

Yttrande från styrelsen (art. 64)



Yttrande 22/2024 om vissa skyldigheter vid anlitande av personuppgiftsbiträden och underleverantörer

Antaget den 7 oktober 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Sammanfattning

Den danska tillsynsmyndigheten begärde att Europeiska dataskyddsstyrelsen (EDPB) skulle avge ett yttrande i frågor med allmän räckvidd i enlighet med artikel 64.2 i den allmänna dataskyddsförordningen. Yttrandet bidrar till en harmoniserad tolkning från de nationella tillsynsmyndigheternas sida när det gäller vissa aspekter av artikel 28 i den allmänna dataskyddsförordningen, i förekommande fall tillsammans med kapitel V i samma förordning. I yttrandet behandlas i synnerhet frågor rörande tolkningen av vissa skyldigheter för personuppgiftsansvariga som använder sig av personuppgiftsbiträden och underleverantörer (underbiträden), särskilt enligt artikel 28 i den allmänna dataskyddsförordningen, samt frågor om hur avtalen mellan personuppgiftsansvariga och personuppgiftsbiträden bör formuleras. Frågorna gäller behandling av personuppgifter inom EES samt behandling efter överföring till tredje land.

EDPB drar i detta yttrande slutsatsen att personuppgiftsansvariga alltid bör ha informationen om identiteten (dvs. namn, adress och kontaktperson) på alla personuppgiftsbiträden, underleverantörer osv. tillgänglig så att de på bästa sätt kan fullgöra sina skyldigheter enligt artikel 28 i den allmänna dataskyddsförordningen, oavsett behandlingens riskbild. I detta syfte bör personuppgiftsbiträdet proaktivt förse den personuppgiftsansvarige med all denna information och hålla den uppdaterad löpande.

I artikel 28.1 i den allmänna dataskyddsförordningen föreskrivs att personuppgiftsansvariga är skyldiga att endast anlita personuppgiftsbiträden som ger "tillräckliga garantier" om att genomföra "lämpliga" åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. I detta yttrande anser EDPB att tillsynsmyndigheterna i sin bedömning av de personuppgiftsansvarigas efterlevnad av denna skyldighet och av principen om ansvarsskyldighet (artikel 24.1 i den allmänna dataskyddsförordningen) bör ta hänsyn till att anlitan av personuppgiftsbiträden inte får medföra ett försämrat skydd av de registrerades rättigheter. Den personuppgiftsansvariges *skyldighet* att kontrollera om personuppgiftsbiträdena/underentreprenörerna ger "tillräckliga garantier" om att genomföra de lämpliga åtgärder som den personuppgiftsansvarige har fastställt bör gälla oavsett risken för de registrerades rättigheter och friheter. *Omfattningen* av denna kontroll kommer dock i praktiken att variera beroende på typen av tekniska och organisatoriska åtgärder, som kan vara striktare eller mer omfattande beroende på graden av nämnda risk.

EDPB anger vidare i sitt yttrande att även om det ursprungliga personuppgiftsbiträdet bör se till att föreslå underleverantörer som ger tillräckliga garantier, ligger det slutliga beslutet om huruvida en specifik underleverantör ska anlitas och tillhörande ansvar, även i fråga om kontroll av garantierna, hos den personuppgiftsansvarige. Tillsynsmyndigheterna bör bedöma om den personuppgiftsansvarige kan visa att kontrollen av tillräckligheten hos de garantier som lämnas av dess personuppgiftsbiträden (eller underentreprenörer) har skett på ett för den personuppgiftsansvarige tillfredsställande sätt. Den personuppgiftsansvarige kan välja att förlita sig på den information som den fått från sitt personuppgiftsbiträde och vid behov komplettera den (t.ex. om den verkar ofullständig, felaktig eller ger anledning till tvivel). Vid behandling som medför en hög risk för de registrerades rättigheter och friheter bör den personuppgiftsansvarige utföra en noggrannare kontroll av den information som lämnas. I detta avseende anser EDPB att den personuppgiftsansvarige enligt den

allmänna dataskyddsförordningen inte har någon skyldighet att systematiskt begära in underleverantörsavtalen för att kontrollera om de skyldigheter i fråga om uppgiftsskydd som föreskrivs i det ursprungliga avtalet har överförts vidare i behandlingskedjan. Den personuppgiftsansvarige bör bedöma från fall till fall huruvida det är nödvändigt att begära en kopia av sådana avtal eller att när som helst granska dem för att kunna visa efterlevnad mot bakgrund av principen om ansvarsskyldighet.

