

Databeskyttelsesrådets udtalelser (artikel 64)



Udtalelse 14/2019 om udkast til standardkontraktbestemmelser forelagt af den danske tilsynsmyndighed (artikel 28, stk. 8, i GDPR)

Vedtaget den 9. juli 2019

1 INDHOLDSFORTEGNELSE

2	Resumé af de faktiske omstændigheder	4
3	Vurdering	5
3.1	Databeskyttelsesrådets generelle ræsonnement vedrørende standardkontraktbestemmelserne	5
3.2	Analyse af udkastet til standardkontraktbestemmelser	5
3.2.1	Generel bemærkning vedrørende standardkontraktbestemmelserne som helhed	5
3.2.2	Baggrund for databehandleraftalen (afsnit 2 i standardkontraktbestemmelserne)	6
3.2.3	Den dataansvarliges forpligtelser og rettigheder (afsnit 3 i standardkontraktbestemmelserne)	6
3.2.4	Databehandleren handler efter instruks (afsnit 4 i standardkontraktbestemmelserne)	7
3.2.5	Fortrolighed (afsnit 5 i standardkontraktbestemmelserne)	7
3.2.6	Behandlingsikkerhed (afsnit 6 i standardkontraktbestemmelserne)	8
3.2.7	Anvendelse af underdatabehandlere (afsnit 7 i standardkontraktbestemmelserne)	9
3.2.8	Overførsel af oplysninger til tredjelande eller internationale organisationer (afsnit 8 i standardkontraktbestemmelserne)	11
3.2.9	Bistand til den dataansvarlige (afsnit 9 i standardkontraktbestemmelserne)	12
3.2.10	Underretning om brud på persondatasikkerheden (afsnit 10 i standardkontraktbestemmelserne)	14
3.2.11	Sletning og tilbagelevering af oplysninger (afsnit 11 i standardkontraktbestemmelserne)	14
3.2.12	Tilsyn og revision (afsnit 12 i standardkontraktbestemmelserne)	15
3.2.13	Parternes aftaler om andre forhold (afsnit 13 i standardkontraktbestemmelserne)	16
3.2.14	Ikrafttræden og ophør (afsnit 14 i standardkontraktbestemmelserne)	16
3.2.15	Bilag A	16
4	Konklusioner	16
5	Afsluttende bemærkninger	17

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 28, stk. 8, artikel 63 og artikel 64, stk. 1, litra d), og artikel 64, stk. 3-8, i Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter "GDPR"),

under henvisning til EØS-aftalen, særligt bilag XI og protokol 37 til EØS-aftalen, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018¹,

under henvisning til artikel 10 og artikel 22 i forretningsordenen af 25. maj 2018, og

ud fra følgende betragtninger:

1) Det Europæiske Databeskyttelsesråd (herefter "Databeskyttelsesrådet") har som sin vigtigste opgave at sikre ensartet anvendelse af GDPR i hele Det Europæiske Økonomiske Samarbejdsområde. Med henblik herpå følger det af artikel 64, stk. 1, litra d), i GDPR, at Databeskyttelsesrådet afgiver en udtalelse, når en tilsynsmyndighed har til hensigt at vedtage standardkontraktbestemmelser i henhold til artikel 28, stk. 8, i GDPR. Formålet med denne udtalelse er derfor at bidrage til en harmoniseret tilgang vedrørende grænseoverskridende behandling eller behandling, som kan påvirke den frie udveksling af personoplysninger eller fysiske personer i hele Det Europæiske Økonomiske Samarbejdsområde, og en ensartet gennemførelse af GDPR's specifikke bestemmelser.

2) I forbindelse med forholdet mellem en dataansvarlig og en databehandler eller databehandlere fastsætter GDPR i artikel 28 med hensyn til behandling af personoplysninger en række bestemmelser med hensyn til indgåelse af en specifik kontrakt mellem de involverede parter og obligatoriske bestemmelser, der bør indgå deri.

3) I henhold til artikel 28, stk. 3, i GDPR skal en databehandlers behandling være *reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige*, og som fastsætter en række specifikke aspekter med henblik på at regulere kontraktforholdet mellem parterne. Disse omfatter bl.a. genstanden for og varigheden af behandlingen, dens karakter og formål, typen af personoplysninger og kategorierne af registrerede.

4) I henhold til artikel 28, stk. 6, i GDPR, kan kontrakten eller det andet retlige dokument, der er omhandlet i artikel 28, stk. 3 og 4, i GDPR, helt eller delvis baseres på standardkontraktbestemmelser, uden at det berører en individuel kontrakt mellem den dataansvarlige og databehandleren. Disse standardkontraktbestemmelser skal vedtages i de tilfælde, der er omhandlet i stk. 3 og 4.

5) Endvidere fastsætter artikel 28, stk. 8, i GDPR, at en tilsynsmyndighed kan vedtage en række standardkontraktbestemmelser i overensstemmelse med sammenhængsmekanismen, der er omhandlet i artikel 63. Dette indebærer, at tilsynsmyndighederne skal samarbejde med andre medlemmer af Databeskyttelsesrådet og, hvis det er relevant, med Europa-Kommissionen gennem sammenhængsmekanismen. Tilsynsmyndigheder skal i henhold til artikel 64, stk. 1, litra d), sende Databeskyttelsesrådet et udkast til afgørelse med henblik på at vedtage

¹ Henvisninger til "medlemsstater" i denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater".

standardkontraktbestemmelser i henhold til artikel 28, stk. 8. I denne forbindelse skal Databeskyttelsesrådet i henhold til artikel 64, stk. 3, afgive udtalelse om spørgsmålet, hvis det ikke allerede har gjort dette.

6) Vedtagne standardkontraktbestemmelser udgør en række garantier, der skal anvendes, som de er vedtaget, da de skal beskytte registrerede og begrænse specifikke risici i forbindelse med de grundlæggende principper for databeskyttelse —

VEDTAGET FØLGENDE UDTALELSE:

2 RESUMÉ AF DE FAKTISKE OMSTÆNDIGHEDER

1. Den kompetente tilsynsmyndighed i Danmark har forelagt sit udkast til standardkontraktbestemmelser for Databeskyttelsesrådet via IMI-systemet med anmodning om en udtalelse fra Databeskyttelsesrådet i henhold til artikel 64, stk. 1, litra d), med henblik på en ensartet tilgang på EU-plan. Beslutningen om, at sagen var komplet, blev truffet den 4. april 2019. Databeskyttelsesrådets sekretariat udsendte på formandens vegne sagen til alle medlemmer den 4. april.
2. Databeskyttelsesrådet har modtaget udkastet til standardkontraktbestemmelser fra den danske tilsynsmyndighed² sammen med en skrivelse, hvori standardkontraktbestemmelsernes struktur forklares. Disse to dokumenter blev af den danske tilsynsmyndighed stillet til rådighed i en engelsk version. Databeskyttelsesrådet afgiver herved udtalelse om den engelske version af dokumentet, selv om Databeskyttelsesrådet bemærker, at standardkontraktbestemmelserne også er tilgængelige på dansk på den danske tilsynsmyndigheds websted. Den danske tilsynsmyndighed tager videst muligt hensyn til Databeskyttelsesrådets udtalelse.
3. I overensstemmelse med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden³ har formanden på grund af det foreliggende spørgsmåls kompleksitet besluttet at forlænge den oprindelige frist for vedtagelse af en udtalelse på otte uger med yderligere seks uger (indtil den 9. juli 2019).

