Hjælp til udfyldelse af Bilag C og D i Datatilsynets standardkontraktsbestemmelser - Version 1.0 af 31. august 2020

Indhold

Baggrund

Datatilsynet har i december 2019 offentliggjort en revideret udgave af deres databehandleraftaleskabelon. Det er sket efter, at Det Europæiske Databeskyttelsesråd har haft den til kommentering. Den reviderede udgave har nu karaktér af "standardkontraktsbestemmelser" som betyder, at Datatilsynet fx ved tilsynsbesøg ikke vil tjekke lovligheden af kontrakten. Der er dog ikke lovkrav om, at kommunerne skal benytte standardkontraktsbestemmelserne.

Flere kommuner har spurgt KL om, Datatilsynets standardkontraktsbestemmelser skal anvendes i stedet for KL-KOMBIT-databehandleraftaleskabelonen. KL har derfor gennemgået standardkontraktsbestemmelserne og sammenholdt dem med KL-KOMBIT-skabelonen.

KL anbefaler, at kommunerne anvender Datatilsynets standardkontraktsbestemmelser, når kommunerne indgår nye databehandleraftaler eller reviderer eksisterende aftaler. KL anbefaler desuden, at kommunerne opretholder eksisterende databehandleraftaler og ikke bruger tid på at overføre indholdet til Datatilsynets standardkontraktsbestemmelser. Databehandleraftaler, som er indgået via KL-KOMBIT´s databehandleraftaleskabelon, er fortsat fuldt lovlige.

Til KL-KOMBIT-skabelonen hørte notatet "Kommentarer til skabelon for databehandleraftaler mellem kommuner og it-leverandører". Notatet gav hjælp til udfyldelse og forståelse af KL-KOMBIT-databehandleraftaleskabelonen.

Flere kommuner har efterspurgt vejledning til udfyldelse af standardkontraktsbestemmelsernes bilag C og D, hvilket nærværende notat skal være en hjælp til. Notatet består primært af tekst fra notatet "Kommentarer til skabelon for databehandleraftaler mellem kommuner og it-leverandører" og relevante passager fra Datatilsynets vejledning om behandlingssikkerhed (markeret med kursiv i indramning), men er tilpasset standardkontraktsbestemmelsernes struktur.

Anvendelse af notatet

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

Notatet består af tre dele:

- Udfyldelse af Bilag C i Datatilsynets standardkontraktsbestemmelser
- Udfyldelse af Bilag D i Datatilsynets standardkontraktsbestemmelser
- Udfyldelse af Bilag D i Datatilsynets standardkontraktsbestemmelser (engelsk)

I første del uddybes, hvad der efterspørges i Bilag C1-C8, med forslag til hvad man som kommune kan skrive ind i bilagene. Bilag C2 indeholder flere underpunkter og er således også inddelt i underpunkter i dette notat.

I anden og tredje del af notatet kan databehandleren og den dataansvarlige aftale regulering af andre forhold i Bilag D. Her står forslag til konkrete krav, som kommunen kan kopiere over i aftalen, hvis dette ønskes.

Udfyldelse af Bilag C i Datatilsynets standard-kontraktsbestemmelser

Bilag C.1 Behandlingens genstand/instruks

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

Bilag C.2 Behandlingssikkerhed

[Beskriv elementer, der er afgørende for sikkerhedsniveauet]