Om överföringar av personuppgifter utanför EES sker mellan två personuppgiftsbiträden (eller underleverantörer) i enlighet med den personuppgiftsansvariges instruktioner, omfattas den personuppgiftsansvarige fortfarande av de skyldigheter som följer av artikel 28.1 i den allmänna dataskyddsförordningen avseende "tillräckliga garantier", utöver dem som anges i artikel 44, för att säkerställa att den skyddsnivå som garanteras genom dataskyddsförordningen inte undergrävs av överföringar av personuppgifter. Personuppgiftsbiträdet/uppgiftsutföraren bör utarbeta relevant dokumentation i enlighet med rättspraxis och i enlighet med förklaringarna i EDPB:s rekommendationer 01/2020. Den personuppgiftsansvarige bör bedöma och kunna visa den behöriga tillsynsmyndigheten sådan dokumentation. Den personuppgiftsansvarige kan välja att förlita sig på den dokumentation eller information som erhållits från personuppgiftsbiträdet/uppgiftsutföraren och vid behov komplettera den. Omfattningen och arten av den personuppgiftsansvariges skyldighet att bedöma denna dokumentation kan variera beroende på den grund som används för överföringen och huruvida överföringen utgör en inledande överföring eller en vidareöverföring.

I yttrandet behandlar EDPB också hur avtal mellan personuppgiftsansvariga och personuppgiftsbiträden bör formuleras. Ett grundläggande inslag i detta avseende är personuppgiftsbitrådets åtagande att endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte *"denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* (artikel 28.3 a i den allmänna dataskyddsförordningen) – vilket påminner om den allmänna principen att avtal inte får åsidosätta lagen. Mot bakgrund av den avtalsfrihet som personuppgiftsansvariga och personuppgiftsbiträden har för att anpassa avtalen efter sina omständigheter, inom ramen för artikel 28.3 i den allmänna dataskyddsförordningen, anser EDPB att tillägg av formuleringen *"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* (antingen ordagrant eller i mycket likartade ordalag) starkt bör rekommenderas (utan att för den skull göra det obligatoriskt).

När det gäller varianter av typen *"såvida inte denna behandling krävs enligt lag eller bindande beslut av ett statligt organ"* anser EDPB att detta ligger inom ramen för parternas avtalsfrihet och inte i sig strider mot artikel 28.3 a i den allmänna dataskyddsförordningen. Samtidigt har EDPB identifierat ett antal problem under utarbetandet av sitt yttrande, eftersom en sådan klausul inte befriar personuppgiftsbiträdet från att fullgöra sina skyldigheter enligt dataskyddsförordningen.

För personuppgifter som överförs utanför EES anser EDPB att det är osannolikt att ordalydelsen *"såvida inte denna behandling krävs enligt lag eller bindande beslut av ett statligt organ"* i sig är tillräcklig för att uppnå överensstämmelse med artikel 28.3 a i den allmänna dataskyddsförordningen läst tillsammans med kapitel V. Som framgår av Europeiska kommissionens rekommendationer avseende standardavtalsklausuler för internationella överföringar och bindande företagsbestämmelser för personuppgiftsansvariga hindrar artikel 28.3 a i den allmänna dataskyddsförordningen i princip inte att man i avtalet inför bestämmelser som tar hänsyn till krav för

behandling av överförda personuppgifter i tredjeländers lagstiftning. Liksom i dessa dokument bör dock en åtskillnad göras mellan tredjelandets lagstiftning som skulle undergräva den skyddsnivå som garanteras genom dataskyddsförordningen, och lagstiftning som inte gör det. Slutligen påminner EDPB om att risken för att tredjelandets lagstiftning hindrar efterlevnad av dataskyddsförordningen bör vara en faktor som beaktas av parterna innan de ingår avtalet (mellan personuppgiftsansvarig och personuppgiftsbiträde eller mellan personuppgiftsbiträde och underleverantör).

