databehandleren, såfremt dette skyldes ændringer i gældende databeskyttelsesret eller tilhørende praksis. Databehandleren skal ved sådanne ændringer uden ugrundet ophold sikre, at eventuelle underdatabehandlere tillige forpligtes af ændringerne.

Hvis den Dataansvarlige ønsker at fravige nogle af bestemmelserne i Databehandleraftalen, skal det ske efter skriftlig aftale med Databehandleren.

11. Varighed og ophør af Databehandleraftalen

Databehandleraftalen træder i kraft ved Parternes underskrift og er gældende så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige eller frem til tilmeldingens ophør, alt efter hvilket tidspunkt, der indtræder senest.

I tilfælde af ophør af Databehandleraftalen, uanset det juridiske grundlag herfor, skal Databehandleren yde de fornødne overgangsydelser til den Dataansvarlige. De fornødne overgangsydelser omfatter bl.a., at Databehandleren skal handle efter instruks fra den Dataansvarlige, herunder instruks om straks at tilbagelevere eller slette samtlige personoplysninger, uanset opbevaringsmedie.

Databehandleren er forpligtet til loyalt og hurtigst muligt at medvirke til, at udførelse af ydelserne overgår til en anden databehandler eller tilbageføres til den Dataansvarlige. Databehandleren skal straks efter anmodning fra den Dataansvarlige ændre, overføre eller slette personoplysninger, som Databehandleren behandler for den Dataansvarlige, medmindre gældende lovgivning foreskriver opbevaring af personoplysningerne.

Hvis den Dataansvarlige bliver bekendt med, at Databehandleren ikke behandler personoplysninger som beskrevet i Databehandleraftalen eller behandler oplysninger i strid med sine forpligtelser efter databeskyttelsesloven, kan den Dataansvarlige pålægge Databehandleren at stoppe den videre behandling af oplysningerne med øjeblikkelig virkning.

Databehandleraftalen kan til enhver tid opsiges skriftligt af såvel den Dataansvarlige som Databehandleren. I så fald skal Databehandleren uigenkaldeligt slette den Dataansvarliges elektroniske fakturadata inden for en periode på 30 dage samt sende den Dataansvarlige en skriftlig bekræftelse på, at dette er foregået.

Opsiges Databehandleraftalen ikke, sletter Databehandleren den Dataansvarliges elektroniske fakturadata senest 5 år efter modtagelsen af den Dataansvarliges data. Sletningen omfatter ikke anonymiserede personoplysninger.

Tavshedspligtsbestemmelserne tilhørende Databehandleraftalen ophører ikke ved Databehandleraftalens ophør.

12. Forrang

I tilfælde af uoverensstemmelse mellem bestemmelserne i Databehandleraftalen og bestemmelserne i andre skriftlige eller mundtlige aftaler indgået mellem Parterne – herunder ved den Dataansvarliges tilmelding via Tilmeldingsskemaet – skal bestemmelserne i Databehandleraftalen have forrang, medmindre andet direkte fremgår i en allonge tilknyttet Databehandleraftalen.

13. Underskrifter

Aftalen underskrives, og Parterne opbevarer hver en kopi af aftalen.

Dato 12. april 2021



For Databehandleren
økonomidirektør Jonas Klinting
Staten og Kommunernes Indkøbsservice A/S

For den Dataansvarlige

Bilag A til Databehandleraftalen

om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles ved Databehandleren

1. Generelle sikkerhedsbestemmelser

Databehandleren skal fastsætte interne bestemmelser om sikkerhedsforanstaltninger til uddybning af de krav, der fremgår af dette bilag. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Derudover skal der fastsættes retningslinjer for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for Databehandleren.

Databehandleren skal sikre, at der stilles tilsvarende sikkerhedskrav til underdatabehandleren, som Databehandleren selv er underlagt fra den dataansvarlige. Databehandleren sikrer således, at Microsoft i forbindelse med behandlingen af personoplysninger i Azure-plattformen som minimum lever op til samme sikkerhedskrav, som Databehandleren selv er underlagt ("back to back").

De interne bestemmelser skal gennemgås mindst én gang årligt med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold hos Databehandleren.

Databehandleren skal fastsætte særlige retningslinjer for behandling af personoplysninger omfattet af Databehandleraftalen, der finder sted på en arbejdsplads uden for Databehandlerens lokalteter (fjernarbejdsplads), således at det sikres, at de fornødne tekniske og organisatoriske foranstaltninger iagttages i relation til denne behandling af oplysningerne.

Såfremt behandlingen af personoplysninger hos Databehandleren sker helt eller delvist ved anvendelse af hjemmearbejdspladser, skal Databehandleren fastsætte retningslinjer for medarbejdernes behandling af personoplysninger ved anvendelse af hjemmearbejdspladser.

I forbindelse med salg, genbrug og kassation af anvendt udstyr, herunder dataudstyr og datamedier, der indeholder personoplysninger omfattet af Databehandleraftalen, og som har været anvendt til Databehandleraftalens opfyldelse, skal Databehandleren træffe passende tekniske og organisatoriske foranstaltninger for at sikre, at disse oplysninger hverken hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt træffe foranstaltninger mod, at disse personoplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de databeskyttelsesretlige regler og/eller Databehandleraftalen.