² "Databehandlersaftale" er det udtryk, som den danske tilsynsmyndighed har anvendt om standardkontraktbestemmelser i det dokument, der er forelagt for Databeskyttelsesrådet.

³ Version 2, sidst ændret og vedtaget den 23. november 2018.

3 VURDERING

3.1 Databeskyttelsesrådets generelle ræsonnement vedrørende standardkontraktbestemmelserne

4. Alle standardkontraktbestemmelser, der forelægges Databeskyttelsesrådet, skal yderligere præcisere bestemmelserne i artikel 28 i GDPR. Databeskyttelsesrådets udtalelse har til formål at sikre sammenhæng og en korrekt anvendelse af artikel 28 i GDPR med hensyn til det forelagte udkast til bestemmelser, der kunne tjene som standardkontraktbestemmelser i overensstemmelse med artikel 28, stk. 8, i GDPR.
5. Databeskyttelsesrådet bemærker, at det dokument, der er forelagt Databeskyttelsesrådet, er et udkast til standardkontraktbestemmelser, der indeholder to dele:
 - 1) en generel del, der indeholder generelle bestemmelser, der skal anvendes, som de er vedtaget, og
 - 2) en specifik del, der skal udfyldes af parterne, med hensyn til den specifikke behandling, som kontrakten har til formål at regulere.
6. Desuden har den danske tilsynsmyndighed forklaret i sin skrivelse, at de afsnit i standardkontraktbestemmelserne, der er markeret med fed, er obligatoriske og udgør minimumskravene i en kontrakt i henhold til artikel 28 i GDPR. De resterende afsnit er frivillige og kan medtages i standardkontraktbestemmelserne efter parternes ønske, selv om de er hensigtsmæssige at have med.
7. Databeskyttelsesrådet er af den opfattelse, at afsnit, som blot gentager bestemmelserne i artikel 28, stk. 3 og 4, er utilstrækkelige til at udgøre standardkontraktbestemmelser. Databeskyttelsesrådet har derfor besluttet at analysere dokumentet i dets helhed, herunder bilagene. Efter Databeskyttelsesrådets opfattelse bør en kontrakt i henhold til artikel 28 i GDPR yderligere fastsætte og præcisere, hvordan bestemmelserne i artikel 28, stk. 3 og 4, vil blive opfyldt. Det er i dette lys, at de standardkontraktbestemmelser, der er forelagt Databeskyttelsesrådet, analyseres.
8. Når der i denne udtalelse ikke er anført noget vedrørende et eller flere afsnit i de standardkontraktbestemmelser, som den danske tilsynsmyndighed har forelagt, betyder det, at Databeskyttelsesrådet ikke anmoder den danske tilsynsmyndighed om at træffe yderligere foranstaltninger med hensyn til dette specifikke afsnit. Afsnit 6.4, 9.3 og 14.3 i de danske standardkontraktbestemmelser kræves ikke i artikel 28 og vedrører kommercielle aspekter, og Databeskyttelsesrådet anser derfor ikke disse afsnit for at være en del af standardkontraktbestemmelserne. Det er op til parterne, om og hvordan de indgår en aftale.

3.2 Analyse af udkastet til standardkontraktbestemmelser

3.2.1 Generel bemærkning vedrørende standardkontraktbestemmelserne som helhed

9. Databeskyttelsesrådet er af den opfattelse, at hvis standardkontraktbestemmelserne kun indeholdt de dele, der er markeret med fed, ville de ikke være tilstrækkelige som standardkontraktbestemmelser, da nogle af de dele, der ikke er markeret med fed, vedrører obligatoriske bestemmelser i henhold til artikel 28, stk. 3, i GDPR. Databeskyttelsesrådet anbefaler derfor, at den danske tilsynsmyndighed undgår denne sondring ved klart at anføre enten i afsnittene eller i et separat dokument med en vejledning i anvendelsen af disse afsnit, at alle afsnit i

standardkontraktbestemmelserne sammen med bilagene bør medtages i de standardkontraktbestemmelser, der aftales mellem parterne.

10. Desuden minder Databeskyttelsesrådet om, at muligheden for at bruge standardkontraktbestemmelser, der er vedtaget af en tilsynsmyndighed, ikke udelukker muligheden for, at parterne medtager andre bestemmelser eller yderligere garantier, såfremt de hverken direkte eller indirekte er i strid med de standardkontraktbestemmelser, der er vedtaget, eller berører de registreredes grundlæggende rettigheder eller frihedsrettigheder. Såfremt standardkontraktbestemmelserne ændres, vil parterne endvidere ikke længere kunne anses for at have gennemført vedtagne standardkontraktbestemmelser.
11. Databeskyttelsesrådet bemærker, at formuleringen af flere afsnit i standardkontraktbestemmelserne ikke er i overensstemmelse med de relevante bestemmelser i GDPR. Databeskyttelsesrådet har anført dette i sin udtalelse nedenfor og anbefaler, at den danske tilsynsmyndighed bringer formuleringen af disse afsnit i overensstemmelse med de relevante bestemmelser i GDPR.