Personuppgiftsbiträden som behandlar personuppgifter inom EES kan under vissa omständigheter ändå ställas inför tredje lands lagstiftning. EDPB understryker att tillägget i avtalet av en formulering liknande *"såvida inte denna behandling krävs enligt lag eller bindande beslut av ett statligt organ"* inte befriar personuppgiftsbiträdet från sina skyldigheter enligt dataskyddsförordningen.

När det gäller personuppgiftsbitrådets åtagande att endast behandla uppgifter på dokumenterade instruktioner anser EDPB slutligen att *"såvida inte denna behandling krävs enligt lag eller bindande beslut av ett statligt organ"* (antingen ordagrant eller i mycket likartade ordalag) inte kan tolkas som en dokumenterad instruktion från den personuppgiftsansvarige.

Innehållsförteckning

1	Inledning.....	5
1.1	Sammanfattning av omständigheterna	5
1.2	Tillåtlighet för begäran om ett yttrande enligt artikel 64.2 i dataskyddsförordningen	7
2	Huruvida begäran är välgrundad	8
2.1	Om tolkningen av artiklarna 28.1, 28.2 och 28.4 i dataskyddsförordningen i kombination med artiklarna 5.2 och 24.1 (frågorna 1.1 och 1.3)	8
2.1.1	Identifiering av aktörerna i behandlingskedjan	9
2.1.2	Den personuppgiftsansvariges verifiering och dokumentation av att de garantier som tillhandahålls av alla personuppgiftsbiträden i behandlingskedjan är tillräckliga.....	12
2.1.3	Verifiering av avtalet mellan det ursprungliga personuppgiftsbiträdet och de ytterligare personuppgiftsbiträdena.....	18
2.2	Om tolkningen av artikel 28.1 i dataskyddsförordningen läst tillsammans med artikel 44 i dataskyddsförordningen (överföringar i behandlingskedjan – frågor 1.2 och 1.3).....	22
2.3	Om tolkningen av artikel 28.3 a i dataskyddsförordningen (fråga 2)	30

Europeiska dataskyddsstyrelsen har antagit detta yttrande

med beaktande av artiklarna 63 och 64.2 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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 (den allmänna dataskyddsförordningen, nedan kallad *dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018¹,

med beaktande av artikel 10 och artikel 22 i arbetsordningen, och

av följande skäl:

1) Den viktigaste uppgiften för Europeiska dataskyddsstyrelsen (nedan kallad dataskyddsstyrelsen eller EDPB) är att säkerställa en enhetlig tillämpning av dataskyddsförordningen inom hela Europeiska ekonomiska samarbetsområdet (EES). I artikel 64.2 i dataskyddsförordningen föreskrivs att varje tillsynsmyndighet, styrelsens ordförande eller kommissionen, i syfte att utarbeta ett yttrande får begära att en fråga med allmän räckvidd eller som har följder i mer än en EES-medlemsstat ska granskas av styrelsen. Syftet med detta yttrande är att granska en fråga med allmän räckvidd eller som har följder i mer än en EES-medlemsstat.

2) Styrelsens yttrande ska antas i enlighet med artikel 64.3 i dataskyddsförordningen, jämförd med artikel 10.2 i dataskyddsstyrelsens arbetsordning, inom åtta veckor från det datum då ordföranden och den behöriga tillsynsmyndigheten har beslutat att handlingarna i ärendet är fullständiga. På beslut av ordföranden får denna period förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1 INLEDNING

1.1 Sammanfattning av omständigheterna

1. Den 5 juli 2024 begärde den danska tillsynsmyndigheten att Europeiska dataskyddsstyrelsen (nedan kallad EDPB eller dataskyddsstyrelsen) skulle avge ett yttrande om de personuppgiftsansvarigas ansvarsskyldigheter med avseende på behandlingskedjan och förhållandet mellan de personuppgiftsansvariga och deras personuppgiftsbiträden eller underentreprenörer (underbiträden) (nedan kallad *begäran*).
2. Den 8 juli 2024 förklarade den danska tillsynsmyndigheten att handlingarna var fullständiga. Den 9 juli 2024 meddelade dataskyddsstyrelsens ordförande att handlingarna ansågs vara fullständiga.

