KOMMENTARER TIL
SKABELON FOR DATABEHANDLERAFTALER
MELLEM KOMMUNER OG IT-LEVERANDØRER
– version 2.1 af 24. januar 2019

Indhold

1. Indledning og baggrund

KL og KOMBITs skabelon for databehandleraftaler mellem kommuner og it-leverandører er udarbejdet med input fra kommuner. Et udkast til skabelonen var i offentlig høring i november - december 2016, og der kom i den forbindelse en lang række kommentarer fra såvel kommuner som leverandører – kommentarer, som i videst muligt omfang er indarbejdet i skabelonen. Første version af skabelonen blev publiceret i april 2017 og Datatilsynet vurderede, at skabelonen opfyldte kravene i persondataloven og databeskyttelsesforordningen.

Version 2.0 af skabelonen er blevet justeret sådan, at bestemmelser, der vedrører lovgivning, som ikke vil være gældende efter 25. maj 2018 er fjernet. Desuden er skabelonen konsekvensrettet i forhold til, at Databeskyttelsesforordningens regler i stedet finder anvendelse pr. 25. maj 2018. Efter ønske fra kommuner og leverandører er der enkelte steder genbrugt ordlyd fra forordningen for at sikre genkendelighed. Kommunerne skal således ikke ændre i de databehandleraftaler, som de har indgået med udgangspunkt i KL og KOMBIT´s skabelon af 3. april 2017 (version 1.0). I kommentarnotatet er der bl.a. foretaget indholdsmæssige tilføjelser vedrørende forståelsen af sikkerhedsforanstaltninger, samt eksempler på formuleringer fra Datatilsynets skabelon for databehandleraftaler. Herudover er der indsat henvisninger til artikler i Databeskyttelsesforordningen.

Skabelonen er udarbejdet således, at den indeholder den regulering, der gælder, når Databeskyttelsesforordningen får virkning 25. maj 2018.

Supplerende praksis

Kommunerne har ønsket en skabelon for databehandleraftaler, hvor deres interesser varetages i forhold til de særlige forhold, der typisk gør sig gældende for kommunerne, når de skal indgå en databehandleraftale med en it-leverandør. Der er derfor blevet indarbejdet nogle mere praktiske og processuelle bestemmelser, der kan have relevans for et aftaleforhold mellem en kommune som dataansvarlig og en leverandør som databehandler (disse er markeret med gult i skabelonen).

Det er vigtigt at understrege, at den supplerende praksis ikke er krav til indholdet i en databehandleraftale i medfør af lovgivningen. **Kommunen kan derfor undlade at medtage de supplerende praksisbestemmelser og stadig overholde lovgivningen.** De supplerende praksisbestemmelser regulerer bl.a. forhold, som kommunerne også kan vælge at aftale andetsteds end i en databehandleraftale – f.eks. i Hovedaftalen.

Anvendelse af skabelonen

Kommunen er dataansvarlig og vil således altid være ansvarlig for indholdet af de databehandleraftaler, der indgås med kommunens leverandører. Brug af skabelonen i original eller tilpasset form er derfor kommunens ansvar.

Der er, jf. ovenfor, bestemmelser i skabelonen, som ikke udspringer af lovgivning på området, men er udtryk for supplerende praksis. Kommunerne skal derfor overveje, om de ønsker at anvende nogle af disse forslag til supplerende praksisbestemmelser i deres databehandleraftale, og i givet fald hvilke. Kommunen bør således foretage en egen

vurdering af konsekvenser af til- og fravalg, herunder økonomiske, og gøre sig klart, hvad der allerede er indeholdt i Hovedaftalen.

I skabelonen anvendes en model, hvor priser og vederlag forudsættes aftalt i Hovedaftalen. Det betyder, at betaling til Leverandøren, som relaterer sig til databehandleraftalen, forventes at indgå i det vederlag, der aftales i Hovedaftalen mellem Kommunen og Leverandøren. Hvis skabelonen anvendes til at indgå en ny databehandleraftale til en allerede eksisterende Hovedaftale, kan der derfor være behov for at foretage en mapping af bestemmelserne i databehandleraftalen i forhold til hvilke af disse, der vil være inkluderet i det aftalte vederlag i den eksisterende Hovedaftale.

Skabelonen er en model, som kommunerne kan supplere og ændre efter behov, f.eks. i forhold til den Hovedaftale, som kommunen har med leverandøren. Særligt i forhold til de bestemmelser, der er markeret med gult i skabelonen (supplerende praksisbestemmelser), bør kommunen sikre sig, at der er sammenhæng mellem indholdet i Hovedaftalen og i databehandleraftalen, da der kan være tale om et fordyrende krav på nye aftaler eller eventuelt krav om merbetaling afhængigt af hvad, der er aftalt i den eksisterende hovedaftale**. Kommunen bør derfor forholde sig til kommentarerne til skabelonen i dette dokument.**

Nærværende overordnede kommentarer til bestemmelserne er udarbejdet som en læsevejledning og hjælp til forståelsen af skabelonen. Kommentarerne er udarbejdet på baggrund af de input, som er indkommet i forbindelse med høringen af et udkast til skabelonen. De er således ikke juridiske, men derimod mere praktiske kommentarer, der er målrettet kommunerne og kommunernes arbejde med formuleringen af databehandleraftaler. Kommentarerne kan derfor *ikke* bruges som fortolkningsbidrag i forbindelse med tvister, der måtte opstå mellem leverandøren og kommunen herom.

