Gemensamt yttrande 1/2021 från Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) om Europeiska kommissionens genomförandebeslut om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden

för de frågor som avses i artikel 28.7 i förordning (EU) 2016/679 och artikel 29.7 i förordning (EU) 2018/1725

Innehåll

1 Bakgrund 3
2 Yttrandets tillämpningsområde 4
3 Allmän motivering till utkastet till beslut och utkasten till standardavtalsklausuler 4
3.1 Allmänna kommentarer 5
3.2 Förklaring av den metod som tillämpats och dokumentets struktur 6
4 Analys av utkastet till beslut och dess bilaga 6
4.1 De viktigaste kommentarerna till utkastet till beslut 6
4.1.1 Om beslutets tillämpningsområde och om kopplingen till den andra uppsättningen av utkast till standardavtalsklausuler om överföringar 6
4.2 Huvudsakliga kommentarer om bilagan till kommissionens genomförandebeslut 7
4.2.1 Syfte och tillämpningsområde (klausul 1 i utkastet till standardavtalsklausuler) 7
4.2.2 Beständighet (klausul 2 i utkastet till standardavtalsklausuler) 8
4.2.3 Dockningsklausul (klausul 5 i utkastet till standardavtalsklausuler) 8
4.2.4 Parternas skyldigheter (klausul 7 i utkastet till standardavtalsklausuler) 8
4.2.5 Rättigheter för registrerade (klausul 8 i utkastet till standardavtalsklausuler) 11
4.2.6 Bilagor till utkastet till standardavtalsklausuler 12

Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen har

med beaktande av artikel 42.2 i Europaparlamentets och rådets förordning 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (***persondataskydds-förordningen***),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

ANTAGIT FÖLJANDE GEMENSAMMA YTTRANDE

1 BAKGRUND

1. När det gäller förhållandet mellan en personuppgiftsansvarig och ett eller flera personuppgifts-biträden, för behandling av personuppgifter, föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (***allmänna dataskyddsförordningen***) en uppsättning bestämmelser avseende upprättandet av ett särskilt avtal mellan de parter som är berörda, och obligatoriska bestämmelser som ska ingå i detta.

2. Enligt artikel 28.3 i dataskyddsförordningen ska ett personuppgiftsbiträdes behandling av uppgifter regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgifts-ansvarige, där en uppsättning specifika aspekter för att reglera avtalsförhållandet mellan parterna fastställs. Dessa omfattar bland annat föremålet för och varaktigheten av behandlingen, dess art och ändamål, typen av personuppgifter och kategorier av registrerade. I artikel 28.4 föreskrivs ytterligare krav när ett personuppgiftsbiträde anlitar ett annan personuppgiftsbiträde för att utföra specifik behandlingsverksamhet på den personuppgiftsansvariges vägnar.

3. Enligt artikel 28.6 i dataskyddsförordningen får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, det avtal eller den andra rättsakt som avses i punkterna 3 och 4 i artikel 28 i dataskyddsförordningen helt eller delvis grunda sig på standardavtalsklausuler. Dessa standardavtalsklausuler ska antas för de frågor som avses i punkterna 3 och 4.

[1] Hänvisningar till ”medlemsstater” i detta yttrande ska förstås som hänvisningar till ”medlemsstater i EES”.

4. Enligt artikel 28.7 i allmänna dataskyddsförordningen får kommissionen fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i denna artikel, i enlighet med det granskningsförfarande som avses i artikel 93.2.

5. I persondataskyddsförordningen fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner och organ samt bestämmelser om det fria flödet av personuppgifter mellan dem eller till andra mottagare som är etablerade i unionen.

6. Artiklarna 29.3, 29.4 och 29.7 i persondataskyddsförordningen innehåller föreskrifter som liknar dem i artiklarna 28.3, 28.4 och 28.7 i allmänna dataskyddsförordningen Detta motiveras av det faktum att de dataskyddsregler som är tillämpliga på den offentliga sektorn i medlemsstaterna och dataskyddsreglerna för unionens institutioner, organ, kontor och byråer har anpassats i största möjliga utsträckning, för att säkerställa dels en enhetlig strategi för skydd av personuppgifter i hela unionen, dels det fria flödet av personuppgifter inom unionen.