¹ Hänvisningar till "medlemsstater" som görs i hela detta yttrande ska förstås som hänvisningar till "EES-medlemsstater". Hänvisningar till "unionen" som görs i detta yttrande ska förstås som hänvisningar till "EES".

Samma datum sändes filen av EDPB:s sekretariat. Med hänsyn till ärendets komplexitet beslutade ordföranden att förlänga den rättsliga tidsfristen i enlighet med artikel 64.3 i dataskyddsförordningen och artikel 10.4 i arbetsordningen.

3. I sin begäran hänvisar den danska tillsynsmyndigheten också till den rapport som EDPB antog i januari 2023 om resultaten av dess första samordnade verkställighetsåtgärd² inom ramen för samordnat verkställande (CEF)³. Denna samordnade åtgärd var inriktad på den offentliga sektorns användning av molntjänster. I EDPB:s rapport identifierade de tillsynsmyndigheter som deltog i den samordnade åtgärden åtta utmaningar när det gäller offentliga organs användning av molntjänster, och tillhandahöll en förteckning över punkter som berörda parter bör beakta i samband med bedömning av molntjänster och anlitande av molntjänstleverantörer⁴. För de flesta av dessa punkter är omfattningen av de skyldigheter som införs genom dataskyddsförordningen tydligt definierad för såväl personuppgiftsansvariga som personuppgiftsbiträden, men för vissa av de skyldigheter som följer av dataskyddsförordningen är den exakta omfattningen fortfarande oklar enligt den danska tillsynsmyndighetens mening⁵.

Följande frågor ställdes av den danska tillsynsmyndigheten:

4. Fråga 1.1: Mot bakgrund av artiklarna 5.2 och 24.1 i dataskyddsförordningen, när ett personuppgiftsbiträde anlitas för att utföra behandling för den personuppgiftsansvariges räkning, i syfte att dokumentera överensstämmelse med bland annat artikel 28.1 och 28.2 (inbegripet när dokumentation läggs fram för tillsynsmyndigheten vid inspektion):
- a. Måste den personuppgiftsansvarige identifiera alla personuppgiftsbitrådets underentreprenörer, deras underleverantörer osv. i hela behandlingskedjan, eller endast identifiera den första nivån av underentreprenörer som anlits av personuppgiftsbiträdet?
 - b. I vilken utsträckning och på vilken detaljnivå måste den personuppgiftsansvarige kontrollera och dokumentera följande?
 - i. Huruvida de skyddsåtgärder som tillhandahålls av personuppgiftsbiträdena, deras underleverantörer eller andra mellanhänder är tillräckliga.
 - ii. En jämförelse av innehållet i avtalen mellan det ursprungliga personuppgiftsbiträdet och de ytterligare personuppgiftsbiträdena, för att kontrollera att samma skyldigheter har ålagts de ytterligare personuppgiftsbiträdena i enlighet med artikel 28.4 i dataskyddsförordningen.
 - iii. Huruvida personuppgiftsbiträdena, deras underentreprenörer osv. uppfyller de krav som åligger den personuppgiftsansvarige enligt artikel 28.1?
5. Fråga 1.2: Vid överföringar eller vidareöverföringar från ett personuppgiftsbiträde (eller en underentreprenör) till ett annat personuppgiftsbiträde (eller en annan underentreprenör) i enlighet med den personuppgiftsansvariges instruktioner: I vilken utsträckning måste den personuppgiftsansvarige, som en del av sin skyldighet enligt artikel 28.1 i dataskyddsförordningen läst tillsammans med artikel 44 i samma förordning, bedöma och kunna framlägga dokumentation från

² Rapport om 2022 års samordnade verkställighetsåtgärder – den offentliga sektorns användning av molnbaserade tjänster, 17 januari 2023 (nedan kallad *CEF-rapporten om molntjänster*).

³ Den samordnade ramen för verkställande inrättades av EDPB i oktober 2020 i syfte att effektivisera kontrollen av verkställigheten och samarbetet mellan tillsynsmyndigheterna. Se EDPB:s dokument om en ram för samordnat verkställande enligt förordning 2016/679, som antogs den 20 oktober 2020, version 1.1.

⁴ CEF:s rapport om molntjänster, s. 10–20.