I afsnit 2 nedenfor er beskrevet, hvordan skabelonen tilpasses, så den passer til det konkrete aftaleforhold.

2. Sådan tilpasses skabelonen

Skabelonen skal altid tilpasses i forhold til den konkrete aftale, som du ønsker at indgå. Nedenfor er beskrevet, hvordan du tilpasser skabelonen, så den kun indeholder lovkrav, der følger af Databeskyttelsesforordningen, eller så den også indeholder en eller flere bestemmelser, der er udtryk for supplerende praksis.

Hvis du vil indgå en databehandleraftale, der kun indeholder de lovkrav, der gælder fra 25. maj 2018

Hvis kommunen alene ønsker en databehandleraftale med de bestemmelser, der gælder fra 25. maj 2018, vil kommunen kunne tilpasse skabelonen ved at:

- Fjerne tekst markeret med gult
- Fjerne vejledende tekst skrevet i kursiv
- Udfylde tekststeder markeret med grønt.

Hvis du vil indgå en databehandleraftale, der indeholder lovkrav, der gælder fra 25. maj 2018, men også ønsker, at den skal indeholde en eller flere udvalgte supplerende praksisbestemmelser

Hvis kommunen ønsker en databehandleraftale med de bestemmelser, der gælder fra 25. maj 2018 og udvalgte supplerende praksisbestemmelser, vil kommunen kunne tilpasse skabelonen ved at:

- Fjerne tekst markeret med gult, der **ikke** ønskes inkluderet i Aftalen (dette kan medføre, at der skal rettes henvisninger til punkter i Aftalen)
- Fjerne vejledende tekst skrevet i kursiv
- Udfylde tekststeder markeret med grønt.

Generelt er det ved tilpasning af skabelonen vigtigt at sikre sig, at henvisningerne til punkter i Aftalen stadig er retvisende, så der ikke henvises til et punkt, som er fjernet.

3. Kommentarer til bestemmelser

Punkt 1 – Generelt

Punkt 1.3

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen.

Det er vigtigt, at Kommunen gør sig klart, om der alt afhængig af løsningens størrelse og kompleksitet f.eks. skal stilles krav om, at Leverandøren er ISO-certificeret eller, om der skal stilles krav om, at Leverandøren overholder alle eller dele af principper og anbefalinger i ISO27001.

Kommunen skal være opmærksom på, at der – hvis der stilles krav til Leverandøren om en ISO27001-certificering – vil kunne blive tale om et fordyrende krav, som afhængig af løsningens eller ydelsens karakter, kan risikere ikke at stå mål med udbyttet. Kommunen skal også være opmærksom på, at der ved et krav om, at Leverandøren skal være ISO-certificeret, kan opstå en situation, hvor der vil være leverandører, som rent faktisk kan levere løsningen eller ydelsen, men som på grund af kravet om ISO-certificering, må afstå fra at byde på opgaven.

Som alternativ til en ISO-certificering kan Kommunen konkret udpege krav fra principper og anbefalinger i ISO-certificeringen, som vil være relevante at stille krav om, at Leverandøren overholder.

Med baggrund i disse overvejelser skal Kommunen beslutte, om der skal stilles krav til Leverandøren om helt eller delvist at skulle efterleve principperne og anbefalingerne i ISO27001 og herefter eventuelt indsætte et krav herom i pkt. 1.3. En overordnet formulering af dette krav kan være: ”*Principperne og anbefalingerne i ISO27001 med senere ændringer vil på alle relevante områder finde anvendelse i det omfang andet ikke fremgår af Aftalen*”. Kommunen bør dog være opmærksom på, at et sådant krav vil være vanskeligt for leverandører at vurdere omfanget af, og prisen for at få denne formulering med i aftalen vil være tilsvarende høj.

Kommunen kan, hvis der ønskes en sikring af dele af principperne og anbefalingerne i ISO27001, f.eks. i Hovedaftalen mellem Kommunen og Leverandøren, udarbejde nogle konkrete krav, der skal være opfyldt eller angive hvilke kontroller, der konkret skal anvendes, f.eks. som specificeret i en sikkerhedspolitik. Kommunen kan eventuelt hente inspiration i Digitaliseringsstyrelsens sikkerhedskrav. Denne løsning vil være lettere for leverandører at prissætte.

Punkt 1.4

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

God databehandlingsskik indebærer f.eks., at databehandler og dataansvarlig skal overholde reglerne i lovgivningen såvel i ånd som i bogstav og ikke må forsøge at omgå reglerne. God databehandlingsskik medfører også, at en behandling, der er i strid med anden lovgivning end den persondataretlige, heller ikke lovligt vil kunne foretages.

Punkt 1.5

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen.

Hvis Kommunen ønsker at forpligte Leverandøren i forhold til Kommunens sikkerhedspolitik, regulativ eller regler, skal Kommunen træffe beslutning om, hvorvidt Leverandøren skal gøre "sig bekendt med" disse politikker, regulativer eller regler og om Leverandøren skal "forpligtes til at følge konkrete krav" og iværksætte særskilte foranstaltninger til overholdelse heraf. Kommunen skal være opmærksom på, at der – hvis der stilles krav til Leverandøren om dette – vil kunne blive tale om et fordyrende krav, som afhængigt af løsningens eller ydelsens karakter kan risikere ikke at stå mål med udbyttet.