2 YTTRANDETS TILLÄMPNINGSOMRÅDE

7. Den 12 november 2020 offentliggjorde kommissionen följande:

   - Ett utkast till kommissionens genomförandebeslut om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden för de frågor som avses i artiklarna 28.3 och 28.4 i förordning (EU) 2016/679 och artikel 29.7 i förordning (EU) 2018/1725 (***utkastet till beslut***).

   - Ett utkast till bilaga till kommissionens genomförandebeslut om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden för de frågor som avses i artiklarna 28.3 och 28.4 i förordning (EU) 2016/679 och artikel 29.7 i förordning (EU) 2018/1725 (***utkastet till standardavtalsklausuler***).

8. Samma dag offentliggjorde Europeiska kommissionen också ett utkast till kommissionens genomförandebeslut och dess bilaga om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med förordning (EU) 2016/679.

9. Den 12 november 2020 begärde Europeiska kommissionen ett gemensamt yttrande från Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen på grundval av artikel 42.1 och 42.2 i förordning (EU) 2018/1725 (persondataskyddsförordningen) om dessa två uppsättningar utkast till standardavtalsklausuler och respektive genomförandeakter.

10. För tydlighetens skull beslutade Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att avge två separata yttranden om dessa två uppsättningar av standardavtalsklausuler.

11. Tillämpningsområdet för detta yttrande är således begränsat till utkastet till beslut och utkastet till standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden för de frågor som avses i artiklarna 28.3 och 28.4 i den allmänna dataskyddsförordningen och artikel 29.3 och 29.4 i persondataskyddsförordningen.

3 ALLMÄN MOTIVERING TILL UTKASTET TILL BESLUT OCH UTKASTEN TILL STANDARDAVTALSKLAUSULER

3.1 Allmänna kommentarer

12. Alla uppsättningar av standardavtalsklausuler måste ytterligare specificera bestämmelserna i artikel 28 i den allmänna dataskyddsförordningen och artikel 29 i persondataskyddsförordningen. Yttrandet från Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen syftar till att säkerställa konsekvens och korrekt tillämpning av artikel 28 i allmänna dataskyddsförordningen när det gäller det framlagda utkastet till standardavtalsklausuler som skulle kunna fungera som standardavtalsklausuler i enlighet med artikel 28.7 i den allmänna dataskyddsförordningen och artikel 29.7 i persondataskyddsförordningen.

13. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att klausuler som endast upprepar bestämmelserna i artiklarna 28.3 och 28.4 i allmänna dataskyddsförordningen och artiklarna 29.3 och 29.4 persondataskyddsförordningen inte är tillräckliga för att utgöra standardavtalsklausuler. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen har därför beslutat att analysera dokumentet i sin helhet, inklusive bilagorna. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att ett avtal enligt artikel 28 i den allmänna dataskyddsförordningen eller artikel 29 i persondataskyddsförordningen ytterligare bör ange och klargöra hur bestämmelserna kommer att uppfyllas. Mot denna bakgrund analyseras utkastet till standardavtalsklausuler som överlämnats till Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen för yttrande.

14. Antagna standardavtalsklausuler utgör en uppsättning garantier som ska tillämpas som de är, eftersom de syftar till att skydda de registrerade och minska de särskilda risker som sammanhänger med de grundläggande principerna för uppgiftsskydd.

15. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen välkomnar generellt antagandet av standardavtalsklausuler som ett kraftfullt verktyg för ansvarsskyldighet som gör det lättare för personuppgiftsansvariga och personuppgiftsbiträden att uppfylla sina skyldigheter enligt den allmänna dataskyddsförordningen och persondataskyddsförordningen.

16. Europeiska dataskyddsstyrelsen har redan avgett yttranden om standardavtalsklausuler som utarbetats av den danska tillsynsmyndigheten[2] och den slovenska tillsynsmyndigheten[3].

17. För att säkerställa en enhetlig strategi för skydd av personuppgifter i hela unionen välkomnar Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen varmt kommissionens planerade antagande av standardavtalsklausuler med rättsverkan i hela EU.