Der er med forordningen […] kommet fokus på en risikobaseret tilgang. Den risikobaserede tilgang til sikkerhed er i forvejen kendt fra eksempelvis informationssikkerhedsstandarderne ISO 27001 og ISO/IEC 29134: 2017, som beskrives nærmere straks nedenfor. Denne risikobaserede tænkning kendetegnes ved implementeringen af processer, der tager højde for løbende identifikation af både risici og muligheder samt den efterfølgende overvågning, måling, evaluering og analyse af disse. […]
Det er vigtigt, at du er opmærksom på, at de risikovurderinger, du hidtil [inden 25. maj 2018] *har foretaget, ikke nødvendigvis er dækkende i forhold til forordningens risikobaserede tilgang, idet risici kan handle om mange ting. Forordningen har f.eks. ikke fokus på risici for organisationens aktiver/værdier, men derimod udelukkende fokus på risici for fysiske personers rettigheder og frihedsrettigheder. Dette indebærer, at andre (eller flere) konsekvenser og sandsynligheder kan komme i spil, når risici vurderes i henhold til forordningen.*
Udgangspunktet er således, at behandling af personoplysninger, er forbundet med risici for fysiske personer. Princippet er herefter, at der under selve udformningen og under iværksættelsen af en behandling skal etableres et sikkerhedsniveau, som passer til disse risici ved hjælp af passende tekniske og organisatoriske foranstaltninger, som du gennemfører. De foranstaltninger, som du etablerer, skal således søges målrettet mod de afdækkede risici.
De konsekvenser, der kan være for de registrerede, og som følgelig skal indgå i din risikovurdering er især (men ikke udelukkende):

- *Fysisk skade*
- *Materiel skade*
- *Immateriel skade*
- *Forskelsbehandling*
- *Identitetstyveri*
- *Identitetssvig*
- *Økonomiske konsekvenser, herunder finansielle tab*

- *Skade på omdømme*
- *Sociale konsekvenser*
- *Indflydelse på privatliv*
- *Skade på menneskelig værdighed*
- *Skade på legitime interesser*
- *Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder*
- *Forhindring i udøvelse af kontrol med egne personoplysninger*

Arbejdet med fastlæggelse af et tilstrækkeligt sikkerhedsniveau gennemgås nærmere i afsnit 3.3. af Datatilsynets og Justitsministeriets vejledning 'Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger'.

[Beskriv eventuelle krav vedrørende pseudonymisering og kryptering af personoplysninger]
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."

"Man kan f.eks. erstatte et personnummer med en "kode", som kan genfindes på en separat liste, hvor man kan se koblingen mellem personnummeret og koden. Det må dog ikke være muligt for uvedkommende at genskabe sammenhængen mellem person og kode."

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

"Kryptering skal f.eks. forstås således, at udvalgte (person)oplysninger (evt. enkelte identificerende parametre) ved hjælp af en hemmelig krypteringsnøgle gøres ulæselige."

[Beskriv eventuelle krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester]
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 tjeksum/hashing, samt at dette vedligeholdes/kontrolleres vedvarende.

Teknisk set handler integritet om, at de data, du har gemt i systemet, forbliver uændret, sådan som de er gemt, medmindre du har til hensigt at ændre dem. Som eksempler på sikkerhedsforanstaltninger i forhold til integritet kan nævnes elektronisk signatur, individuelle fortrolige adgangskoder og VPN-forbindelser.

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.

Det kan også være reetableringen ved f.eks. hændelig eller ulovlig tilintetgørelse af oplysninger. […]
Det er normalt en forudsætning, at der (samtidig) er fastsat organisatoriske processer for, hvordan disse opgaver udføres, og hvordan f.eks. backup testes.

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.

Der kan igen henvises til den internationale standard ISO 29151: 2017 om persondatakontroller, som i høj grad supplerer ISO IEC 27001: 2013 i forhold til foranstaltninger/kontroller til beskyttelse af personoplysninger.

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

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.

Det ligger heri, at din organisation har et beredskab for, hvordan adgangen til personoplysninger genoprettes i tilfælde af fysiske eller tekniske hændelser.

Det er derfor vigtigt, at din organisation har planlagt, hvordan it-driften i tilfælde af sådanne hændelser kan genoprettes inden for et nærmere bestemt tidsrum (og hvordan det bedst undgås, at du bliver ramt af f.eks. tekniske hændelser). Det kan f.eks. være, at der tages regelmæssige sikkerhedskopier, at du begrænser brugen og installationen af browser-plugins (udvidelses programmer der nok giver funktionalitet men også kan benyttes til afvikling af kode der kan kompromittere ens sikkerhed), eller at du kan etablere en overgang til alternative datakommunikationslinjer m.v.