⁵ Fråga, s. 1.

personuppgiftsbiträden (eller deras underentreprenörer) som visar att skyddsnivån för personuppgifter inte undergrävs av (vidare)överföringarna?

6. Fråga 1.3: Varierar omfattningen av skyldigheterna enligt artikel 28.1 och 28.2 i dataskyddsförordningen, lästa tillsammans med artiklarna 5.2 och 24 i samma förordning, såsom de har definierats i frågorna 1.1 och 1.2, beroende på den risk som är förenad med behandlingen? Om så är fallet, vilken är omfattningen av sådana skyldigheter vid personuppgiftsbehandlingar förenade med låg risk och vilken är omfattningen för personuppgiftsbehandlingar med hög risk?
7. Fråga 2: Måste ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt i enlighet med artikel 28.3 i dataskyddsförordningen innehålla det undantag som föreskrivs i artikel 28.3 a *"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* (antingen ordagrant eller i mycket likartade ordalag) för att vara förenliga med dataskyddsförordningen?
8. Fråga 2a: Om svaret på fråga 2 är nej och det upprättas ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt som utvidgar undantaget i artikel 28.3 a i dataskyddsförordningen så att det även omfattar tredjelandslagstiftning i allmänhet (t.ex. *"såvida inte detta krävs enligt lag eller bindande beslut av ett statligt organ"*), är detta i sig en överträdelse av artikel 28.3 a i dataskyddsförordningen?
9. Fråga 2b: Om svaret på fråga 2a är nej, ska ett sådant utvidgat undantag i stället tolkas som en dokumenterad instruktion från den personuppgiftsansvarige i den mening som avses i artikel 28.3 a i dataskyddsförordningen?

1.2 Tillåtlighet för begäran om ett yttrande enligt artikel 64.2 i dataskyddsförordningen

10. I artikel 64.2 i dataskyddsförordningen föreskrivs specifikt att varje tillsynsmyndighet, i syfte att erhålla ett yttrande, får begära att en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat ska granskas av dataskyddsstyrelsen.
11. De första frågorna från den danska tillsynsmyndigheten (frågorna 1.1, 1.2 och 1.3) avser de personuppgiftsansvarigas ansvarsskyldigheter enligt artikel 28 i dataskyddsförordningen, medan den sista (fråga 2) avser det specifika innehållet i avtalet eller rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt artikel 28.3 a i dataskyddsförordningen.
12. Dataskyddsstyrelsen anser att dessa frågor rör tolkningen av dataskyddsförordningen, särskilt när det gäller förhållandet mellan de personuppgiftsansvariga och deras personuppgiftsbiträden (eller underentreprenörer) och tolkningen av artiklarna 5.2, 24 och 28 i den förordningen. Begäran rör, å ena sidan, de personuppgiftsansvarigas ansvarsskyldigheter och den nivå av dokumentation som tillsynsmyndigheterna bör förvänta sig av alla personuppgiftsansvariga som anlitar personuppgiftsbiträden (eller deras underentreprenörer) för att utföra behandling för deras räkning och, å andra sidan, innehållet i avtalen eller rättsakterna mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Denna begäran avser därför en *fråga med allmän räckvidd* i den mening som avses i artikel 64.2 i dataskyddsförordningen.
13. Dessutom anser styrelsen att begäran från den danska tillsynsmyndigheten är motiverad i enlighet med artikel 10.3 i dataskyddsstyrelsens arbetsordning, eftersom den danska tillsynsmyndigheten har lagt fram argument för behovet av en konsekvent tolkning av de frågor som tas upp i begäran.

14. Enligt artikel 64.3 i dataskyddsförordningen ska EDPB inte avge ett yttrande om den redan har avgivit ett yttrande i ärendet⁶. EDPB har ännu inte gett svar på de frågor som ingår i den danska tillsynsmyndighetens begäran. Vidare ger EDPB:s tillgängliga riktlinjer, särskilt EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR⁷ (nedan kallade *EDPB:s riktlinjer 07/2020*), viss vägledning om omfattningen av den personuppgiftsansvariges ansvarsskyldigheter enligt artikel 28 i dataskyddsförordningen, men den befintliga vägledningen behandlar inte till fullo alla de frågor som anges i begäran⁸. Den vägledning som finns tillgänglig avseende artikel 28.3 a i dataskyddsförordningen behandlar till exempel inte specifikt den fråga som ingår i den danska tillsynsmyndighetens begäran om huruvida ordalydelsen *"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* bör inkluderas i avtal eller rättsakter mellan personuppgiftsansvariga och personuppgiftsbiträden.
15. Av dessa skäl anser dataskyddsstyrelsen att den danska tillsynsmyndighetens begäran är tillåtlig och att de frågor som uppstår till följd av den danska tillsynsmyndighetens begäran bör analyseras i ett yttrande som antas i enlighet med artikel 64.2 i dataskyddsförordningen.