18. Samma uppsättning standardavtalsklausuler kommer att gälla oavsett om det aktuella förhållandet upprättas mellan privata enheter, myndigheter i medlemsstaterna eller EU:s institutioner eller organ. Dessa EU-omfattande standardavtalsklausuler kommer att säkerställa ytterligare harmonisering och rättssäkerhet.

[2] Yttrande 14/2019 om det utkast till standardavtalsklausuler som lämnats in av den danska tillsynsmyndigheten (artikel 28.8 i den allmänna dataskyddsförordningen): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf

[3] Yttrande 17/2020 om det utkast till standardavtalsklausuler som lämnats in av den slovenska tillsynsmyndigheten (artikel 28.8 i den allmänna dataskyddsförordningen): https://edpb.europa.eu/our-work-tools/our-documents/opinjoni-tal-bord-art-64/opinion-172020-draft-standard-contractual_en

19. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen välkomnar också att samma uppsättning standardavtalsklausuler bör tillämpas när det gäller förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden som omfattas av den allmänna dataskyddsförordningen respektive persondataskyddsförordningen.

3.2 Förklaring av den metod som tillämpats och dokumentets struktur

20. För tydlighets skull innehåller detta yttrande i) en central del med allmänna kommentarer som Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen vill framföra och ii) en bilaga där kommentarer av mer teknisk art framförs direkt avseende utkastet till beslut och utkastet till standardavtalsklausuler för att ge några exempel på möjliga ändringar. Någon hierarki finns ej mellan de allmänna och de tekniska kommentarerna.

21. Dessutom presenteras de viktigaste kommentarerna om utkastet till beslut och utkastet till standardavtalsklausuler i två separata avsnitt. Vid behov görs korshänvisningar för att säkerställa enhetlighet.

22. För konsekvensens skull görs vid behov även korshänvisningar till Europeiska dataskyddsstyrelsens och Europeiska datatillsynsmannens gemensamma yttrande 02/2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer.

4 ANALYS AV UTKASTET TILL BESLUT OCH DESS BILAGA

4.1 De viktigaste kommentarerna till utkastet till beslut

4.1.1 Om beslutets tillämpningsområde och om kopplingen till den andra uppsättningen av utkast till standardavtalsklausuler om överföringar

23. I artikel 2 i utkastet till beslut föreskrivs att "standardavtalsklausulerna i bilagan får användas i avtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde som behandlar personuppgifter för dennes vägnar, om den personuppgiftsansvariga och personuppgiftsbiträdet omfattas av förordning (EU) 2016/679 eller förordning (EU) 2018/1725".

24. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att den nuvarande lydelsen av denna artikel ger upphov till rättsosäkerhet när det gäller de situationer där enheter kommer att kunna förlita sig på dessa standardavtalsklausuler.

25. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen förstår kommissionens avsikt, att dessa standardavtalsklausuler endast är avsedda att täcka situationer inom EU och att dessa klausuler inte bör åberopas vid överföring i den mening som avses i kapitel V. I dessa fall bör parterna snarare förlita sig på den separata uppsättning standardavtalsklausuler som har fastställts för överföring av personuppgifter till tredjeländer i enlighet med förordning (EU) 2016/679 och som också syftar till att täcka kraven i artiklarna 28.3 och 28.4 i dataskyddsförordningen (***standardavtalsklausuler för överföring***).

26. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att utkastet till beslut inte ger parterna tillräcklig klarhet och att beslutets exakta räckvidd måste anges tydligt och specificeras i ett särskilt skäl i utkastet till beslut, till exempel före det nuvarande skäl 10 i utkastet till beslut.

27. Dessutom anser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att den nuvarande lydelsen av artikel 2 i utkastet till beslut inte begränsar tillämpningsområdet till situationer

inom EU, eftersom personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av den allmänna dataskyddsförordningen för en viss behandling kan vara etablerade utanför EU i enlighet med artikel 3.2 i allmänna dataskyddsförordningen. Det bör sedan klargöras om dessa standardavtalsklausuler skulle kunna tillämpas i denna situation.