Kommunen bør herudover nærmere beskrive, hvad der er indeholdt i de tre typer dokumenter (politik, regulativ, regler) og hvilke operationelle krav herfra, som Leverandøren skal efterleve. Disse fremgår typisk af it-sikkerhedsreglerne.

Forslag til formulering: "*Leverandøren forpligter sig herudover til at gøre sig bekendt med Kommunens it-sikkerhedsregulativ og it-sikkerhedspolitik, jf. bilag 4 og 5, og følge de relevante dertil hørende uddybende it-sikkerhedsregler, som vedlægges Aftalen som bilag 6. En skærpelse eller ændring af Kommunens it-sikkerhedsregler efter Aftalens indgåelse behandles efter ændringshåndteringsbestemmelserne i pkt. 11*".

Punkt 2 – Formål

Punkt 2.1

Skabelonen for databehandleraftaler mellem kommuner og it-leverandører er udarbejdet ud fra en forudsætning om, at Kommunen har indgået en aftale med Leverandøren, der nærmere beskriver den opgave, der skal løses samt vilkår herfor. Denne aftale er benævnt "Hovedaftale" og er således noget andet end databehandleraftalen mellem Kommunen og Leverandøren. Hovedaftalen mellem Kommunen og Leverandøren er en forudsætning for, at der overhovedet bliver behov for en databehandleraftale.

Punkt 3 – Kommunens rettigheder og forpligtelser

Punkt 3.1

Teksten markeret med gult er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage teksten markeret med gult og stadig overholde lovgivningen.**

Teksten er medtaget for at synliggøre den grundlæggende forudsætning om, at Kommunen har ansvaret for at sikre grundlaget for behandlingen af personoplysningerne.

Punkt 3.3
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Se kommentarer under punkt 1.5. Ændring af bilag med sikkerhedsregler mv. vil være udtryk for en ændring af databehandleraftalen, som skal håndteres i henhold til pkt. 11 i Aftalen.

Punkt 4 – Leverandørens forpligtelser

Punkt 4.1
Teksten markeret med gult er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage teksten markeret med gult og stadig overholde lovgivningen.**

Teksten synliggør den grundlæggende forudsætning om, at Leverandøren er underlagt de forpligtelser, der følger af lovgivningen.

Punkt 4.3
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Fortegnelser over behandlinger af personoplysninger
Leverandøren bliver i medfør af Databeskyttelsesforordningen pålagt en række nye forpligtelser, heriblandt kravet i artikel 30, stk. 2, om at føre fortegnelser over behandlinger af personoplysninger.

Man kan læse mere om fortegnelser i vejledningen på Datatilsynets hjemmeside og på KL´s hjemmeside.

Fortegnelser over brud på persondatasikkerheden
Kravet til Leverandøren om at føre fortegnelse over alle brud på persondatasikkerheden er ikke et krav, som Leverandøren er pålagt efter Databeskyttelsesforordningen, men kan være et krav, som Kommunen vælger at stille for, at Kommunen lettere vil kunne leve op til sin egen forpligtelse til at kunne dokumentere alle sikkerhedsbrud. Kommunen skal være opmærksom på, at hvis dette krav medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler. Det kan desuden allerede i Hovedaftalen være aftalt, at leverandøren løbende rapporterer om brud på persondatasikkerheden i f.eks. månedlige statusrapporter – dette bør i så fald indgå i kommunens overvejelser om, hvorvidt denne bestemmelse er nødvendig at inkludere i databehandleraftalen.

Punkt 4.4
Hvis der i Hovedaftalen er aftalt yderligere sikkerhedsforanstaltninger, skal disse fremgå af Aftalens bilag 1 – Sikkerhed.

Punkt 4.5

Leverandørens forpligtelse til at hjælpe Kommunen med at opfylde dennes forpligtelser i forhold til den registreredes rettigheder følger eksplicit af Databeskyttelsesforordningen og er dermed en forpligtelse, som Leverandøren også fremadrettet må forudse i forbindelse med indgåelse af Hovedaftalen. Af Databeskyttelsesforordningens artikel 28, stk. 3, litra e, fremgår det, at en databehandler *"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".*

Ligeledes følger forpligtelsen til at hjælpe Kommunen med at opfylde sine forpligtelser i forhold til underretning af den registrerede ved brud på persondatasikkerheden også af Databeskyttelsesforordningen, jf. artikel 28, stk. 3, litra f.

Nogle leverandører har ved høringssvar gjort opmærksom på, at det kan være vanskeligt at estimere omfanget af denne forpligtelse, da de ikke på forhånd vil kunne vide hvor meget tid og ressourcer, de vil skulle bruge på at bistå Kommunen. Omfanget af forpligtelsen kan afhænge af hvilke tekniske og organisatoriske foranstaltninger, der anvendes for at kunne bistå Kommunen, f.eks. i forhold til, om det er muligt for Kommunen selv at få adgang til relevante oplysninger eller at kunne efterkomme anmodninger fra registrerede om udøvelse af deres rettigheder.

Jf. afsnit 1, Anvendelse af skabelonen, ovenfor, vil der ved indgåelse af en databehandleraftale til en eksisterende Hovedaftale med fordel kunne foretages en mapping af, om Leverandørens leverancer i forhold til denne forpligtelse er indeholdt i det aftalte vederlag i Hovedaftalen.