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

Til eksempel kan du finde inspiration til en model for processer for arbejdet med it-sikkerhed i ISO IEC 27001:2013, anneks A, og for en gennemgang i katalogform over hvilke mulige sikkerhedsforanstaltninger, der kan benyttes, beskriver ISO IEC 29151: 2017 flere af disse.

Bilag C.3 Bistand til den dataansvarlige

Denne forpligtelse følger eksplicit af Databeskyttelsesforordningen og vil dermed være en forpligtelse, som databehandleren 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 databehandlere har 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.

Der vil ved indgåelse af en databehandleraftale til en eksisterende Hovedaftale med fordel kunne foretages en mapping af, om databehandlerens leverancer i forhold til denne forpligtelse er indeholdt i det aftalte vederlag i Hovedaftalen.

Bilag C.4 Opbevaringsperiode/sletterutine

Kommunen skal træffe beslutning om, hvorvidt kommunens data ønskes slettet eller tilbageleveret ved udløb af Hovedaftalen. Databehandleren forpligtelse til at slette eller tilbagelevere personoplysningerne følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra g.

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

I C.4 kan man eksempelvis vælge at stille krav om at databehandleren skal fremsende dokumentation for den påkrævede sletning. Eller man kan stille krav om at databehandleren foretager den påkrævede sletning efter en ønsket etableret international standard for sletning, f.eks. NIST 800-88.

Vælger kommunen at stille krav om, at der skal slettes i medfør af en etableret international standard, skal man være opmærksom på, at denne standard blot er 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 databehandleren.

Kommunen skal være opmærksom på, at hvis disse 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.

Bilag C.5 Lokalitet for behandling

Her angives de steder, hvor kommunens personoplysninger opbevares/behandles.

Bilag C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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 databehandleren bør således sikre, at der er et gyldigt grundlag for at kunne overføre til den pågældende databehandleren /underdatabehandleren i et tredjeland, inden en overførsel finder sted.

Kommunen kan her eksplicit angive, at databehandleren ikke må overføre kommunens oplysninger til tredjelande, for eksempel ved at skrive:
"Databehandleren må ikke overføre personoplysninger til tredjelande."
Man kan læse mere om tredjelande og overførselsgrundlag i vejledningen på Datatilsynets hjemmeside.

Bilag C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

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

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

Forpligtelsen til at give kommunen de nødvendige oplysninger følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra h.

Bilag C.8 [HVIS RELEVANT] Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

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

Databehandleren har over for kommunen ansvaret for underdatabehandlerens overholdelse af dennes forpligtelser. Forpligtelsen følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 4.

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

I forhold til databehandlerens tilsyn med underdatabehandleren vil betalingen herfor være et forhold, som er aftalt mellem databehandleren og underdatabehandleren.

Det følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra h, at databehandleren er forpligtet til at hjælpe kommunen med at påse, at databehandleren overholder Bestemmelserne og har indgået de krævede underdatabehandleraftaler med eventuelle underdatabehandlere.

Udfyldelse af bilag D i Datatilsynets standard-kontraktsbestemmelser

I bilag D kan databehandleren og den dataansvarlige aftale regulering af andre forhold. Her følger den tekst, som i KL/KOMBIT skabelonen for databehandleraftaler var markeret med gult, fordi de var valgfri tilføjelser ønsket af kommuner. Hvor det fortsat er relevant, står der under flere krav tilhørende hjælpetekst fra det tidligere kommentarnotat, som er en hjælp til kommunen og ikke skal kopieres over i en databehandleraftale. Nedenstående tekst er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen). Kommunen kan derfor undlade at medtage teksten markeret og stadig overholde lovgivningen. Teksten giver blot mulighed for, at kommuner kan tilføje krav til databehandleraftalen, der ligger udover det lovmæssigt krævede. I teksten er enkelte formuleringer markeret med [grønt]. Den grønne markering viser, at der her skal angives en ønsket tidsfrist eller en standard.