28. Slutligen anser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen snarare att den avsedda begränsningen till situationer inom EU inte är motiverad. Till exempel ser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen ingen anledning att hindra enheter från att förlita sig på dessa standardavtalsklausuler – i syfte att efterleva artiklarna 28.3 och 28.4 i allmänna dataskyddsförordningen – om en av parterna inte omfattas av den allmänna dataskyddsförordningen för en viss behandlingsverksamhet men befinner sig i ett lämpligt land. Om tillämpningsområdet för standardavtalsklausulerna utvidgas till situationer som inbegriper överföringar utanför EU bör det klargöras för parterna att dessa standardavtalsklausuler kommer att uppfylla kraven i artiklarna 28.3 och 28.4 i den allmänna dataskyddsförordningen eller artiklarna 29.3 och 29.4 i persondataskyddsförordningen, men inte alla krav som följer av den allmänna dataskyddsförordningen eller EU-dataskyddsförordningen, till exempel regler som rör internationella överföringar.

29. Enligt Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen är det också viktigt att i beslutet tydligt förklara kopplingen och samverkan mellan denna uppsättning av standardavtalsklausuler och standardavtalsklausulerna för överföring. Redan i beslutet bör klargöras för parterna att när de avser att dra nytta av standardavtalsklausuler både enligt artikel 28.7 i dataskyddsförordningen och artikel 46.2 c i dataskyddsförordningen, måste de förlita sig på standardavtalsklausuler för överföring.

4.2 Huvudsakliga kommentarer om bilagan till kommissionens genomförandebeslut

4.2.1 Syfte och tillämpningsområde (klausul 1 i utkastet till standardavtalsklausuler)

30. I **klausul 1 a** i utkastet till standardavtalsklausuler anges att syftet med standardavtalsklausulerna är att säkerställa överensstämmelse med den allmänna dataskyddsförordningen och persondataskyddsförordningen. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att avtalsparterna vid undertecknandet av klausulerna bör kunna välja mellan hänvisningar till den allmänna dataskyddsförordningen eller persondataskyddsförordningen beroende på vilken relevant förordning som är tillämplig på deras situation.

31. På så sätt skulle enheter som använder standardavtalsklausuler enligt artikel 28 i allmänna dataskyddsförordningen inte ha någon hänvisning till persondataskyddsförordningen i sina standardavtalsklausuler och enheter som förlitar sig på artikel 29 i persondataskyddsförordningen skulle undvika hänvisningarna till den allmänna dataskyddsförordningen. Detta skulle bidra till att skapa klarhet i förbindelserna mellan parter som ofta är mindre förtrogna med sådana föreskrifter. Om så är fallet bör standardavtalsklausulerna ange att ett sådant val är möjligt och utformningen av standardavtalsklausulerna bör anpassas i enlighet med detta.

32. Som föreskrivs i **klausulerna 1 b och 1 c**, och i enlighet med **klausul 5** (dockningsklausul), kan flera personuppgiftsansvariga eller personuppgiftsbiträden, förtecknade i **bilaga I**, vara parter anslutna till standardavtalsklausulerna för den behandling som avses i **bilaga II**. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att det i fall som dessa där det finns flera avtalsparter bör fastställas i standardavtalsklausulerna (och deras bilagor) att parterna ytterligare specificerar och avgränsar ansvarsfördelningen och tydligt anger vilken behandling som utförs av vilka personuppgiftsbiträden på vilka personuppgiftsansvarigas vägnar och för vilka ändamål. Den

nuvarande formuleringen av dessa klausuler i standardavtalsklausulerna och bilagorna kan leda till förvirring när det gäller varje enhets kvalifikationer och roll med avseende på en viss behandling, särskilt med tanke på möjligheten att införa en dockningsklausul.

4.2.2 Beständighet (klausul 2 i utkastet till standardavtalsklausuler)

33. Enligt **klausul 2 b** i utkastet till standardavtalsklausuler åtar sig parterna att inte ändra dem såvida inte ytterligare klausuler "*direkt eller indirekt strider mot* standardavtalsklausulerna". För att skapa rättssäkerhet för personuppgiftsansvariga och personuppgiftsbiträden skulle Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen välkomna förtydliganden om vilken typ av klausuler som Europeiska kommissionen skulle anse stå i strid med standardavtalsklausuler antingen direkt eller indirekt. Ett sådant klargörande skulle till exempel kunna indikera att klausuler som strider mot standardavtalsklausulerna skulle vara sådana som undergräver eller negativt påverkar skyldigheterna i standardavtalsklausulerna eller förhindrar efterlevnad av de skyldigheter som ingår i standardavtalsklausulerna. Till exempel skulle klausuler som gör det möjligt för personuppgiftsbiträden att använda uppgifterna för egna ändamål strida mot personuppgiftsbiträdets skyldighet att behandla personuppgifter endast på den personuppgiftsansvariges vägnar och för de ändamål och med de medel som denna person har identifierat.