Man kan læse mere om registreredes rettigheder i vejledningen på Datatilsynets hjemmeside.

Punkt 4.6

Denne forpligtelse følger eksplicit af Databeskyttelsesforordningen og vil dermed være en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen. Forpligtelsen handler om at hjælpe Kommunen med Kommunens forpligtelser ift. behandlingssikkerhed, anmeldelse af og underretning om sikkerhedsbrud, konsekvensanalyser og forudgående høringer hos Datatilsynet. Af Databeskyttelsesforordningens artikel 28, stk. 3, litra f, fremgår det, at en databehandler *" 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".*

Nogle leverandører har ved høringssvar gjort opmærksom på, at det kan være vanskeligt at estimere omfanget af denne forpligtelse, da de ikke på forhånd vil kunne vide hvor meget tid og ressourcer, de vil skulle bruge på at bistå Kommunen.

Jf. afsnit 1, Anvendelse af skabelonen, ovenfor, vil der ved indgåelse af en databehandleraftale til en eksisterende Hovedaftale med fordel kunne foretages en mapping af, om Leverandørens leverancer i forhold til denne forpligtelse er indeholdt i det aftalte vederlag i Hovedaftalen.

Punkt 4.7
Her er tale om en forpligtelse, som følger af Databeskyttelsesforordningens artikel 28, stk. 1, og dermed en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

Punkt 4.8
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Af hensyn til Kommunens mulighed for at kunne føre tilsyn med Leverandørens overholdelse af databehandleraftalen, bør Kommunen dog stille krav om, at Leverandøren angiver den præcise adresse, hvor Kommunens personoplysninger behandles og opbevares.

Punkt 5 – Underleverandør (underdatabehandler)

Punkt 5.2
Skabelonen indeholder et krav om, at Leverandøren i hvert enkelt tilfælde skal indhente tilladelse fra Kommunen om brug af underdatabehandler. Dette er et ønske fra kommuner til indholdet i skabelonen.

Efter Databeskyttelsesforordningens artikel 28, stk. 2, har Kommunen dog også mulighed for at afgive en generel tilladelse til Leverandøren om brug af underdatabehandlere. I så fald skal der udarbejdes bestemmelser herom. Et bud på en sådan bestemmelse kan være: "*Leverandøren har ret til at anvende andre underdatabehandlere end dem, som er angivet i bilag 2, til at behandle de personoplysninger, som Kommunen har overladt til Leverandøren i medfør af Hovedaftalen. Leverandøren skal ajourføre oplysninger om underdatabehandlere i bilag 2 ved enhver ændring, og dermed give Kommunen mulighed for at gøre indsigelse mod ændringen*".

I Aftalens pkt. 5.2 er der givet mulighed for at medtage en sætning om, at Kommunen ikke kan nægte at godkende udskiftning eller tilføjelse af en underdatabehandler, medmindre der er en saglig grund hertil. Teksten markeret med gult er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage teksten markeret med gult og stadig overholde lovgivningen.**

Punkt 5.3
Hvis Leverandøren gør brug af en underdatabehandler vil Leverandøren være forpligtet til at indgå en underdatabehandleraftale med denne, der som minimum indeholder de samme forpligtelser og krav, som der er aftalt i databehandleraftalen mellem Kommunen og Leverandøren. Forpligtelsen følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 4, og er dermed en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

Punkt 5.4
Her er tale om en forpligtelse, som følger af Databeskyttelsesforordningens artikel 28, stk. 4, og dermed en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

I det omfang Leverandøren ønsker at anvende underdatabehandlere, der har egne standardvilkår for databehandling og det ansvar, der følger hermed, vil Leverandøren fortsat skulle sikre sig, at disse overholder de samme krav, som dem Kommunen har stillet til Leverandøren. Leverandøren skal over for Kommunen kunne dokumentere, at disse krav er overholdt også i de tilfælde, hvor der er tale om standardvilkår fra større internationale underleverandører.

Punkt 5.5
Leverandøren har over for Kommunen ansvaret for underdatabehandlerens overholdelse af dennes forpligtelser. Forpligtelsen følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 4, og er dermed en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

Leverandøren er således forpligtet til at sikre et tilsyn med underdatabehandleren, der påviser underdatabehandlerens overholdelse af underdatabehandleraftalen.

I forhold til Leverandørens tilsyn med underdatabehandleren vil betalingen herfor være et forhold, som er aftalt mellem Leverandøren og underleverandøren.

Punkt 5.6
Leverandørens forpligtelse til at hjælpe Kommunen med at påse, at Leverandøren overholder Aftalen og har indgået de krævede underdatabehandleraftaler med eventuelle underleverandører følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra h.

Punkt 5.7
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

I Aftalen etableres et kædeansvar, hvor Leverandøren er ansvarlig for underdatabehandleren. Derfor anbefales det, at Kommunen ikke kommunikerer direkte med underdatabehandleren, men i stedet lader kommunikationen gå gennem Leverandøren.

Punkt 6 – Instrukser

Punkt 6.1
Kravet om, at en databehandler kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige følger af Databeskyttelses-forordningens artikel 28, stk. 3, litra a.