2 HURUVIDA BEGÄRAN ÄR VÄLGRUNDADERROR! BOOKMARK NOT DEFINED.

2.1 Om tolkningen av artiklarna 28.1, 28.2 och 28.4 i dataskyddsförordningen i kombination med artiklarna 5.2 och 24.1 (frågorna 1.1 och 1.3)

16. I detta avsnitt behandlas frågorna 1.1 och 1.3 som ställts till dataskyddsstyrelsen och som återges i avsnittet om tillåtlighet ovan.
17. I artikel 28 i dataskyddsförordningen fastställs förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet. I den artikeln åläggs personuppgiftsansvariga och personuppgiftsbiträden direkta skyldigheter. Inledningsvis bör det noteras att dataskyddsförordningen i artikel 4.8 definierar "personuppgiftsbiträde" på ett allmänt sätt som omfattar både det ursprungliga personuppgiftsbiträdet som anlitas direkt av den personuppgiftsansvarige och personuppgiftsbiträdets personuppgiftsbiträde (underentreprenör), och så vidare längs hela behandlingskedjan.
18. EDPB understryker att bedömningen av parternas roller (och huruvida de agerar som ensamma eller gemensamma personuppgiftsansvariga, eller som personuppgiftsbiträden) faller utanför tillämpningsområdet för begäran. Dataskyddsstyrelsen påminner om att det i första hand är upp till parterna att bedöma rollfördelningen utifrån ärendets faktiska element eller omständigheter⁹, utan att det påverkar tillsynsmyndighetens behörighet att kontrollera huruvida deras bedömning är korrekt.
19. Mot bakgrund av frågorna ovan inriktar sig detta yttrande enbart på omfattningen och räckvidden av den personuppgiftsansvariges skyldigheter enligt artikel 28.1 i dataskyddsförordningen, dvs. att

⁶ Artikel 64.3 i dataskyddsförordningen och artikel 10.4 i dataskyddsstyrelsens arbetsordning.

⁷ EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR), version 2.1, antagna den 7 juli 2021.

⁸ Se särskilt EDPB:s riktlinjer 07/2020, avsnitt 1.1 "Val av personuppgiftsbiträde" på sidan 30, avsnitt 1.3.4 "Personuppgiftsbiträdet måste respektera de villkor som avses i artikel 28.2 och 28.4 för att anlita ett annat personuppgiftsbiträde (artikel 28.3 d i dataskyddsförordningen)" på sidan 37, avsnitt 1.6 "Underbiträden", på sidan 42.

⁹ EDPB:s riktlinjer 07/2020, punkt 12.

kontrollera om personuppgiftsbiträdena (eller underentreprenörerna) lämnar "tillräckliga garantier" enligt artikel 28.2, och av den personuppgiftsansvariges motsvarande ansvarsskyldigheter enligt artiklarna 5.2 och 24.1 i dataskyddsförordningen¹⁰.

20. Dataskyddsstyrelsen noterar dessutom att ovanstående frågor inte rör den personuppgiftsansvariges ansvar gentemot de registrerade för den behandling som utförs för den personuppgiftsansvariges räkning, till exempel när det gäller registrerades rätt till ersättning enligt artikel 82 i dataskyddsförordningen. Detta avsnitt kommer därför att inriktas på att klargöra för tillsynsmyndigheterna hur artiklarna 28.1 och 28.2 i dataskyddsförordningen ska tolkas i kombination med artiklarna 5.2 och 24 i dataskyddsförordningen när det gäller vissa skyldigheter som följer av att ett eller flera personuppgiftsbiträden och underleverantörer anlitas. För att besvara dessa frågor kommer dataskyddsstyrelsen att genomföra en analys med fokus på situationer där det inte sker någon överföring av personuppgifter utanför EES. I avsnittet nedan, som rör fråga 1.2, bedöms däremot situationer där det sker överföringar längs behandlingskedjan.