4.2.3 Dockningsklausul (klausul 5 i utkastet till standardavtalsklausuler)

34. Enligt **klausul 5** i utkastet till standardavtalsklausuler får varje enhet som ett alternativ ansluta sig till standardavtalsklausulerna och därmed bli en ny part i avtalet som personuppgiftsansvarig eller personuppgiftsbiträde. Som redan nämnts ovan bör en sådan ny avtalsparts kvalifikationer och roll tydligt framgå av bilagorna genom att parterna uppmanas att närmare precisera och avgränsa ansvarsfördelningen och tydligt ange vilken behandling som utförs av vilka personuppgiftsbiträden på vilka personuppgiftsansvarigas vägnar och för vilka ändamål.

35. Enligt **klausul 5 a** är nya parters anslutning till standardavtalsklausulerna beroende av att alla övriga parter samtycker. För att undvika eventuella svårigheter i praktiken skulle Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen välkomna ett klargörande av hur ett sådant samtycke skulle kunna ges av de andra parterna (om det ska vara skriftligt eller inte, tidsfristen för att meddela ett sådant samtycke, den information som behövs innan man kan komma överens). Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen skulle också välkomna ett klargörande av huruvida och på vilket sätt ett sådant samtycke måste ges av alla parter, oberoende av deras kvalifikationer och roll i behandlingen.

4.2.4 Parternas skyldigheter (klausul 7 i utkastet till standardavtalsklausuler)

36. Även om rubriken på denna klausul är ”Parternas skyldigheter”, hänvisar **klausul 7 a** i sin nuvarande form endast till de skyldigheter som åläggs personuppgiftsbiträdet. Enligt artikel 28.3 i dataskyddsförordningen ska den personuppgiftsansvariges/personuppgiftsbiträdets rättigheter och skyldigheter anges i avtalet. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen föreslår därför att en hänvisning till den personuppgiftsansvariges skyldigheter läggs till i denna klausul för fullständighetens och tydlighetens skull. Till exempel skulle följande mening kunna läggas till före klausul 7 a: ”Den personuppgiftsansvarige har rätt och skyldighet att fatta beslut om ändamålen och medlen för behandlingen av personuppgifter och ansvarar för att se till att behandlingen av personuppgifter sker i enlighet med EU:s eller medlemsstaternas tillämpliga dataskyddsbestämmelser

och klausulerna (däribland att säkerställa att den behandling av personuppgifter som personuppgiftsbiträdet instrueras att utföra bygger på en rättslig grund i enlighet med artikel 6 i allmänna dataskyddsförordningen eller artikel 5 i persondataskyddsförordningen)".

37. I klausul 7 a föreskrivs också att närmare instruktioner ska ges i bilaga IV och att efterföljande instruktioner också får ges av den personuppgiftsansvarige. Möjligheten för den personuppgiftsansvarige att ge "*efterföljande instruktioner*" är nödvändig för att parternas rättigheter och skyldigheter till fullo ska genomföras enligt standardavtalsklausulerna, men är inte obegränsad. Eventuella efterföljande instruktioner bör överensstämma med parternas respektive rättigheter och skyldigheter enligt standardavtalsklausulerna. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen anser att detta tydligt bör anges i den berörda klausulen.

38. För att öka överensstämmelsen med texten i 28.3 a i den allmänna dataskyddsförordningen och artikel 29.3 a i persondataskyddsförordningen och för att införa en sådan skyldighet direkt i avtalet föreslår Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen dessutom att slutet av första meningen i klausul 7 a ändras enligt följande understrukna lydelse: "Personuppgiftsbiträdet ska behandla personuppgifter endast enligt dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte personuppgiftsbiträdet är skyldigt att göra detta enligt unionsrätten eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av. I sådana fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om detta rättsliga krav före behandlingen, såvida inte sådan information är förbjuden enligt denna lag av vägande skäl som rör allmänintresset".