Kravet om, at Leverandøren skal fremsende instruksen til eventuelle underdatabehandlere, er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage**

teksten markeret med gult og stadig overholde lovgivningen. Hvis man anvender formuleringen i pkt. 5.7 om, at kommunikation til underdatabehandlere går gennem Leverandøren, bør en eventuel fremsendelse af instruks følge samme kommunikationsvej.

Punkt 6.2

Det følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, at databehandleren også bærer et ansvar for, at en instruks ikke er i strid med lovgivningen. Det overordnede ansvar er fortsat Kommunens, men i de sikkert få tilfælde, hvor der opstår en situation, hvor Kommunen udsteder en instruks, som Leverandøren ved ikke er lovlig, da bærer Leverandøren også et ansvar for at sige fra.

Punkt 7 – Tekniske og organisatoriske sikkerhedsforanstaltninger

Punkt 7.2

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Her er tale om, at Leverandøren skal gennemgå egne interne sikkerhedsforskrifter og retningslinjer. Kommunen skal være opmærksom på, at hvis dette krav medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler eller eventuelt et krav om merbetaling afhængigt af hvad, der er aftalt i en eksisterende Hovedaftale.

Punkt 7.3

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Her er tale om, at Leverandørens og dennes ansattes adgang til data mv. skal begrænses så meget som muligt. De må altså hverken kunne se, tilvejebringe, benytte etc. oplysninger, som ikke er nødvendige for udførelse af de opgaver, de er pålagt i henhold til Aftalen eller Hovedaftalen.

Punkt 7.4

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Punkt 7.5

Leverandøren bliver i medfør af Databeskyttelsesforordningen pålagt en række nye forpligtelser, heriblandt kravet om at underrette Kommunen ved brud på persondatasikkerheden, men det er ikke et krav, at denne forpligtelse fremgår af en databehandleraftale.

Ifølge Databeskyttelsesforordningens artikel 33, stk. 2, skal en databehandler underrette den dataansvarlige om et brud på persondatasikkerheden *'uden unødig forsinkelse'*. I bestemmelsen i skabelonen er der mulighed for i stedet at vælge

formuleringen '*straks*', da dette er et kommunalt ønske. Kommunen skal ved anvendelse af skabelonen tilpasse bestemmelsen, så den afspejler den ordlyd, som Kommunen ønsker i den konkrete aftale.

Man kan læse mere om håndtering af brud på persondatasikkerheden i vejledningen på Datatilsynets hjemmeside.

Der vil kunne være situationer, hvor Leverandøren ikke i første omgang kan udrede alle detaljer om det konkrete sikkerhedsbrud eller lignende, og Leverandøren vil da skulle sørge for den fornødne efterfølgende og mere detaljerede underretning til Kommunen løbende derefter.

Kommunen skal angive kontaktoplysninger på personer eller mailadresser, hvortil Leverandøren skal give sin underretning. Dette kan f.eks. være angivet i Hovedaftalens afsnit/bilag om samarbejdsorganisationen. Har Kommunen ikke angivet sådanne særlige kontaktoplysninger, vil Leverandøren skulle sende underretningen til Kommunens centrale mail samt til den medarbejder hos Kommunen, som har underskrevet og indgået aftalen med Leverandøren.

De angivne underpunkter om situationer af sikkerhedsmæssig karakter, hvor Leverandøren straks skal underrette Kommunen, er ikke krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage teksten markeret med gult og stadig overholde lovgivningen.** Kommunen skal være opmærksom på, at hvis underpunkterne medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler eller eventuelt et krav om merbetaling afhængigt af hvad, der er aftalt i en eksisterende Hovedaftale.

Punkt 7.6

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Emnet kan eventuelt behandles i Hovedaftalen.

Punkt 8 – Overførsler til andre lande

Punkt 8.1

Dette er et eksplicit krav i Databeskyttelsesforordningen til indholdet af en databehandleraftale.

Af artikel 28, stk. 3, litra a, fremgår det, at også overførsel til internationale organisationer er betinget af den dataansvarliges instruks. Hvis det er relevant i forhold til den enkelte aftale, kan Kommunen derfor tilføje "eller internationale organisationer" efter "(tredjelande)" i bestemmelsen.

Punkt 8.2

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Man kan læse mere om overførsel til tredjelande og gyldige overførselsgrundlag i vejledningen på Datatilsynets hjemmeside.

Punkt 8.3

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Bestemmelsen kan tages med i de tilfælde, hvor Justitsministeren har fastsat regler om, at personoplysninger, der behandles i nærmere bestemte IT-systemer, og som føres for den offentlige forvaltning, helt eller delvist alene må opbevares her i landet, jf. Databeskyttelseslovens § 3, stk. 9.

Hvis 8.3 anvendes, bortfalder skabelonens pkt. 8.1-8.2, og 8.3 bliver således til nyt pkt. 8.1.

Kommunen kan i instruksen angive, at Leverandøren ikke må overføre Kommunens oplysninger til tredjelande.

Punkt 9 – Tavshedspligt og fortrolighed

Punkt 9.1

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Punkt 9.2

Denne forpligtelse følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra b, og vil dermed være en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

Punkt 10 – Kontroller og erklæringer

Det er vigtigt, at Kommunen gør sig klart hvilken form for inspektion eller revision, der vil være relevant og nødvendig at gennemføre hos Leverandøren, når der henses til f.eks. løsningens størrelse, omfanget og klassifikationen af de behandlede personoplysninger og kompleksitet samt konkrete forhold hos Leverandøren, idet dette vil kunne få betydning for Leverandørens priser, samt mindre leverandørers muligheder for i det hele taget at indgå aftaler med kommuner herom.