3.2.2 Baggrund for databehandleraftalen (afsnit 2 i standardkontraktbestemmelserne)

12. Vedrørende **afsnit 2.3** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at forholdet mellem databehandleraftalen og "hovedaftalen" kunne være mere fleksibelt. Der kan være tilfælde, hvor standardkontraktbestemmelserne er en særskilt dokumentdel af hovedaftalen, og som sådan er der ikke behov for særskilte standardkontraktbestemmelser. Der kan også være situationer, hvor den databehandling, der reguleres af standardkontraktbestemmelserne, ikke er en del af hovedaftalen. Databeskyttelsesrådet opfordrer derfor den danske tilsynsmyndighed til at omformulere dette afsnit, således at det afspejler denne fleksibilitet. Denne specifikke ændring skal gennemføres i hvert tilfælde, hvor standardkontraktbestemmelserne henviser til hovedaftalen.
13. Vedrørende første punktum i **afsnit 2.4** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at databehandleraftalen i nogle situationer kunne blive opsagt inden "hovedaftalen". Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed tilføjer i slutningen af det første punktum, at aftalen "*i princippet ikke [kan] opsiges særskilt, undtagen hvis databehandlingen afsluttes inden opsigelsen af hovedaftalen, eller hvis andre vilkår for en særskilt opsigelse af databehandleraftalen, jf. opsigelsesbestemmelserne, er opfyldt (jf. ligeledes anbefaling vedrørende afsnit 14.4 nedenfor)*".

3.2.3 Den dataansvarliges forpligtelser og rettigheder (afsnit 3 i standardkontraktbestemmelserne)

14. Vedrørende **afsnit 3.1** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at formuleringen "*har overfor omverdenen [...] ansvaret*" er vildledende. Den kunne faktisk forstås således, at forpligtelser over for registrerede eller andre interessenter udelukkende er pålagt den dataansvarlige. Databeskyttelsesrådet er af den opfattelse, at dette afsnit ville blive klarere, hvis der henvises til artikel 24 i GDPR og ansvarlighedsprincippet heri. Databeskyttelsesrådet anbefaler derfor, at den danske tilsynsmyndighed medtager en sådan henvisning.
15. Endvidere vedrørende afsnit 3.1 ville det være bedre generelt at henvise til den gældende lovgivning på databeskyttelsesområdet, hvis det er relevant, i stedet for til en specifik lov. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed ændrer henvisningen til databeskyttelsesloven. Endelig foreslår Databeskyttelsesrådet, at ordene "indenfor rammerne af" erstattes med "i overensstemmelse med".

Databeskyttelsesrådet foreslår derfor følgende formulering som et eksempel:

"1. Den dataansvarlige har som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (jf. artikel 24 i GDPR), EU's eller medlemsstaternes gældende databeskyttelsesbestemmelser () og denne databehandleraftale."

16. Vedrørende **afsnit 3.2** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at dette afsnit er uklart, da den dataansvarlige allerede har defineret formålene og hjælpemidlerne i forbindelse med den behandlingsaktivitet, der er omfattet af standardkontraktbestemmelserne. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed ændrer dette afsnit på følgende måde:
17. *"Den dataansvarlige har ret og forpligtelse til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling"*.
18. Vedrørende **afsnit 3.3** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at dets betydning er uklar. Databeskyttelsesrådet antager, at idéen bag dette afsnit er at sikre, at de behandlingsaktiviteter, hvortil den dataansvarlige ønsker at gøre brug af en databehandler, har et retsgrundlag. Hvis det er tilfældet, anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed præciserer afsnittet i overensstemmelse hermed.

Endelig bemærker Databeskyttelsesrådet, at formuleringen "behandlingen af personoplysninger" er anvendt i afsnit 3.1 i standardkontraktbestemmelserne. I afsnit 3.3 i standardkontraktbestemmelserne er ordet "behandling" anvendt. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed anvender den samme terminologi for at undgå forvirring.

Som et eksempel foreslår Databeskyttelsesrådet derfor følgende formulering:

"3. Den dataansvarlige er blandt andet ansvarlig for, at den behandling af personoplysninger, som databehandleren instrueres i at foretage, har et retsgrundlag."

3.2.4 Databehandleren handler efter instruks (afsnit 4 i standardkontraktbestemmelserne)

19. Vedrørende **afsnit 4.1** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at der bør henvises til bilag A og C, da den dataansvarliges instruks er yderligere præciseret heri. Databeskyttelsesrådet er af den opfattelse, at den dataansvarlige kan give yderligere instruks i hele kontraktperioden, men at en sådan instruks altid skal være dokumenteret.

Endvidere bemærker Databeskyttelsesrådet, at dette afsnit er inspireret af artikel 28, stk. 3, litra a), i GDPR. Databeskyttelsesrådet vil derfor opfordre den danske tilsynsmyndighed til at anvende samme formulering som i GDPR.

20. Vedrørende **afsnit 4.2** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at parterne bør fastsætte konsekvenser og anviser løsninger i tilfælde af en ulovlig instruks.

3.2.5 Fortrolighed (afsnit 5 i standardkontraktbestemmelserne)

21. Databeskyttelsesrådet forstår afsnit 5 i standardkontraktbestemmelserne som en specificering af artikel 28, stk. 3, litra b), i GDPR, hvorefter databehandleren "*sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt*".

22. Vedrørende **afsnit 5.1** i standardkontraktbestemmelserne forstås ordet "aktuelt" af Databeskyttelsesrådet som nødvendigheden af at overvåge statussen som "autoriserede personer". Endvidere er det uklart for Databeskyttelsesrådet, hvem der giver autorisationen til disse personer, navnlig da adgangen til personoplysninger skal gives på "need-to-know"-basis.
23. Vedrørende **afsnit 5.2** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at dette afsnit vedrører princippet om adgang til personoplysningerne på "need-to-know"-basis. Databeskyttelsesrådet er af den opfattelse, at afsnit 5.1 og 5.2 i standardkontraktbestemmelserne kan kombineres på følgende måde:
- "Det er databehandlerens ansvar kun at give personer under dennes tilsyn adgang til de personoplysninger, der behandles på vegne af den dataansvarlige, på need-to-know-basis; disse personer har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. Listen over personer, som har fået adgang, bør gennemgås løbende. På grundlag af denne gennemgang kan adgangen til personoplysninger tilbagetrækkes, og i dette tilfælde er personoplysninger ikke længere tilgængelige for disse personer."*
24. Vedrørende **afsnit 5.3** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at det er omfattet af den ovenfor foreslåede formulering, og at afsnit 5.3 derfor kan udelades.
25. Vedrørende **afsnit 5.4** i standardkontraktbestemmelserne anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed lader formuleringen "kunne" udgå, eftersom databehandleren skal påvise overholdelse af fortrolighedskravene. Endvidere opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til at vedtage en bredere formulering, når der henvises til "*medarbejdere*", da der kan være andre personer end medarbejdere, der behandler personoplysninger under databehandlerens tilsyn. En formulering som "*personer under databehandlerens tilsyn*" eller "*personer ansat direkte eller indirekte af*" ville være mere hensigtsmæssig.