Præambel

"Databehandleren skal leve op til principper og anbefalinger i ISO27001."
Det er vigtigt, at kommunen gør sig klart, om der alt afhængig af løsningens størrelse og kompleksitet f.eks. skal stilles krav om, at databehandleren er ISO-certificeret eller, om der skal stilles krav om, at databehandleren overholder alle eller dele af principper og anbefalinger i ISO27001.

Kommunen skal være opmærksom på, at der – hvis der stilles krav til databehandleren 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 databehandleren 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 databehandleren overholder.

Med baggrund i disse overvejelser skal kommunen beslutte, om der skal stilles krav til databehandleren om helt eller delvist at skulle efterleve principperne og anbefalingerne i ISO27001 og herefter eventuelt indsætte et krav herom. 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 Bestemmelserne ". 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 databehandleren, 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.

"Databehandleren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger."

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

"Databehandleren er forpligtet til at gøre sig bekendt med den dataansvarliges it-sikkerhedsregulativ, it-sikkerhedspolitik og følge de eventuelle, dertilhørende uddybende it-sikkerhedsregler, som vedlægges Bestemmelserne som bilag [E-G]."

Hvis kommunen ønsker at forpligte databehandleren i forhold til kommunens sikkerhedspolitik, regulativ eller regler, skal kommunen træffe beslutning om, hvorvidt databehandleren skal gøre "sig bekendt med" disse politikker, regulativer eller regler og om databehandleren 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 databehandleren 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 databehandleren skal efterleve. Disse fremgår typisk af it-sikkerhedsreglerne.

3. Den dataansvarliges rettigheder og forpligtelser

"Den dataansvarlige har ansvaret for, at de personoplysninger, som den dataansvarlige instruerer databehandleren om at behandle, må behandles af databehandleren, herunder at behandlingen er nødvendig og legitim i forhold til den dataansvarliges opgavevaretagelse."

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

"Den dataansvarlige er forpligtet til at orientere databehandleren i tilfælde af den dataansvarliges eventuelle skærpede it-sikkerhedsregler og ved ændringer i den dataansvarliges it-sikkerhedspolitik og it-sikkerhedsregulativ, jf. bilag [E-G]."

Ændring af bilag med sikkerhedsregler mv. vil være udtryk for en ændring af databehandleraftalen, som skal håndteres i henhold til pkt. 14 i Bestemmelserne.

4. Databehandleren handler efter instruks

"Databehandleren har de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Bestemmelsernes pkt. 2.2."
Teksten synliggør den grundlæggende forudsætning om, at databehandleren er underlagt de forpligtelser, der følger af lovgivningen.

"Databehandleren skal føre fortegnelser over behandlingen af personoplysninger samt fortegnelser over alle brud på persondatasikkerheden."
Databehandleren 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 Datatilsynets vejledning og på KL´s hjemmeside.

Kravet til databehandleren om at føre fortegnelse over alle brud på persondatasikkerheden er ikke et krav, som databehandleren 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.

"Databehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor Den dataansvarliges personoplysninger behandles, jf. bilag C,C.5. Databehandleren skal ajourføre oplysningerne over for den dataansvarlige ved enhver ændring."
Af hensyn til kommunens mulighed for at kunne føre tilsyn med databehandlerens overholdelse af databehandleraftalen, bør kommunen dog stille krav om, at databehandleren angiver den præcise adresse, hvor kommunens personoplysninger behandles og opbevares.

"Det er databehandlerens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt 7, får tilsendt den dataansvarlige instruks, jf. bilag C."
Kravet om, at en databehandler kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige følger af Databeskyttelsesforordningens artikel 28, stk. 3, litra a.

5. Fortrolighed

"Databehandleren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Bestemmelserne indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse."

"Databehandleren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver."
Her er tale om, at databehandlerens 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 Bestemmelserne eller Hovedaftalen.

"Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, jf. pkt 10.1 uden forudgående skriftlig aftale med den dataansvarlige om indholdet af en sådan kommunikation, medmindre databehandleren har en retlig forpligtelse til sådan kommunikation."
Emnet kan eventuelt behandles i Hovedaftalen.

6. Behandlingssikkerhed

"Databehandleren skal [mindst en gang årligt] gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. C,C.2."
Her er tale om, at databehandleren 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.

"Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den dataansvarliges personoplysninger, om databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 5."

"Databehandleren er forpligtet til [straks/uden unødig forsinkelse] at underrette den dataansvarlige om

> *(i) enhver anmodning om videregivelse af personoplysninger omfattet af Bestemmelserne 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,

(ii) anden manglende overholdelse af databehandlerens, samt eventuelle underdatabehandleres forpligtelser uanset, om dette sker hos databehandleren eller hos en underdatabehandler."

Databehandleren bliver i medfør af Databeskyttelsesforordningen pålagt en række nye forpligtelser, heriblandt kravet om at underrette den dataansvarlige 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'.
Man kan læse mere i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden.

Der vil kunne være situationer, hvor databehandleren ikke i første omgang kan udrede alle detaljer om det konkrete sikkerhedsbrud eller lignende, og databehandleren 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 databehandleren skal give sin underretning. Dette kan f.eks. være angivet i Hovedaftalens afsnit/bilag om samarbejdsorganisationen. Har kommunen ikke angivet sådanne særlige kontaktoplysninger, vil databehandleren skulle sende underretningen til kommunens centrale mail samt til den medarbejder hos kommunen, som har underskrevet og indgået aftalen med databehandleren.

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.

7. Anvendelse af underdatabehandlere

"Den dataansvarlige kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor."

"Al kommunikation mellem den dataansvarlige og underdatabehandleren sker via databehandleren."

8. Overførsel til tredjelande eller internationale organisationer

"Ved overførsel til tredjelande er databehandleren og den dataansvarlige i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag."
Man kan læse mere om overførsel til tredjelande og gyldige overførselsgrundlag i vejledningen på Datatilsynets hjemmeside.

"Databehandleren må ikke overføre eller tillade overførsel af personoplysninger til udlandet."
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.

Kommunen kan i instruksen angive, at databehandleren ikke må overføre kommunens oplysninger til tredjelande.

12. Revision, herunder inspektion

"Databehandleren er forpligtet til uden ugrundet ophold at give den dataansvarlige de nødvendige oplysninger til, at den dataansvarlige til enhver tid kan sikre sig, at databehandleren overholder de krav, der følger af disse Bestemmelser."
Forpligtelsen til at give den dataansvarlige de nødvendige oplysninger følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra h, og er dermed en forpligtelse, som databehandleren må forudse i forbindelse med indgåelse af Hovedaftalen.

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.

"I forbindelse med revisioner, herunder inspektioner, har den dataansvarlige eller en repræsentant for den dataansvarlige ret til at få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at databehandleren overholder de krav, der følger af disse Bestemmelser."
Dette kan være en hjælp i forhold til aftaler med mindre databehandlere. Logningskrav vil ikke være et specifikt krav, der følger af Databeskyttelsesforordningen. 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.

"I tilfælde af at Datatilsynet ønsker at foretage en inspektion af de ovennævnte

foranstaltninger i henhold til denne aftale, forpligter databehandleren og databehandlerens underdatabehandlere sig til uden yderligere omkostninger for den dataansvarlige at stille tid og ressourcer til rådighed herfor."
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 underdatabehandleraftalerne.

14. Ikrafttræden og ophør

"Den dataansvarlige kan til enhver tid, med et forudgående varsel på mindst [XX dage], foretage ændringer i Bestemmelserne og instruksen, jf. bilag C. Ændringsprocessen og omkostningerne aftales skriftligt mellem den dataansvarlige og databehandleren i Hovedaftalen. Databehandleren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne."
Bestemmelserne og instruksen, jf. bilag C, kan til enhver tid ændres med et varsel, der angives nærmere i Bestemmelserne. 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.