Man kan læse mere om tilsyn med databehandlere og underdatabehandlere i den vejledende tekst på Datatilsynets hjemmeside.

Punkt 10.1

Forpligtelsen til at give Kommunen de nødvendige oplysninger følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra h, og er dermed en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

De gule markeringer er præciseringer/skærpelser, som Kommunen kan vælge at tage med eller fjerne. Kommunen skal være opmærksom på, at hvis disse præciseringer medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler eller eventuelt et krav om merbetaling, afhængigt af hvad der er aftalt i en eksisterende Hovedaftale.

Punkt 10.2

Der er med gult markeret en mulighed for, at Kommunen kan specificere hvilke former for dokumentation, der ønskes. Dette kan være en hjælp i forhold til aftaler med mindre leverandører. Logningskrav vil ikke være et specifikt krav, der følger af Databeskyttelsesforordningen. Kommunen skal være opmærksom på, at hvis de gule markeringer medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler eller eventuelt et krav om merbetaling, afhængigt af hvad der er aftalt i en eksisterende Hovedaftale.

Punkt 10.3, 10.4 og 10.5

Det er en god ide at specificere, hvordan man som dataansvarlig ønsker at føre kontrol med sin databehandler. Valg af model og pris bør ske ud fra overvejelser om Kommunens eget organisatoriske set-up og kapacitet, løsningsstørrelse, mængden af eller hvilke kategorier af oplysninger, der er tale om (almindelige eller følsomme oplysninger) mv.

Punkt 10.3

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Bestemmelsen indeholder en mulighed for at vælge enten en erklæring, der overholder gældende og anerkendte branchestandarder, eller en standarderklæring.

Underdatabehandlers efterlevelse kan eventuelt påvises ved, at der vedlægges en særskilt erklæring, som er udarbejdet for dennes behandling.

Såfremt Kommunen medtager denne bestemmelse i den konkrete aftale, bør Kommunen og Leverandøren aftale en frekvens for fremsendelse af en erklæring til Kommunen. Det bør ligeledes aftales, hvornår første erklæring skal fremsendes.

Leverandørens pris for erklæringen forudsættes her inkluderet i det vederlag, der er aftalt i forbindelse med indgåelse af Hovedaftalen.

Punkt 10.4

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Bestemmelsen indeholder en mulighed for at vælge enten en erklæring, der overholder gældende og anerkendte branchestandarder, eller en standarderklæring.

Underdatabehandlers efterlevelse kan eventuelt påvises ved, at der vedlægges en særskilt erklæring, som er udarbejdet for dennes behandling.

Såfremt Kommunen medtager denne bestemmelse i den konkrete aftale, bør Kommunen og Leverandøren aftale en frekvens for fremsendelse af en erklæring til Kommunen bl.a. af hensyn til fastlæggelse af Leverandørens pris herfor. Det bør ligeledes aftales, hvornår første erklæring skal fremsendes. Betaling for erklæringen aftales mellem Kommunen og Leverandøren.

Punkt 10.5

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Der er her tale om Kommunens eget tilsyn – altså et tilsyn, der træder i stedet for anvendelse af revisionserklæringer. Såfremt Kommunen medtager denne bestemmelse i den konkrete aftale, bør Kommunen og Leverandøren i Hovedaftalen nærmere aftale Leverandørens indsats samt betaling for, at Leverandøren giver mulighed for og bidrager til dette tilsyn.

Punkt 10.6

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Såfremt Kommunen medtager denne bestemmelse i den konkrete aftale, bør forpligtelsen for eventuelle underdatabehandlere til at stille tid og ressourcer til rådighed ved inspektion af foranstaltningerne fremgå af underdatabehandler-aftalerne.

Punkt 11 – Ændringer i Aftalen

Punkt 11.1

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Aftalen og instruksen, jf. bilag 3, kan til enhver tid ændres med et varsel, der angives nærmere i Aftalen. Varslet bør følge det angivne varsel i Hovedaftalen. Der kan dog være forskellige varsler, hvorfor processen kan aftales skriftligt.

Processen og de praktiske forhold for gennemførelse af ændringer vil som hovedregel følge de bestemmelser, der er fastlagt herom i Hovedaftalen, og i det omfang Kommunen måtte ønske anden proces eller ændringer herfor, vil dette skulle angives særskilt.

Punkt 11.2

Kommunen angiver det ønskede varsel.

Punkt 12 – Sletning af data

Punkt 12.1
Kommunen skal træffe beslutning om, hvorvidt Kommunens data ønskes slettet eller tilbageleveret ved udløb af Hovedaftalen. Leverandørens forpligtelse til at slette eller tilbagelevere personoplysningerne følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra g, og er dermed en forpligtelse, som Leverandøren må forudse i forbindelse med indgåelse af Hovedaftalen.

Punkt 12.2
Se kommentar til punkt 12.1.

Hvis Kommunen stiller særlige krav til dataformat ved tilbagelevering, vil dette med fordel kunne angives i Hovedaftalen mellem Kommunen og Leverandøren.

Punkt 12.3
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Kommunen skal være opmærksom på, at hvis dette krav medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler eller eventuelt et krav om merbetaling, afhængigt af hvad der er aftalt i en eksisterende Hovedaftale.