3.2.6 Behandlingssikkerhed (afsnit 6 i standardkontraktbestemmelserne)

26. Vedrørende **afsnit 6.1** i standardkontraktbestemmelserne anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed erstatter ordene "*under hensyntagen til det aktuelle niveau*" i begyndelsen af sætningen med ordene "*under hensyntagen til det aktuelle tekniske niveau*", som er formuleringen i artikel 32, stk. 1, i GDPR. Denne specifikke formulering anvendes i GDPR for at sikre, at sikkerhedsniveauet i forbindelse med behandlingen af personoplysninger altid er i overensstemmelse med den seneste teknologiske udvikling. Den formulering, som den danske tilsynsmyndighed har foreslået, henviser til et aktuelt niveau, som ikke vil være det aktuelle tekniske niveau om to år.
27. Vedrørende **afsnit 6.2** i standardkontraktbestemmelserne forstår Databeskyttelsesrådet, at dette afsnit vedrører artikel 28, stk. 3, litra c), i GDPR, og at afsnit 9.2 vedrører artikel 28, stk. 3, litra f), i GDPR. Sondringen mellem de to afsnit og databehandlerens forskellige opgaver er imidlertid ikke særlig klar. Databeskyttelsesrådet minder om, at artikel 28, stk. 3, litra f), i GDPR fastsætter, at databehandleren bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 i GDPR under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren.

Databeskyttelsesrådet er af den opfattelse, at den "risikovurdering", der er henvist til i første punktum i afsnit 6.2, skal foretages af de behandlingsaktiviteter, som den dataansvarlige overdrager til databehandleren. Den dataansvarlige bør derfor give databehandleren alle de oplysninger, der er nødvendige, for at databehandleren kan overholde artikel 28, stk. 3, litra c) og f), i GDPR. Databeskyttelsesrådet vil gerne understrege, at den dataansvarlige herved ikke fritages for ansvaret

for at være i overensstemmelse med sine egne forpligtelser i henhold til artikel 25, 32 eller 35-36 i GDPR.

Desuden bør slutningen af første punktum i afsnit 6.2 omformuleres for i højere grad at være i overensstemmelse med afsnit 9.2 og bilag C2, da det ikke er klart for Databeskyttelsesrådet, hvordan formuleringen "*herefter gennemføre foranstaltninger for at imødegå identificerede risici*" i afsnit 6.2 er relateret til afsnit 9.2 og bilag C2. Databeskyttelsesrådet har bemærket, at afsnit 9.2.a og bilag C2 behandler emnet risikovurdering, men ikke på samme måde som afsnit 6.2. I henhold til afsnit 6.2 skal risikovurderingen foretages af databehandleren, mens risikovurderingen i henhold til afsnit 9.2 og bilag C2 skal foretages af den dataansvarlige. Bilag C2 fastsætter desuden, at databehandleren skal gennemføre foranstaltninger, som er aftalt med den dataansvarlige.

Vedrørende bilag C2 er Databeskyttelsesrådet af den opfattelse, at formuleringen "*Sikkerhedsniveauet skal afspejle*" kunne ændres til "*Sikkerhedsniveauet skal tage højde for*". Med hensyn til de elementer, der skal tages højde for, nævner artikel 32, stk. 1, og artikel 32, stk. 2, i GDPR behandlingens karakter, omfang, sammenhæng og formål samt risikoen for fysiske personers rettigheder og frihedsrettigheder. Disse kunne være elementer, der kunne nævnes med henblik på at præcisere, hvad der forventes i forbindelse med "*Beskriv elementer, der er afgørende for sikkerhedsniveauet*".

Databeskyttelsesrådet anbefaler derfor, at den danske tilsynsmyndighed præciserer og tilpasser afsnit 6.2 og 9.2 og bilag C2.

3.2.7 Anvendelse af underdatabehandlere (afsnit 7 i standardkontraktbestemmelserne)

28. Vedrørende **afsnit 7.2 og 7.5** i standardkontraktbestemmelserne anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed erstatter ordet "godkendelse" ("consent") med "godkendelse" ("authorisation"), da dette er formuleringen i artikel 28, stk. 2, i GDPR.

Endvidere er Databeskyttelsesrådet af den opfattelse, at det ville være mere praktisk at give valgmuligheder i dette afsnit på følgende måde:

"2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af denne databehandleraftale uden forudgående [valgmulighed 1] specifik godkendelse fra den dataansvarlige / [valgmulighed 2] eller generel skriftlig godkendelse fra den dataansvarlige."

29. Vedrørende **afsnit 7.3 og 7.4** i standardkontraktbestemmelserne finder Databeskyttelsesrådet det vigtigt at tilføje, at den liste over underdatabehandlere, der er godkendt af den dataansvarlige på tidspunktet for kontraktens underskrivelse, bør vedhæftes som bilag til standardkontraktbestemmelserne, hvad enten det er på grundlag af en generel eller en specifik godkendelse. Formålet med denne liste er at sikre, at den dataansvarlige selv i tilfælde af en generel godkendelse forbliver underrettet om listen over underdatabehandlere samt yderligere ændringer. Databeskyttelsesrådet anbefaler, at det præciseres i standardkontraktbestemmelsen, at listen over underdatabehandlere i bilag B2 skal fremlægges både i tilfælde af en generel og en specifik forudgående godkendelse.

Endvidere er der i bilag B1 til standardkontraktbestemmelserne eksempler på afsnit, som parterne kan vælge imellem. Databeskyttelsesrådet finder imidlertid, at det ville være bedre at medtage sådanne afsnit i selve standardkontraktbestemmelserne i stedet for i bilagene.

Endelig med hensyn til den generelle forudgående godkendelse er Databeskyttelsesrådet af den opfattelse, at eventuelle betingelser, som databehandleren måtte fastsætte for den dataansvarliges

mulighed for at gøre indsigelse mod ændringer af underdatabehandlere, skal gøre det muligt for den dataansvarlige i praksis at udøve sin valgfrihed og sætte den dataansvarlige i stand til fortsat at udøve kontrol over personoplysningerne. Dette indebærer også, at den dataansvarlige bør have tilstrækkelig tid til at gøre indsigelse mod en sådan ændring.

Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed omformulerer afsnit 7.3, således at der inden for afsnittet gives valgmuligheder, som kan vælges af parterne inden for standardkontraktbestemmelserne, og indholdet af afsnit 7.4 og 7.5 indarbejdes i afsnit 7.3.