"Misligholdelse og tvistigheder er reguleret i Hovedaftalen."
Ved kommunens eventuelle misligholdelse af Hovedaftalen, må databehandleren ikke tilbageholde kommunens data – dette kan man eventuelt sikre sig fremgår eksplicit af Hovedaftalen.

"Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen."

Bilag B. Underdatabehandlere

"Overlader databehandleren behandling af den dataansvarlige oplysninger til underdatabehandlere, er databehandleren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Bestemmelsernes pkt 7.1."

Bilag C, C.7. Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

"Erklæringen skal udarbejdes i overensstemmelse med [vælg enten "gældende, anerkendte branchestandarder på området" eller angiv den ønskede standard, f.eks. ISAE 3000, type X eller ISAE 3402]."
Her er 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 databehandleren aftale en frekvens for fremsendelse af en erklæring til kommunen. Det bør ligeledes aftales, hvornår første erklæring skal fremsendes.

Bilag C, C.8. Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

"Erklæringen skal udarbejdes i overensstemmelse med [vælg enten "gældende anerkendte branchestandarder på området" eller angiv den ønskede standard f.eks. ISAE 3000 type X eller ISAE 3402]."
Her er 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 databehandleren aftale en frekvens for fremsendelse af en erklæring til kommunen. Det bør ligeledes aftales, hvornår første erklæring skal fremsendes.

"[Bilag E – Den dataansvarlige it-sikkerhedsregulativ]"

"[Bilag F – Den dataansvarlige it-sikkerhedspolitik]"

"[Bilag G – Den dataansvarlige supplerende it-sikkerhedsregler]"

Udfyldelse af bilag D i Datatilsynets standard-kontraktsbestemmelser (engelsk)

I bilag D kan databehandleren og den dataansvarlige aftale regulering af andre forhold. Her følger den tekst, som i KL/KOMBIT skabelonen for databehandleraftaler var markeret med gult, fordi de var valgfri tilføjelser ønsket af kommuner. Hvor det fortsat er relevant, står der under flere krav tilhørende hjælpetekst fra det tidligere kommentarnotat, som er en hjælp til kommunen og ikke skal kopieres over i en databehandleraftale. Nedenstående tekst er ikke et krav til indholdet af en databehandleraftale i medfør af lovgivningen, i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen). Kommunen kan derfor undlade at medtage teksten markeret og stadig overholde lovgivningen. Teksten giver blot mulighed for, at kommuner kan tilføje krav til databehandleraftalen, der ligger udover det lovmæssigt krævede. I teksten er enkelte formuleringer markeret med [grønt]. Den grønne markering viser, at der her skal angives en ønsket tidsfrist eller en standard.

Preamble

"The data processor shall comply with principles and recommendations of ISO27001"
Det er vigtigt, at kommunen gør sig klart, om der alt afhængig af løsningens størrelse og kompleksitet f.eks. skal stilles krav om, at databehandleren er ISO-certificeret eller, om der skal stilles krav om, at databehandleren overholder alle eller dele af principper og anbefalinger i ISO27001.

Kommunen skal være opmærksom på, at der – hvis der stilles krav til databehandleren 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 databehandleren 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 databehandleren overholder.

Med baggrund i disse overvejelser skal kommunen beslutte, om der skal stilles krav til databehandleren om helt eller delvist at skulle efterleve principperne og anbefalingerne i ISO27001 og herefter eventuelt indsætte et krav herom. 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 Bestemmelserne ". 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 databehandleren, 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.

"The data processor shall process personal data in accordance with good data processing practice, cf. the rules and regulations for processing personal data that are applicable at any given time."

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

"The data processor is obligated to become familiar with the data controller's IT security regulations, IT security policy and to follow any related detailed IT security rules that are attached to the Clauses as Appendices [E-G]."

Hvis kommunen ønsker at forpligte databehandleren i forhold til kommunens sikkerhedspolitik, regulativ eller regler, skal kommunen træffe beslutning om, hvorvidt databehandleren skal gøre "sig bekendt med" disse politikker, regulativer eller regler og om databehandleren 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 databehandleren 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 databehandleren skal efterleve. Disse fremgår typisk af it-sikkerhedsreglerne.