2.1.1 Identifiering av aktörerna i behandlingskedjan

21. När det gäller frågan om huruvida den personuppgiftsansvarige i huvudsak bör identifiera alla personuppgiftsbitrådets underentreprenörer, dessas underbiträden osv. genom hela behandlingskedjan, eller endast identifiera den första nivån av underentreprenörer som personuppgiftsbitrådet anlitar, erinrar EDPB för det första om att *"Även om [behandlings]kedjan kan vara ganska lång, behåller den personuppgiftsansvarige sin avgörande roll vad gäller bestämmande av behandlingsändamål och behandlingssätt"*¹¹.
22. EDPB tolkar begreppen "identifiera" och "information om identiteten" som syftande till att besvara frågan som rör namn, adress, kontaktperson (namn, befattning, kontaktuppgifter) för personuppgiftsbitrådet och beskrivningen av uppgiftsbehandlingen (inklusive en tydlig avgränsning av ansvarsområden om flera underentreprenörer har godkänts)¹².
23. När det gäller valet av personuppgiftsbiträden bör den personuppgiftsansvarige befinna sig i en position som gör det möjligt att effektivt fastställa ändamålen och medlen för uppgiftsbehandlingen i enlighet med artikel 4.7 i dataskyddsförordningen. I detta avseende anses fastställandet av mottagare (inklusive personuppgiftsbiträden) vara ett "väsentligt medel" för den uppgiftsbehandling som den personuppgiftsansvarige beslutar om¹³.

¹⁰ Denna fråga skiljer sig från alla andra skyldigheter för den personuppgiftsansvarige (eller personuppgiftsbiträdena/underentreprenörerna) för att säkerställa efterlevnaden av dataskyddsförordningen, t.ex. principen om laglighet, artikel 32 eller skyldigheterna enligt kapitel V i samma förordning. Den personuppgiftsansvarige kan fortfarande vara ansvarig för behandling under sitt personuppgiftsansvar som inte är förenlig med sådana bestämmelser i dataskyddsförordningen, även om han eller hon har uppfyllt skyldigheten att kontrollera sina personuppgiftsbiträden (eller deras underentreprenörer) i enlighet med artikel 28.1 i dataskyddsförordningen enligt vad som beskrivs i detta yttrande, och detta yttrande behandlar inte den personuppgiftsansvariges ansvar för efterlevnaden av andra bestämmelser i dataskyddsförordningen än dem som anges i artiklarna 24.1, 28.1 och 28.2 i den förordningen.

¹¹ EDPB:s riktlinjer 07/2020, punkt 152.

¹² Detta speglar den information som krävs för identifiering av personuppgiftsbiträden i bilaga IV till Europeiska kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden (kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021) och bilaga III till Europeiska kommissionens standardavtalsklausuler för överföring av personuppgifter till tredjeländer (kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021).

¹³ EDPB:s riktlinjer 07/2020, punkt 40.