Afsnit 7.3 kunne formuleres på følgende måde:

"3. I tilfælde af generel skriftlig godkendelse skal databehandleren skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere inden mindst [angiv tidsrum] og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer før anvendelsen af en eventuel underdatabehandler. Længere tidsrum for forudgående underretning i forbindelse med underdatabehandleres specifikke tjenester kan fastsættes i bilag B. Listen over underdatabehandlere, der allerede er godkendt af den dataansvarlige, findes i bilag B."

I tilfælde af specifik forudgående godkendelse skal databehandleren kun gøre brug af underdatabehandler med den dataansvarliges forudgående godkendelse. Databehandleren skal indgive anmodningen om specifik godkendelse mindst [angiv tidsrum] før anvendelsen af en eventuel underdatabehandler. Listen over underdatabehandlere, der allerede er godkendt af den dataansvarlige, findes i bilag B."

Da valgmuligheden gives i selve udkastet til standardkontraktbestemmelser, kan bilag B1 udelades. Desuden anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed tilføjer en mulighed for at fastsætte et længere tidsrum for forudgående underretning i bilag B.

30. Vedrørende **afsnit 7.6** i standardkontraktbestemmelserne forstår Databeskyttelsesrådet dette afsnit som en henvisning til artikel 28, stk. 4, i GDPR. Som tidligere nævnt ville det være bedre at henvise til den nøjagtige formulering af teksten i GDPR for at undgå forvirring.

Vedrørende **afsnit 7.8** i standardkontraktbestemmelserne vil Databeskyttelsesrådet gerne understrege, at dets indhold ikke kræves i artikel 28 i GDPR. Databeskyttelsesrådet er af den opfattelse, at ordet "tredjemand" er uklart. Hvis hensigten er at indføre en "tredjepartsrettighed" for den dataansvarlige inden for kontrakten mellem databehandleren og underdatabehandleren, bør dette præciseres.

Efter Databeskyttelsesrådets opfattelse er der som sådan en merværdi i at have et sådant afsnit som en del af standardkontraktbestemmelser. Det sikrer faktisk den dataansvarliges rettigheder, herunder ansvar. Databeskyttelsesrådet opfordrer derfor den danske tilsynsmyndighed til at gøre det mere klart, at hensigten er af indføre en tredjepartsrettighed for den dataansvarlige. Dette ville f.eks. indebære, at underdatabehandleren ville acceptere at være ansvarlig over for den dataansvarlige i tilfælde af den oprindelige databehandleres konkurs, eller muligheden for, at den dataansvarlige direkte kan pålægge underdatabehandleren at tilbagelevere oplysningerne.

31. Vedrørende **afsnit 7.9** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at det er vigtigt at henvise til den registreredes rettigheder. Denne henvisning kan formuleres på følgende måde: "*Dette berører ikke de registreredes rettigheder i henhold til GDPR — navnlig rettighederne i artikel 79 og 82 i GDPR — i forhold til den dataansvarlige og databehandleren, herunder underdatabehandleren.*"

3.2.8 Overførsel af oplysninger til tredjelande eller internationale organisationer (afsnit 8 i standardkontraktbestemmelserne)

32. Vedrørende afsnittets titel er Databeskyttelsesrådet af den opfattelse, at det bør præciseres, at ordet "tredjelande" henviser til lande uden for EØS og ikke uden for Danmark. Databeskyttelsesrådet opfordrer den danske tilsynsmyndighed til at præcisere dette.
33. Databeskyttelsesrådet er af den opfattelse, at afsnit 8 bør præcisere, at den dataansvarlige skal afgøre, om en overførsel er tilladt i henhold til kontrakten, eller om den bør være forbudt. Databeskyttelsesrådet anbefaler den danske tilsynsmyndighed, at dette gøres klart i standardkontraktbestemmelserne, og opfordrer den til at præcisere dette i bilag C5.
34. Vedrørende **afsnit 8.1** i standardkontraktbestemmelserne bemærker Databeskyttelsesrådet, at den danske tilsynsmyndighed har tilføjet en parentes efter ordet "overførsel" med ordlyden "(overladelse, videregivelse samt intern anvendelse)". Databeskyttelsesrådet er i tvivl om, hvorvidt dette har til formål at give en definition af ordet "overførsel". Hvis dette er hensigten er Databeskyttelsesrådet af den opfattelse, at da GDPR ikke indeholder en sådan definition af begrebet overførsel, er det bedre at udelade disse ord i parentesen.

Endelig anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed indleder sit afsnit 8.1 med tilføjelsen "*I overensstemmelse med kapitel V i GDPR ...*" Databeskyttelsesrådet minder således om, at alle bestemmelser i kapitel V i GDPR skal overholdes i forbindelse med enhver overførsel uden for EU. Det bør præciseres i afsnit 8, at disse standardkontraktbestemmelser ikke kan forstås som standardkontraktbestemmelser, der opfylder kravene i artikel 46 i GDPR, og derfor ikke kan anvendes som et værktøj til at foretage internationale overførsler som omhandlet i kapitel V i GDPR. Dette kunne desuden afspejles i afsnit 8's titel, som ellers kan give indtryk af, at overførsler kan foretages på grundlag af disse standardkontraktbestemmelser.

35. Vedrørende **afsnit 8.2** i standardkontraktbestemmelserne har Databeskyttelsesrådet en række bemærkninger.

For det første opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til i begyndelsen af punktummet at tilføje ordet "dokumenterede" inden "instruks" for at skabe retssikkerhed og sikre overensstemmelse med artikel 28, stk. 3, litra a), i GDPR og ændre ordet "godkendelse" ("*approval*") til "godkendelse" ("*authorisation*") i overensstemmelse med ordvalget i artikel 28 i GDPR. Begyndelsen af punktummet bør have ordlyden "*Uden den dataansvarliges dokumenterede instruks eller godkendelse*".

For det andet vedrørende afsnit 8.2.a kunne ordet "*videregive*" skabe forvirring i forhold til begrebet overførsel. Desuden kan personoplysninger overføres til en dataansvarlig (som allerede nævnt i afsnittet), men også til en databehandler i et tredjeland. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed formulerer afsnit 8.2.a på følgende måde: "*overføre personoplysningerne til en dataansvarlig eller en databehandler i et tredjeland eller i en international organisation*".

For det tredje vedrørende afsnit 8.2.b kunne ordet "overlade" ligeledes skabe forvirring i forhold til begrebet overførsel. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed erstatter ordet "overlade" med ordet "overføre".

Endelig vedrørende afsnit 8.2.c er det uklart for Databeskyttelsesrådet, hvad betydningen af ordet "afdelinger" er. Databeskyttelsesrådet opfordrer den danske tilsynsmyndighed til at erstatte afsnit 8.2.c med følgende: "*lade oplysningerne behandle af databehandleren uden for EØS*".