I forbindelse med reparation og service af udstyr, der anvendes til opfyldelse af formålene med behandlingen af oplysninger omfattet af Databehandleraftalen, og som indeholder oplysninger omfattet af Databehandleraftalen, skal Databehandleren træffe de fornødne foranstaltninger for at sikre, at oplysningerne hverken hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt

foranstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de databeskyttelsesretlige regler eller Databehandleraftalen.

2. Inddatamateriale som indeholder personoplysninger

Databehandleren skal sikre, at inddatamateriale indeholdende personoplysninger omfattet af Databehandleraftalen kun behandles af personer, som er beskæftiget med inddatering i forbindelse med opfyldelse af formålene med behandlingen af oplysninger omfattet af Databehandleraftalen.

Inddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til formålene med behandlingen af oplysninger omfattet af Databehandleraftalen, eller til kontrol med de inddaterede personoplysninger, dog senest efter en af den Dataansvarlige nærmere fastsat frist.

Ved tilintetgørelse af inddatamaterialet træffer Databehandleren de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

3. Autorisation og adgangskontrol

Databehandleren skal sikre, at kun de personer, som autoriseres hertil, må have adgang til personoplysninger, der behandles efter Databehandleraftalen.

Databehandleren skal sikre, at Databehandlerens medarbejdere autoriseres og tildeles rettigheder i overensstemmelse med Databehandlerens interne retningslinjer efter Bilag A, punkt 1, hvori det er beskrevet, i hvilket omfang Databehandlerens medarbejdere må forespørge på, inddatere eller slette oplysninger omfattet af Databehandleraftalen.

Databehandleren må kun autorisere personer, der er beskæftiget med de formål, hvortil personoplysninger behandles i forbindelse med Databehandleraftalens opfyldelse. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har specifikt behov for i forbindelse med Tilmeldingsskemaets og Databehandleraftalens opfyldelse.

Databehandleren må endvidere autorisere brugere, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver i forbindelse med opfyldelse af formålene med behandlingen af personoplysningerne.

Databehandleren skal som minimum træffe de foranstaltninger, der er beskrevet i Databehandlerens interne retningslinjer efter Bilag A, punkt 1, for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de oplysninger og anvendelser, som de er autoriserede til i forbindelse med Databehandleraftalens opfyldelse.

Databehandleren skal løbende sikre og dokumentere, at de autoriserede brugere fortsat opfylder betingelserne i dette punkt, og Databehandlerens interne retningslinjer efter Bilag A, punkt 1. Kontrol heraf skal foretages mindst én gang hvert halve år.

4. Kontrol med afviste adgangsforsøg

Databehandleren skal foretage registrering af og dokumentere alle afviste adgangsforsøg. Hvis der inden for en af den Dataansvarlig bestemt periode er registreret et af den Dataansvarlige bestemt antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg i en tidsperiode. Databehandleren skal løbende afrapportere herom til Den Dataansvarlige.

5. Uddatamateriale som indeholder personoplysninger

Databehandleren skal sikre, at uddatamateriale der indeholder personoplysninger omfattet af Databehandleraftalen kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af de givne oplysninger foretages, herunder personer som er beskæftiget med at tilvejebringe uddatamateriale.

Uddatamateriale må dog ligeledes anvendes af personer, som er beskæftiget med revision eller drifts- og systemtekniske opgaver i det pågældende system.

Databehandleren skal opbevare uddatamateriale på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de oplysninger, som er indeholdt heri.

Databehandleren skal tilintetgøre uddatamateriale med personoplysninger, når dette ikke længere skal anvendes i forbindelse med Databehandleraftalen og senest efter 5 år fra modtagelsen i overensstemmelse med Databehandleraftalens afsnit 11. Derudover skal uddatamateriale om enkeltpersoner kunne slettes efter anmodning fra Den Dataansvarlige.

I forbindelse med tilintetgørelse af uddatamateriale skal Databehandleren træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at dette uddatamateriale misbruges eller kommer til uvedkommendes kendskab.

6. Eksterne kommunikationsforbindelser

Databehandleren må kun anvende eksterne kommunikationsforbindelser til behandling af oplysninger indeholdende personhenførbare data omfattet af Databehandleraftalen i forbindelse med Tilmeldingsskemaet og Databehandleraftalens opfyldelse, hvis der træffes særlige foranstaltninger, såsom kryptering, for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

7. Logning

Databehandleren skal foretage logning af alle anvendelser af personoplysninger omfattet af Databehandleraftalen.

Logningen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Logningen skal opbevares i mindst 6 måneder, medmindre andet er aftalt med Den Dataansvarlige, hvorefter den skal slettes.

Databehandleren skal på Den Dataansvarliges anmodning uden unødigt ophold udlevere log-data til Den Dataansvarlige eller til en tilsynsmyndighed.