3. The rights and obligations of the data controller

"The data controller is responsible for ensuring that the personal data that the data controller instructs the data processor to process may be processed by the data processor, including that the processing is necessary and legitimate in relation to the tasks of the data controller."

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

"The data controller is obligated to inform the data processor in case of any stricter IT security rules adopted by the data controller and in case of amendments to the data controller's IT security policy and IT security regulations, cf. Appendices [E-G]."

Ændring af bilag med sikkerhedsregler mv. vil være udtryk for en ændring af databehandleraftalen, som skal håndteres i henhold til pkt. 14 i Bestemmelserne.

4. The data processor acts according to instructions

"The data processor has the obligations that are imposed on a processor pursuant to the legislation, cf. section 2.2 of the Clauses."

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

"The data processor shall maintain records of the processing of personal data and records of all personal data breaches."

Databehandleren 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 Datatilsynets vejledning og på KL´s hjemmeside.

Kravet til databehandleren om at føre fortegnelse over alle brud på persondatasikkerheden er ikke et krav, som databehandleren 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.

"The data processor is obligated to provide information about the precise addresses where the data controller's personal data are processed, cf. Appendix C, C.5. The data processor must keep the data controller updated in case of any changes."

Af hensyn til kommunens mulighed for at kunne føre tilsyn med databehandlerens overholdelse af databehandleraftalen, bør kommunen dog stille krav om, at databehandleren angiver den præcise adresse, hvor kommunens personoplysninger behandles og opbevares.

"It is the data processor's responsibility to ensure that the data controller's instructions, cf. Appendix C, are sent to any subprocessors, cf. section 7."

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

5. Confidentiality

"The data processor is - during the duration of the Main Agreement and afterwards - subject to full obligation of confidentiality regarding all information that it becomes familiar with due to the cooperation. The Clauses entails that the confidentiality provisions in sections 152-152f of the Danish Criminal Code, cf. section 152a of the Danish Criminal Code, shall be applicable."

"The data processor and its employees are not permitted to obtain information of any kind that does not have significance for the fulfilment of the tasks of those in question."
Her er tale om, at databehandlerens 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 Bestemmelserne eller Hovedaftalen.

"The data processor may neither publicly nor to a third party communicate about personal data breaches, cf. section 10.1, without prior written agreement with the data controller regarding the content of such communication, unless the data processor has a legal obligation to provide such communication."
Emnet kan eventuelt behandles i Hovedaftalen.

6. Security of processing

"[At least once a year], the data processor shall review its internal security regulations and guidelines for processing personal data in order to ensure that the necessary security measures are continually observed, cf. section C, C.2."
Her er tale om, at databehandleren 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.

"The data processor is obligated to instruct its employees, who have access to or in another way carry out processing of the data controller's personal data, about the data processor's obligations including the provisions on obligation of confidentiality and secrecy, cf. section 5."

"The data processor is obligated to inform the data controller [immediately/without undue delay] about

(i) every request for transfer of personal data covered by the Clauses from an authority, unless informing the data controller is explicitly prohibited by law, for example, pursuant to rules intended to ensure the confidentiality of an investigation by a law-enforcing authority,

(ii) other lack of compliance with the data processor's and any sub-processor's obligations regardless of whether this takes place at the data processor or at a sub-processor. "

Databehandleren bliver i medfør af Databeskyttelsesforordningen pålagt en række nye forpligtelser, heriblandt kravet om at underrette den dataansvarlige 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'.
Man kan læse mere i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden.

Der vil kunne være situationer, hvor databehandleren ikke i første omgang kan udrede alle detaljer om det konkrete sikkerhedsbrud eller lignende, og databehandleren 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 databehandleren skal give sin underretning. Dette kan f.eks. være angivet i Hovedaftalens afsnit/bilag om samarbejdsorganisationen. Har kommunen ikke angivet sådanne særlige kontaktoplysninger, vil databehandleren skulle sende underretningen til kommunens centrale mail samt til den medarbejder hos kommunen, som har underskrevet og indgået aftalen med databehandleren.