36. Vedrørende **afsnit 8.3** i standardkontraktbestemmelserne forstår Databeskyttelsesrådet, at det er en måde til at dokumentere den dataansvarliges instruks i bilag C5. Som allerede anført i begyndelsen af denne udtalelse betragter Databeskyttelsesrådet bilagene som obligatoriske. Databeskyttelsesrådet er imidlertid af den opfattelse, at det kunne være hensigtsmæssigt at nævne valget af overførselsværktøj, ud over instruksen, da det bidrager til at påvise parternes overholdelse af kapitel V i GDPR. Databeskyttelsesrådet opfordrer den danske tilsynsmyndighed til at ændre afsnit 8.3 på følgende måde:
37. *"Den dataansvarliges instruks vedrørende overførsler af personoplysninger til et tredjeland, herunder det eventuelle overførselsværktøj, som de er baseret på, vil fremgå af bilag C5 til denne databehandleraftale. Den samme procedure finder anvendelse på godkendelsen af overførsler af personoplysninger til et tredjeland."*

3.2.9 Bistand til den dataansvarlige (afsnit 9 i standardkontraktbestemmelserne)

38. **Afsnit 9.1** i standardkontraktbestemmelserne afspejler indholdet af artikel 28, stk. 3, litra e), i GDPR. Databehandlerens forpligtelse i henhold til dette afsnit er at bistå den dataansvarlige med at besvare anmodninger om udøvelse af de registreredes rettigheder. Bistanden kan antage forskellige former. Databeskyttelsesrådet er af den opfattelse, at standardkontraktbestemmelserne skal indeholde oplysninger om den måde, hvorpå databehandleren skal yde bistand, og ikke kun listen over mulige rettigheder, der kan udøves.

Standardkontraktbestemmelserne bør navnlig fastsætte de skridt, der skal tages af databehandleren i tilfælde af, at denne direkte modtager en anmodning fra en registreret vedrørende udøvelsen af den pågældendes rettigheder. Det skal eksempelvis klart fremgå af aftalen i et sådant tilfælde, om databehandleren ikke må have nogen kontakt med de registrerede, og hvordan databehandleren skal underrette den dataansvarlige hvad angår registreredes rettigheder (f.eks. fremsende anmodningen til den dataansvarlige inden for en angiven frist eller andre passende foranstaltninger). I dette tilfælde er bistanden kun i form af en udveksling af oplysninger mellem den dataansvarlige og databehandleren. Et andet scenarie kunne være, at den dataansvarlige instruerer databehandleren om at besvare registreredes anmodninger efter instruks. En anden mulighed kunne være, at databehandleren foretager de tekniske gennemførelser med hensyn til registreredes rettigheder efter instruks fra den dataansvarlige. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed overvejer muligheden for at medtage følgende sætning i afsnit 9.1 i standardkontraktbestemmelserne:

"Parterne fastsætter i bilag C passende tekniske og organisatoriske foranstaltninger, ved hjælp af hvilke databehandleren skal bistå den dataansvarlige, samt rækkevidden og omfanget af den bistand, der er påkrævet. Dette gælder for de forpligtelser, der følger af afsnit 9.1 og 9.2 i databehandleraftalen."

Der bør medtages et nyt punkt i bilag C med henblik på at præcisere de tekniske og organisatoriske foranstaltninger.

Vedrørende afsnit 9.1.a og 9.1.b anbefaler Databeskyttelsesrådet endvidere, at den danske tilsynsmyndighed anvender ordene "*ret til at blive underrettet*" i stedet for ordet "*oplysningspligt*", på følgende måde: "*Ret til at blive underrettet ved indsamling af personoplysninger hos den registrerede*" — "*Ret til at blive underrettet, hvis personoplysninger ikke er indsamlet hos den registrerede.*"

Vedrørende afsnit 9.1.j ville Databeskyttelsesrådet foretrække at have den nøjagtige formulering i GDPR. Databeskyttelsesrådet opfordrer derfor den danske tilsynsmyndighed til at omformulere

afsnittet på følgende måde: "*ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering*".

39. **Afsnit 9.2** i standardkontraktbestemmelserne afspejler indholdet af artikel 28, stk. 3, litra f), i GDPR. Databeskyttelsesrådet anbefaler derfor, at "*oplysninger, der er tilgængelige*" ("*data made available*") erstattes med "*oplysninger, der er tilgængelige*" ("*information available*"). Databehandlerens forpligtelse i henhold til dette afsnit er at bistå den dataansvarlige med opfyldelsen af de retlige forpligtelser vedrørende sikkerhed, konsekvensanalyse vedrørende databeskyttelse og forudgående høring af tilsynsmyndigheder. I denne forbindelse er Databeskyttelsesrådet ligeledes af den opfattelse, at standardkontraktbestemmelserne skal indeholde oplysninger om den måde, hvorpå databehandleren skal yde bistand til den dataansvarlige.

Som allerede anført i punkt 27 i denne udtalelse bør den danske tilsynsmyndighed præcisere forholdet mellem afsnit 9.2 og afsnit 6 om behandlingssikkerhed. Databeskyttelsesrådet forstår forholdet mellem disse to afsnit således, at afsnit 6 henviser til artikel 28, stk. 3, litra c), i GDPR, og afsnit 9.2 til artikel 28, stk. 3, litra f). Afsnit 9.2.a og i et vist omfang afsnit 9.2.b er således forpligtelser, som i alle tilfælde skal opfyldes af databehandleren i henhold til GDPR. Dette følger af artikel 32, stk. 1, og artikel 33, stk. 2, i GDPR. For at afsnit 9.2.a kan bibeholdes, ville det være nødvendigt at foretage en række yderligere tilpasninger til artikel 32, stk. 1, i GDPR. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed gør det klart, at risikoen ville være risikoen "for fysiske personers rettigheder og frihedsrettigheder". Endvidere skal der ikke kun tages hensyn til behandlingens karakter, men også det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens omfang, sammenhæng og formål. Databeskyttelsesrådet forstår, at parterne skal specificere det minimumssikkerhedsniveau og de foranstaltninger, der skal iværksættes af databehandleren, nærmere i bilag C2. Databeskyttelsesrådet finder det vigtigt, at oplysninger om bistand til den dataansvarlige med hensyn til behandlingssikkerhed medtages i instrukserne i bilag C2.

Databeskyttelsesrådet har anført et forslag til formulering af afsnit 9.1 og 9.2 ovenfor.