39. När det gäller olagliga instruktioner från den personuppgiftsansvarige, enligt vad som beskrivs i artikel 28.3 andra stycket i den allmänna dataskyddsförordningen, anser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet bör innehålla mer exakt information om vilka konsekvenser och lösningar som planeras om personuppgiftsbiträdet informerar den personuppgiftsansvarige om sin åsikt att instruktionen strider mot dataskyddsförordningen eller andra tillämpliga dataskyddsbestämmelser. Europeiska kommissionen bör därför uppmana parterna att i avtalet inkludera ytterligare uppgifter om konsekvenserna av anmälan av en olaglig instruktion (t.ex. en klausul om möjligheten för personuppgiftsbiträden att skjuta upp genomförandet av den berörda instruktionen till dess att den personuppgiftsansvarige bekräftar, ändrar eller drar tillbaka sin instruktion eller en klausul om uppsägning av avtalet om den personuppgiftsansvarige fortsätter med en olaglig instruktion).

40. När det gäller de alternativ som den personuppgiftsansvarige har enligt **klausul 7.2** i fråga om radering eller återlämnande av uppgifter uppmanar Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen Europeiska kommissionen att i själva klausulen specificera att den personuppgiftsansvarige bör kunna ändra det val som gjordes vid tidpunkten för undertecknandet av avtalet under avtalets hela löptid och vid uppsägning.

41. Som en allmän kommentar till **klausul 7.3** om säkerhet vid behandling noterar Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att alla skyldigheter tillskrivs personuppgiftsbiträdet utan att den personuppgiftsansvariges roll närmare anges, särskilt när det gäller den riskbedömning som måste utföras för säkerhetsåtgärder med koppling till syftet med behandlingen som fastställts av den personuppgiftsansvarige. I vissa fall kanske personuppgiftsbiträdet inte känner till det exakta syftet med behandlingen, till exempel när det är fråga om värdtjänster. Därför, och i enlighet med artikel 28.3 i dataskyddsförordningen, anser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att klausulen bör kompletteras med de skyldigheter som gäller för behandlingens säkerhet för den personuppgiftsansvarige, som i synnerhet måste tillhandahålla all användbar information till personuppgiftsbiträdet för att uppfylla de relevanta kraven i detta avseende**.**

42. **I klausul 7.3 a** i utkastet till standardavtalsklausuler föreskrivs att personuppgiftsbiträdet har minst 48 timmar på sig att underrätta den personuppgiftsansvarige om ett personuppgiftsbrott. En sådan tidsfrist kan vara kort i vissa situationer och kan också leda till förväxling med den tidsfrist enligt vilken den personuppgiftsansvarige måste anmäla personuppgiftsbrottet till tillsynsmyndigheten (och denna tidsfrist börjar när den personuppgiftsansvarige har fått vetskap om det, dvs. när personuppgiftsbiträdet underrättar honom eller henne). Med beaktande av personuppgiftsbiträdets skyldighet att underrätta den personuppgiftsansvarige ”*utan onödigt dröjsmål*” efter att han eller hon har fått vetskap om personuppgiftsincidenten i enlighet med artikel 33.2 i den allmänna dataskyddsförordningen, föreslår Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att låta parterna ge en lämplig tidsram för att uppfylla detta krav, beroende på den specifika situationen. Parterna bör därför uppmanas att i standardavtalsklausulerna ange den överenskomna tidsramen för en sådan anmälan.

43. I **klausul 7.4 c** i utkastet till standardavtalsklausuler föreskrivs en möjlighet för den personuppgiftsansvarige att använda sig av en oberoende revisor som bemyndigats av personuppgiftsbiträdet i syfte att utföra granskningar. Denna bestämmelse föreskrivs inte i artikel 28.3 h i den allmänna dataskyddsförordningen och behöver anpassas till denna artikel, där det föreskrivs att personuppgiftsbiträdet måste möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige. Personuppgiftsbiträdet kan därför föreslå en revisor, men beslutet om revisorn måste överlåtas till den personuppgiftsansvarige i enlighet med artikel 28.3 h i dataskyddsförordningen.