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.

7. Use of sub-processors

"The data controller cannot refuse to approve the addition or replacement of a sub-processor unless there are specific reasoned grounds to do so."

"All communication between the data controller and the sub-processor shall take place via the data processor."

8. Transfer of data to third countries or international organisations

"In case of transfer to third countries, the data processor and the data controller are jointly responsible for ensuring that an adequate level of protection, e.g. an adequacy decision or appropriate safeguards, exists."
Man kan læse mere om overførsel til tredjelande og gyldige overførselsgrundlag i vejledningen på Datatilsynets hjemmeside.

"The data processor may not transfer or allow the transfer of personal data to other countries."
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.

Kommunen kan i instruksen angive, at databehandleren ikke må overføre kommunens oplysninger til tredjelande.

12. Audit and inspection

"The data processor is obligated to provide the data controller with the information required without undue delay so that the data controller can ensure that the data processor complies with the obligations resulting from these Clauses at any given time."
Forpligtelsen til at give den dataansvarlige de nødvendige oplysninger følger eksplicit af Databeskyttelsesforordningens artikel 28, stk. 3, litra h, og er dermed en forpligtelse, som databehandleren må forudse i forbindelse med indgåelse af Hovedaftalen.

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.

"In relation to audits, including inspections, the data controller, a representative of the data controller has the right to have documentation provided, including logs, and may ask questions, etc. in order to determine whether the data processor complies with the obligations that result from these Clauses."
Dette kan være en hjælp i forhold til aftaler med mindre databehandlere. Logningskrav vil ikke være et specifikt krav, der følger af Databeskyttelsesforordningen. 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.

"In case the Danish Data Protection Agency, wants to carry out an inspection of the measures mentioned above pursuant to these Clauses, the data processor and the

data processor's sub-processors obligate themselves to make time and resources available to do so at no further expense to the data controller."
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 underdatabehandleraftalerne.

14. Commencement and termination

"At any given time, with at least [XX days'] notice, the data controller may make amendments to the Clauses and instructions, cf. Appendix 3. The amendment process and the costs shall be agreed in writing between the data controller and the data processor in the Main Agreement. In case of such amendments, the data processor shall ensure, without undue delay, that the subprocessors are also obligated by the amendments."
Bestemmelserne og instruksen, jf. bilag C, kan til enhver tid ændres med et varsel, der angives nærmere i Bestemmelserne. 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.

"Breaches and disputes are regulated by the Main Agreement."
Ved kommunens eventuelle misligholdelse af Hovedaftalen, må databehandleren ikke tilbageholde kommunens data – dette kan man eventuelt sikre sig fremgår eksplicit af Hovedaftalen.

"Questions regarding compensation and insurance are regulated by the Main Agreement."

Appendix B.

"If the data processor entrusts the processing of the data controller's personal data to sub-processors, the data processor is responsible for entering into written (sub-)processor agreements with them, cf. section 7.1 of the Clauses."

Appendix C, C.7

"The statement shall be prepared in accordance with [choose either 'valid, recognized industry standards in the area' or state the standard required, for example, ISAE 3000, type X or ISAE 3402]"

Her er 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 databehandleren aftale en frekvens for fremsendelse af en erklæring til kommunen. Det bør ligeledes aftales, hvornår første erklæring skal fremsendes.

Appendix C, C.8

"The statement shall be prepared in accordance with [choose either 'valid, recognized industry standards in the area' or state the standard required, for example, ISAE 3000, type X or ISAE 3402]"

Her er 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 databehandleren aftale en frekvens for fremsendelse af en erklæring til kommunen. Det bør ligeledes aftales, hvornår første erklæring skal fremsendes.

"[Appendix E – The data controller's IT security regulations]"

"[Appendix F – The data controller's IT security policy]"

"[Appendix G – The data controller's supplementary IT security rules]"