Vedrørende afsnit 9.2.b er Databeskyttelsesrådet af den opfattelse, at enhver henvisning til en specifik national tilsynsmyndighed bør undgås i en standardkontrakt. Endvidere bør ordet "*anmelde*" ("*report*") erstattes med "*anmelde*" ("*notify*"), og formuleringen "*er blevet bekendt med*" ("*discovering*") bør erstattes med "*er blevet bekendt med*" ("*after becoming aware*") for at være i overensstemmelse med artikel 33, stk. 2, i GDPR.

Afsnit 9.2.b kunne formuleres på følgende måde: "*b. dennes forpligtelse til — medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder — at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, [ANGIV den kompetente tilsynsmyndighed], uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med et sådant brud*".

Vedrørende afsnit 9.2.e er Databeskyttelsesrådet ligeledes i denne forbindelse af den opfattelse, at henvisningen til den danske tilsynsmyndighed bør fjernes. Afsnit 9.2.e kunne formuleres på følgende måde: "*e. forpligtelsen til at høre den kompetente tilsynsmyndighed, [ANGIV den kompetente tilsynsmyndighed], inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen*".

Databeskyttelsesrådet finder det vigtigt, at dette afsnit præciseres nærmere i bilag C eller D for at sikre, at parterne træffer foranstaltninger vedrørende den måde, hvorpå denne bistand vil blive ydet i praksis.

3.2.10 Underretning om brud på persondatasikkerheden (afsnit 10 i standardkontraktbestemmelserne)

40. Vedrørende **afsnit 10.1** i standardkontraktbestemmelserne foretrækker Databeskyttelsesrådet som allerede nævnt formuleringen i GDPR for at undgå forvirring. I dette afsnit bør formuleringen "efter at være blevet opmærksom på" ("discovery") ændres til "efter at være blevet opmærksom på" ("after having become aware"). Endvidere opfordrer Databeskyttelsesrådet den danske tilsynsmyndighed til at tilføje ordet "ethvert" foran brud på persondatasikkerheden for at gøre det klart, at det ikke tilkommer databehandleren at vurdere, hvorvidt et brud på datasikkerheden skal anmeldes til den kompetente tilsynsmyndighed. Dette er den dataansvarliges ansvar⁴.

Sætningen kunne ændres på følgende måde: "*1. I tilfælde af ethvert brud på persondatasikkerheden underretter databehandleren eller underdatabehandleren uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på bruddet.*"

Databeskyttelsesrådet anbefaler, at formuleringen "*hos databehandleren eller en eventuel underdatabehandler*" slettes, da den ville begrænse underretningspligten til tilfælde, hvor bruddet sker i disse faciliteter, mens en sådan begrænsning ikke følger af GDPR.

Vedrørende den anden del af afsnit 10.1 er Databeskyttelsesrådet af den opfattelse, at den kan suppleres på følgende måde:

"Databehandlerens underretning til den dataansvarlige skal om muligt ske senest [antal timer], efter at databehandleren er blevet opmærksom på bruddet, sådan at den dataansvarlige har mulighed for at efterleve den forpligtelse til at anmelde brud på persondatasikkerheden, der allerede er omhandlet i afsnit 9.2.b."

41. Vedrørende **afsnit 10.2** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at formuleringen "*under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne*" kunne præciseres yderligere i bilag D for at være mere konkret og skræddersyet. Følgende formulering kunne tilføjes i et nyt afsnit i slutningen af afsnit 10.2:

"Parterne fastsætter i bilag D de oplysninger, der skal tilvejebringes af databehandleren for at bistå den dataansvarlige med at foretage anmeldelse af et brud til tilsynsmyndigheden."

Endvidere hedder det i begyndelsen af den anden sætning i afsnit 10.2 i udkastet til standardkontraktbestemmelser: "*Det kan betyde (...)*". Databeskyttelsesrådet er af den opfattelse, at det — af hensyn til retssikkerheden — er bedre at undgå denne form for formulering. Databeskyttelsesrådet opfordrer den danske tilsynsmyndighed til at ændre denne formulering ved at lade ordet "*kan*" udgå.

3.2.11 Sletning og tilbagelevering af oplysninger (afsnit 11 i standardkontraktbestemmelserne)

42. Vedrørende **afsnit 11** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at det ville være mere praktisk at give en reel valgmulighed i dette afsnit. Databeskyttelsesrådet

⁴ Jf. retningslinjer om anmeldelse af brud på datasikkerheden (s. 13): "Det skal bemærkes, at databehandleren ikke først skal vurdere sandsynligheden for, at bruddet indebærer en risiko, inden den dataansvarlige underrettes. Det er den dataansvarlige, der skal foretage en vurdering, når denne bliver bekendt med bruddet. Databehandleren skal blot fastslå, om der er sket et brud, og så underrette den dataansvarlige."

opfordrer den danske tilsynsmyndighed til at ændre dette afsnit og give den dataansvarlige to konkrete valgmuligheder.

Afsnittet kunne formuleres på følgende måde:

"Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til [valgmulighed 1] *at slette alle personoplysninger, der er behandlet på vegne af den dataansvarlige*, [valgmulighed 2] *at tilbagelevere alle personoplysningerne til den dataansvarlige samt at slette eksisterende kopier*.

[Valgfrit] *Følgende EU-retlige eller nationale bestemmelser, der gælder for databehandleren, foreskriver opbevaring af personoplysningerne efter ophøret af tjenesterne vedrørende behandling: Databehandleren forpligter sig til udelukkende at behandle oplysningerne til de i de omhandlede bestemmelser fastsatte formål og på de gældende betingelser, der skal overholdes nøje.*"

Der kunne gives flere oplysninger i bilag C3, herunder muligheden for, at den dataansvarlige kunne ændre den mulighed, der blev valgt ved kontraktens underskrivelse. Dette berører som følge heraf indholdet af bilag C3. Databeskyttelsesrådet opfordrer den danske tilsynsmyndighed til i højere grad at skelne mellem opbevaringsperiode og sletterutine i bilag C3 og afspejle muligheden for, at den dataansvarlige kan ændre det foretagne valg.

Endelig er Databeskyttelsesrådet af den opfattelse, at ordene "tjenesterne vedrørende behandling" bør præciseres f.eks. gennem formuleringen "efter at tjenesterne vedrørende behandling er ophørt". Dette kan gøres i bilag D.