44. I **klausul 7.4 c** anges också att om den personuppgiftsansvarige bemyndigar en oberoende revisor ska denna person stå för kostnaderna, och om personuppgiftsbiträdet bemyndigats att genomföra en granskning måste personuppgiftsbiträdet stå för den oberoende revisorns kostnader. Eftersom frågan om kostnadsfördelning mellan en personuppgiftsansvarig och ett personuppgiftsbiträde inte regleras i dataskyddsförordningen anser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen följaktligen att alla hänvisningar till kostnaderna bör strykas från denna klausul.

45. När det gäller **klausul 7.7** om internationella överföringar, och mer specifikt vad gäller situationer där ett personuppgiftsbiträde förlitar sig på en underentreprenör i ett tredjeland, anser Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen att led b skulle kunna vara tydligare vad avser möjligheten för dessa båda parter att underteckna en enda uppsättning standardavtalsklausuler som syftar till efterlevnad av både kapitel V och artikel 28.4 i allmänna dataskyddsförordningen, om detta verkligen är målet med denna klausul, vilket skulle kräva ytterligare förtydligande. Det bör också klargöras om parterna då måste förlita sig på denna uppsättning standardavtalsklausuler eller snarare på de standardavtalsklausuler för överföring som också ger garantier enligt artiklarna 28.3 och 28.4 i dataskyddsförordningen.

46. Dessutom vill Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen betona att även om **klausul 7.7 b** endast hänvisar till tillämpningen av standardavtalsklausulerna för överföring, skulle flera andra överföringsverktyg legitimt kunna användas för att utforma överföringarna från personuppgiftsbiträdet till en underentreprenör i tredjeland, och föreslår därför att man använder en mer generisk formulering som hänvisar till överföringsverktyg enligt artikel 46 i den allmänna dataskyddsförordningen.

47. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen konstaterade också behovet av att ytterligare klargöra den sista delen av klausul 7.7 b, som hänvisar till "villkoren för användning av standardavtalsklausulerna för överföring". Eftersom denna bestämmelse tyder på att det kan finnas

särskilda villkor för tillämpningen av standardavtalsklausulerna för överföring, finns det ett behov av att specificera vilka dessa villkor är.

4.2.5 Rättigheter för registrerade (klausul 8 i utkastet till standardavtalsklausuler)

48. Klausulen har för närvarande rubriken ”*Registrerades rättigheter* ”, men Europeiska dataskydds-styrelsen och Europeiska datatillsynsmannen anser att titeln inte återspeglar klausulens innehåll.

49. I **klausulerna 8 a och 8 b** i utkastet till standardavtalsklausuler nämns personuppgiftsbiträdets skyldighet att bistå den personuppgiftsansvariga när denne fullgör sina skyldigheter att svara på begäranden om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskydds-förordningen och kapitel III i persondataskyddsförordningen. I klausulerna 8 c och 8 d hänvisas det dock till att personuppgiftsbiträdet bistår med andra typer av skyldigheter för personuppgifts-ansvariga, särskilt enligt artiklarna 32 till 36 i den allmänna dataskyddsförordningen och artiklarna 33 till 41 i persondataskyddsförordningen.

50. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen föreslår därför att rubriken på denna klausul ändras till ”*Bistånd till den personuppgiftsansvarige*” för att återspegla de olika slags bistånd som personuppgiftsbiträdet behöver ge.

51. Som ett alternativ skulle Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen rekommendera kommissionen att dela upp klausulen i två delar för att skilja mellan det bistånd som personuppgiftsbiträdet behöver ge

- enligt den personuppgiftsansvariges skyldigheter att besvara begäranden om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskyddsförordningen och kapitel III i persondataskyddsförordningen, och
- enligt den personuppgiftsansvariges skyldigheter enligt artiklarna 32 till 36 i allmänna dataskyddsförordningen och artiklarna 33 till 41 i persondataskyddsförordningen.