Punkt 12.4
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Kommunen skal være opmærksom på, at hvis dette krav medtages i databehandleraftalen, kan der være tale om et fordyrende krav ved nye aftaler eller eventuelt et krav om merbetaling, afhængigt af hvad der er aftalt i en eksisterende Hovedaftale.

Der er i skabelonen angivet et eksempel på en standard for sletning. Denne standard er dog blot én af en række forskellige standarder. Hvis kommunen vælger at medtage denne supplerende praksisbestemmelse i en databehandleraftale, er det derfor vigtigt, at der angives en standard, som passer til den konkrete aftale, type af løsning etc. Hvilken standard, der er egnet og passende, kan evt. afklares i dialog med Leverandøren.

Punkt 13 – Misligholdelse og tvistigheder

Punkt 13.1
Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Ved Kommunens eventuelle misligholdelse af Hovedaftalen, må Leverandøren ikke tilbageholde Kommunens data – dette kan man eventuelt sikre sig fremgår eksplicit af Hovedaftalen.

Punkt 14 – Erstatning og forsikring

Punkt 14.1

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Punkt 15 – Ikrafttræden og varighed

Punkt 15.1

Der er ikke tale om et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage denne supplerende praksisbestemmelse og stadig overholde lovgivningen.**

Bilag 1 – Sikkerhed

Indledning

Idet Leverandøren oftest vil være nærmest til at beskrive den konkrete udmøntning af de sikkerhedsmæssige krav, som Kommunen stiller til den behandling af personoplysninger, som Leverandøren påtager sig på vegne af Kommunen, er der i modellen lagt op til, at det er Leverandøren, der udfylder bilaget med beskrivelse af foranstaltninger.

Med baggrund i det af Leverandøren udfyldte bilag 1, vil Kommunen skulle sikre sig, at dette svarer til de lovgivningsmæssige krav, der er stillet til Leverandørens behandling af personoplysninger på vegne af Kommunen.

Sikkerhedskrav

Kommunen skal således sikre sig en sammenhæng mellem de eventuelle krav, der er stillet i Hovedaftalen om sikkerhed og de krav, som fremgår af bilag 1 i databehandleraftalen, således, at såvel Kommunen som Leverandøren har det fornødne grundlag for at estimere og beregne vederlag m.m. i forhold til den pris, der aftales for Leverandørens leverance. Der er i bilag 1 givet mulighed for, at der kan indsættes krav fra Hovedaftalen eller henvises til relevante afsnit i Hovedaftalen.

I bilag C til Datatilsynets standard-skabelon for databehandleraftaler indgår nedenstående hjælpetekst i forbindelse med angivelse af hvilke foranstaltninger, der kan være aftalt mellem en dataansvarlig og en databehandler:

[Beskriv eventuelle krav vedrørende pseudonymisering og kryptering af personoplysninger]

[Beskriv eventuelle krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester]

[Beskriv eventuelle krav vedrørende evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse]

[Beskriv eventuelle krav vedrørende procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed]

[Beskriv eventuelle krav vedrørende adgang til data via internettet]

[Beskriv eventuelle krav vedrørende beskyttelse af data, hvor de transmitteres]

[Beskriv eventuelle krav vedrørende beskyttelse af data, hvor de opbevares]

[Beskriv eventuelle krav vedrørende fysisk sikring af lokaliteter, hvor der behandles personoplysninger]

[Beskriv eventuelle krav vedrørende anvendelse af hjemme-/fjernarbejdspladser]

[Beskriv eventuelle krav vedrørende logning]

Ovennævnte sikkerhedsforanstaltninger gennemgås nærmere i afsnit 3.3. i Datatilsynets og Justitsministeriets vejledning 'Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger'.

Særlige opmærksomhedspunkter fra 25. maj 2018

Hvis Leverandøren skal behandle personoplysninger på vegne af Kommunen fra 25. maj 2018, skal bilag 1 beskrive, hvordan Leverandøren overholder kravene i Databeskyttelsesforordningens artikel 32.

Som det første eksempel på en foranstaltning, som det kan være relevant at gøre brug af i sikkerhedsmæssige sammenhænge, nævnes i forordningens artikel 32, stk. 1, litra a, begreberne *pseudonymisering og kryptering* af personoplysninger.

Særligt for så vidt angår begrebet pseudonymisering gælder, at dette er nærmere defineret i artikel 4, nr. 5. Det fremgår heraf, at med pseudonymisering menes behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person.

Endvidere fremgår af forordningens betragtning 28 følgende:

"Anvendelsen af pseudonymisering af personoplysninger kan mindske risikoen for de berørte registrerede og gøre det lettere for dataansvarlige og databehandlere at opfylde deres databeskyttelsesforpligtelser. Det er ikke tanken med den udtrykkelige indførelse af "pseudonymisering" i denne forordning at udelukke andre databeskyttelsesforanstaltninger. "

Med kryptering menes en foranstaltning, der, hvis den er behørigt implementeret, kan mindske risikoen for manglende fortrolighed, integritet, uafviselighed og autentifikation.

I forordningens artikel 32, stk. 1, litra b peges endvidere på en anden mulig foranstaltning i form af *evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.*

Med udtrykket *integritet* sigtes bl.a. til, at det er muligt at validere, om data på disse systemer er nøjagtige og fuldstændige, eksempelvis via cheksum/hashing, samt at dette vedligeholdes/kontrolleres vedvarende.