3.2.12 Tilsyn og revision (afsnit 12 i standardkontraktbestemmelserne)

43. **Afsnit 12.1** i standardkontraktbestemmelserne afspejler indholdet af artikel 28, stk. 3, litra h), i GDPR. Databeskyttelsesrådet anbefaler, at der anvendes den samme terminologi som i stk. 1, "revisioner, herunder inspektioner", i stk. 2 og 3, hvori der henvises til tilsyn.
44. Vedrørende **afsnit 12.3** i standardkontraktbestemmelserne forstår Databeskyttelsesrådet det således, at det omfatter revision og inspektioner i forhold til underdatabehandleren. I henhold til artikel 28, stk. 4, i GDPR pålægges underdatabehandleren de samme forpligtelser som dem, der er fastsat i kontrakten eller et andet retligt dokument mellem den dataansvarlige og databehandleren. Dette omfatter forpligtelsen i henhold til artikel 28, stk. 3, litra h), til at give mulighed for og bidrage til revisioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Formuleringen af afsnit 12.3 synes at begrænse den dataansvarliges ret i denne henseende i forhold til underdatabehandleren ("eventuelle" og "sker [...] gennem databehandleren"). Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed omformulerer afsnit 12.3, således at det er i fuld overensstemmelse med GDPR. Dette kan gøres ved at sammenlægge afsnit 12.2 og 12.3 på følgende måde: "*De nærmere procedurer for den dataansvarliges revisioner, herunder inspektioner, af databehandleren og underdatabehandleren fremgår af bilag C6 og C7 til denne databehandleraftale.*"
45. Vedrørende bilag C6 og C7 anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed ændrer følgende punktum "*Revisionserklæringen sendes snarest muligt efter indhentelsen til den dataansvarlige til orientering*" for at gøre det klart, at den dataansvarlige kan anfægte inspektionens omfang, metode og resultater. Den dataansvarlige bør også kunne anmode om, at der træffes foranstaltninger på baggrund af resultaterne af inspektionen.
46. Endvidere bør henvisningen i bilag C6 til "*hos databehandleren*" og C7 til "*hos underdatabehandleren*" udvides. Den dataansvarliges rettigheder inden for rammerne af inspektioner og/eller revision bør

således ikke begrænses til databehandlerens eller underdatabehandlerens faciliteter. Den dataansvarlige bør have adgang til de steder, for behandlingen foretages. Dette omfatter fysiske faciliteter samt systemer, der anvendes og har relation til behandlingen.

3.2.13 Parternes aftaler om andre forhold (afsnit 13 i standardkontraktbestemmelserne)

47. Vedrørende **afsnit 13** i standardkontraktbestemmelserne anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed tager i betragtning, at hvis der medtages et afsnit, der præciserer ansvar, gældende lovgivning, jurisdiktion eller andre forhold, må dette ikke være i strid med de relevante bestemmelser i GDPR eller svække den beskyttelse, der følger af GDPR eller kontrakten.

3.2.14 Ikrafttræden og ophør (afsnit 14 i standardkontraktbestemmelserne)

48. Vedrørende **afsnit 14.4** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at et specifikt afsnit om kontraktens opsigelse også kunne være relevant for standardkontraktbestemmelserne. Da det er Databeskyttelsesrådets opfattelse, at forholdet mellem databehandleraftalen og hovedaftalen bør være mere fleksibelt, anbefaler Databeskyttelsesrådet, at den danske tilsynsmyndighed medtager et afsnit om opsigelse i standardkontraktbestemmelserne.
49. Vedrørende **afsnit 14.5** i standardkontraktbestemmelserne er Databeskyttelsesrådet af den opfattelse, at dette afsnit kunne være i strid med afsnit 2.4 eller 14.4. Databeskyttelsesrådet anbefaler, at den danske tilsynsmyndighed præciserer forholdet mellem disse tre afsnit.

3.2.15 Bilag A

50. Bilag A har til formål at give oplysninger om de behandlingsaktiviteter, der udføres af databehandleren på vegne af den dataansvarlige. Med henblik herpå anbefaler Databeskyttelsesrådet, at formålet med og karakteren af behandlingen beskrives samt typen af personoplysninger, der behandles, kategorierne af berørte registrerede og varigheden af behandlingen. Denne beskrivelse bør være så detaljeret som muligt, og under alle omstændigheder skal typerne af personoplysninger præciseres mere end blot "personoplysninger som defineret i artikel 4, nr. 1)", eller det skal angives, hvilken kategori (artikel 6, 9 eller 10) af personoplysninger der skal behandles. Databeskyttelsesrådet er af den opfattelse, at det bør være klart, at i tilfælde af flere behandlingsaktiviteter skal disse oplysninger angives for hver af dem. Endvidere finder Databeskyttelsesrådet ikke de to første eksempler overbevisende, da det er vanskeligt at skelne mellem formålet med og karakteren af behandlingen.

4 KONKLUSIONER

51. Databeskyttelsesrådet bifalder i høj grad det danske initiativ til at forelægge deres udkast til standardkontraktbestemmelser til udtalelse. Det vil bidrage til en harmoniseret gennemførelse af GDPR.
52. Databeskyttelsesrådet er af den opfattelse, at den danske tilsynsmyndigheds udkast til standardkontraktbestemmelser, som er forelagt til udtalelse, bør justeres for at kunne betragtes som standardkontraktbestemmelser. Databeskyttelsesrådet har fremsat en række anbefalinger i sin ovenstående udtalelse. Hvis alle anbefalinger gennemføres, vil den danske tilsynsmyndighed kunne anvende dette udkast til aftale som standardkontraktbestemmelser i henhold til artikel 28, stk. 8, i GDPR uden behov for en efterfølgende vedtagelse fra Europa-Kommissionens side.

5 AFSLUTTENDE BEMÆRKNINGER

53. Denne udtalelse er rettet til Datatilsynet og vil blive offentliggjort i henhold til artikel 64, stk. 5, litra b), i GDPR.
54. I henhold til artikel 64, stk. 7 og 8, i GDPR giver tilsynsmyndigheden senest to uger efter modtagelsen af udtalelsen formanden elektronisk meddelelse om, hvorvidt den agter at ændre eller fastholde sit udkast til standardkontraktbestemmelser. Inden for samme frist forelægger den det ændrede udkast til standardkontraktbestemmelser ⁵, eller, såfremt den ikke agter at følge udtalelsen fra Databeskyttelsesrådet, giver den en relevant begrundelse for, hvorfor den helt eller delvist ikke agter at følge denne udtalelse.

For Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)

⁵ Tilsynsmyndigheden sender den endelige afgørelse til Databeskyttelsesrådet med henblik på optagelse i registret over afgørelser, som har været genstand for sammenhængsmekanismen, i henhold til artikel 70, stk. 1, litra y), i GDPR.