52. I klausul 8 a i utkastet till standardavtalsklausuler föreskrivs också *att "personuppgiftsbiträdet utan dröjsmål ska underrätta den personuppgiftsansvarige om varje begäran som mottas direkt från den registrerade". Personuppgiftsbiträdet ska inte själv besvara denna begäran, såvida inte och inte förrän den personuppgiftsansvarige har bemyndigat vederbörande att göra detta.*

53. Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen anser att denna klausul bör

- ytterligare precisera att svaren till de registrerade ska lämnas i enlighet med den person-uppgiftsansvariges instruktioner (t.ex. om innehållet i svaret) i enlighet med bilaga IV,
- ytterligare precisera att omfattningen av personuppgiftsbiträdets skyldighet att utöva den registrerades rättigheter på den personuppgiftsansvariges vägnar bör beskrivas och tydligt anges i bilaga VII.

54. I **klausul 8 c 1** och **klausul 9 a** föreskrivs att behörig tillsynsmyndighet måste anges, men inget föreskrivs för de fall där det finns flera personuppgiftsansvariga parter i avtalet och därmed flera behöriga tillsynsmyndigheter. Därför bör möjligheten att nämna flera behöriga tillsynsmyndigheter läggas till. Dessutom kan det finnas fall där den behandling som omfattas av klausulerna är gränsöverskridande och en ansvarig tillsynsmyndighet ska identifieras som behörig tillsynsmyndighet. Detta bör också avspeglas i klausulerna 8 c 1 och 9 a.

55. Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen föreslår att kommissionen, om personuppgiftsbiträden inom EU är bundna av tredjeländers lagstiftning eller praxis som påverkar efterlevnaden av dessa klausuler, bör bedöma om det är lämpligt med ytterligare en klausul för att hantera dessa fall.

4.2.6 Bilagor till utkastet till standardavtalsklausuler

56. Standardavtalsklausulerna är utformade för att användas för databehandlingsavtal som kan omfatta mer än en part som personuppgiftsansvarig och/eller mer än en part som personuppgiftsbiträde. Detta innebär en risk för att parternas ansvar blir otydligt om bilagorna inte fylls i på lämpligt sätt. Denna risk ökar om nya parter senare ansluter sig till avtalet genom att använda dockningsklausulen och/eller avtalet omfattar behandling för olika ändamål eller under andra omständigheter.

57. Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen anser att det är av yttersta vikt att bilagorna till standardavtalsklausulerna med absolut klarhet avgränsar var och en av parternas roller och ansvarsområden i varje relation och med avseende på varje behandling. Detta är nödvändigt för att parterna ska kunna avgöra vem som behandlar personuppgifter för vem och för vilket ändamål, samt vilka instruktioner som är tillämpliga och vem som får ge instruktioner. Alla oklarheter skulle göra det omöjligt för personuppgiftsansvariga eller personuppgiftsbiträden att fullgöra sina skyldigheter enligt ansvarighetsprincipen.

58. Vissa element kan variera, såsom de parter som tillhandahåller eller använder vissa behandlingstjänster, beskrivningen (närmare uppgifter om) av behandlingen, de tillämpliga tekniska och organisatoriska åtgärderna, instruktionerna från den personuppgiftsansvarige om behandlingen av personuppgifter, de särskilda begränsningarna och/eller ytterligare skyddsåtgärderna avseende uppgifter av särskild kategori, de godkända underentreprenörerna och/eller de tekniska och organisatoriska åtgärder som personuppgiftsbiträdena är skyldiga att bistå den personuppgiftsansvarige med. Om så behövs bör parterna vara skyldiga att ytterligare fylla i bilagorna I–VII, såvida inte skillnaderna är mycket begränsade och undantagen tydligt anges i bilagorna.

59. När det gäller komplexa avtal, som till exempel omfattar flera parter eller flera syften, måste det alltid vara tydligt vilken bilaga (eller vid begränsade avvikelser i en enda bilaga: vilken bestämmelse i en sådan bilaga) som gäller för vilken specifik situation eller vilket förhållande. Det är nödvändigt att tydligt identifiera och särskilja de olika behandlingsverksamheterna.

***

För Europeiska datatillsynsmannen	För Europeiska dataskyddsstyrelsen
Europeiska datatillsynsmannen	Ordförande
(Wojciech Wiewiorowski)	(Andrea Jelinek)