For så vidt angår behandlingssystemer og -tjenesters *tilgængelighed* sigtes bl.a. til, at behandlingssystemer og -tjenester og data i disse er tilgængelige ved anmodning fra autoriseret bruger, eksempelvis ved at sikre en velfungerende backup eller dublerede systemer alt afhængig af om det er relevant, samt at dette vedligeholdes vedvarende.

Med udtrykket *robusthed* sigtes bl.a. til at sikre behandlingssystemer og -tjenester imod udfald f.eks. ved dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning, mv. alt afhængig af om det er relevant, samt at dette vedligeholdes vedvarende.

Endvidere fremgår det af forordningens artikel 32, stk. 1, litra c, at en anden foranstaltning, der kan komme på tale, er *evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse*.

Der sigtes hermed til, at organisationen på forhånd skal vide, hvordan adgangen til personoplysninger genoprettes i tilfælde af hændelser som f.eks. brand, hacking, ransomware eller overgravede datakommunikationskabler. Det kan fordre, at organisationen har planlagt, hvorledes it-driften i pågældende tilfælde kan genoprettes inden for et nærmere bestemt tidsrum, f.eks. ved brug af backup eller overgang til alternative datakommunikationslinjer alt afhængig af, om det er relevant. Evnen til rettidig genoprettelse kan demonstreres ved øvelser og test.

I forordningens artikel 32, stk. 1, litra d, peges endelig på foranstaltningen en *procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed*.

Det sigtes hermed til f.eks. med jævne mellemrum at teste/afprøve, vurdere og evaluere følgende – alt afhængig af om det er relevant: Firewalls, krypterede forbindelser, krypterede lagringer, foranstaltninger imod forsøg på overbelastelsesangreb, foranstaltninger imod forsøg på at gætte adgangsgivende faktorer, adgangskontrol, brugeradministrationsprocessen og meget andet.

Bilag 3 – Instruks

I indledningen til instruksen kan Kommunen vælge at gentage kravet om, at Leverandøren er ansvarlig for at indgå underdatabehandleraftaler med

underleverandører. Dette er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, jf. pkt. 1.1 i Aftalen. **Kommunen kan derfor undlade at medtage teksten markeret med gult og stadig overholde lovgivningen.**

1.1 Behandlingens formål

Datatilsynet har i deres skabelon for databehandleraftaler angivet følgende eksempel på en beskrivelse af **formålet med en behandling**: "*At den dataansvarlige kan anvende systemet X, som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om den dataansvarliges medlemmer*".

1.2 Generel beskrivelse af behandlingen

Kommunen kan eventuelt bede Leverandøren om oplysninger, som gør det muligt for Kommunen at beskrive behandlingerne i medfør af Hovedaftalen udførligt.

Datatilsynet har i deres skabelon for databehandleraftaler angivet følgende eksempel på en beskrivelse af **karakteren af en behandling**: "*At databehandleren stiller systemet X til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges medlemmer på virksomhedens servere*."

Datatilsynet har i deres skabelon for databehandleraftaler angivet følgende eksempel på en beskrivelse af **varigheden af en behandling**: "*Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne*".

1.3 Typen af personoplysninger

Datatilsynet har i deres skabelon for databehandleraftaler angivet følgende eksempler på en beskrivelse af typer af personoplysninger: "*Navn, e-mailadresse, telefonnummer, adresse, cpr-nummer, betalingsoplysninger, medlemsnummer, type af medlemskab, fremmøde i fitnesscenteret og tilmelding til konkrete fitnesshold.*"
I skabelonen er der gjort plads til, at der kan angives hvilke typer af personoplysninger, som der foretages behandling af.

1.5 Tredjelande (ikke EU-medlemslande)

Med tredjeland menes et land, som ikke er medlem af EU eller EØS. Tredjelande er opdelt i to kategorier: Sikre og usikre. Der er forskel på, hvad der regnes for et gyldigt overførselsgrundlag alt efter, om der vil ske overførsel til et sikkert eller usikkert tredjeland – kommunen og leverandøren bør således sikre, at der er et gyldigt grundlag for at kunne overføre til den pågældende leverandør/underleverandør i et tredjeland, inden en overførsel finder sted.

Kommunen kan her eksplicit angive, at Leverandøren ikke må overføre Kommunens oplysninger til tredjelande. I stedet for den eksisterende tekst i punktet, kan der i så fald indsættes følgende tekst: *"Leverandøren må ikke overføre personoplysninger til tredjelande."*

Man kan læse mere om tredjelande og overførselsgrundlag i vejledningen på Datatilsynets hjemmeside.

4. Versionshistorik

Versionsnr.	Dato	Kommentar
1.0	3. april 2017	
2.0	30. maj 2018	Tilpasset i forhold til version 2.0 af skabelon for databehandleraftaler mellem kommuner og it-leverandører, der ikke indeholder henvisninger og krav relateret til tidligere persondatalovgivning.
2.1	24. januar 2019	Indsat præcisering i afsnit 'Punkt 12.4' vedr. valg af egnet, passende standard for sletning. Indsat henvisning i afsnit 'Bilag 1 – Sikkerhed' til vejledning fra Datatilsynet og Justitsministeriet om behandlingssikkerhed. Indsat versionshistorik.