24. För detta ändamål, med avseende på anlitande av **ytterligare personuppgiftsbiträden** av det ursprungliga personuppgiftsbiträdet, krävs ett specifikt eller allmänt skriftligt godkännande på förhand från den personuppgiftsansvarige enligt artikel 28.2 i dataskyddsförordningen. I EDPB:s riktlinjer 07/2020 klargjordes att de skyldigheter som föreskrivs i artikel 28.2 *"utlöses när ett (under)personuppgiftsbiträde avser att anlita en annan aktör och därigenom lägger till ytterligare en länk i kedjan genom att anförtro denne aktiviteter som kräver behandling av personuppgifter"*¹⁴.
25. I fall där den personuppgiftsansvarige beslutar att godkänna vissa underentreprenörer vid tidpunkten för avtalets undertecknande bör en lista över godkända underbiträden ingå i avtalet eller i en bilaga till detta. Listan bör därefter hållas uppdaterad i enlighet med det allmänna eller specifika tillstånd som utfärdas av den personuppgiftsansvarige¹⁵.
26. När det gäller anlitande av underentreprenörer föreskrivs i dataskyddsförordningen möjligheten att utfärda ett allmänt eller ett specifikt tillstånd. **Vid ett specifikt tillstånd** måste den personuppgiftsansvarige skriftligen ange vilken underentreprenör och vilken behandlingsaktivitet som hänvisas till, samt under vilken tid¹⁶. Om personuppgiftsbitrådets begäran om ett specifikt godkännande inte besvaras inom den angivna tidsramen bör det anses som nekat¹⁷.
27. **Vid ett allmänt tillstånd** ska personuppgiftsbiträdet ge den personuppgiftsansvarige möjlighet att godkänna en förteckning över underentreprenörer vid tidpunkten för undertecknandet av det allmänna tillståndet, samt ge den personuppgiftsansvarige tillräckligt med tid för att kunna invända mot eventuella senare ändringar av de underentreprenörer som ingår i förteckningen¹⁸. Dataskyddsstyrelsen påminner om att det bör vara upp till det ursprungliga **personuppgiftsbiträdet att proaktivt tillhandahålla viss information** till den personuppgiftsansvarige, och *"personuppgiftsbitrådets skyldighet att informera den personuppgiftsansvarige om eventuella ändringar av underentreprenörer innebär att personuppgiftsbiträdet **aktivt** delger eller flaggar sådana ändringar gentemot den personuppgiftsansvarige"*¹⁹.
28. Detta innebär att informationen som rör identifieringen av alla personuppgiftsbitrådets underbiträden bör vara lätt tillgänglig för den personuppgiftsansvarige. Identifieringen av dessa aktörer är särskilt

¹⁴ EDPB:s riktlinjer 07/2020, punkt 151, har följande lydelse: *"Databehandlingsaktiviteter utförs ofta av ett stort antal aktörer, och underleverantörskedjorna blir allt mer komplexa. GDPR inför specifika skyldigheter som träder i kraft när ett (under-)personuppgiftsbiträde avser att anlita en annan aktör och därigenom lägger till ytterligare en länk till kedjan genom att anförtro denne aktiviteter som kräver behandling av personuppgifter. Analysen av huruvida tjänsteleverantören fungerar som ett underbiträde bör utföras i enlighet med vad som beskrivits ovan angående begreppet personuppgiftsbiträde"*.

¹⁵ EDPB:s riktlinjer 07/2020, punkt 154.

¹⁶ EDPB:s riktlinjer 07/2020, punkterna 153 och 155. Enligt klausul 7.7 alternativ 1 i kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden ska förteckningen över de underentreprenörer som uttryckligen godkänts av den personuppgiftsansvarige återfinnas i bilaga IV, som ska hållas uppdaterad av parterna.

¹⁷ EDPB:s riktlinjer 07/2020, punkt 155.

¹⁸ Se även EDPB:s riktlinjer 07/2020, punkt 156: *"Alternativt kan den personuppgiftsansvarige ge sitt allmänna tillstånd för användning av underentreprenörer (i avtalet, kompletterat med en lista över sådana underentreprenörer i en bifogad bilaga) (...)"*. Relevant i detta sammanhang är också EDPB:s yttrande 14/2019 om utkastet till standardavtalsklausuler som lämnats in av den danska tillsynsmyndigheten (artikel 28.8 i dataskyddsförordningen). Enligt klausul 7.7 alternativ 2 i Europeiska kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden har personuppgiftsbiträdet den personuppgiftsansvariges allmänna tillstånd att anlita underentreprenörer från en överenskommen förteckning och ska skriftligen informera den personuppgiftsansvarige på förhand om ändringar av förteckningen planeras genom att underleverantörer läggs till eller ersätts.

¹⁹ EDPB:s riktlinjer 07/2020, punkt 128 (fetstil tillagd). Se även fotnot 14.

relevant för att den personuppgiftsansvarige ska kunna ha kontroll över den behandling av personuppgifter som denne ansvarar för och kan hållas ansvarig för i händelse av en överträdelse av dataskyddsförordningen.

29. Personuppgiftsbiträdet bör därför tillhandahålla all information om hur behandlingen kommer att utföras för den personuppgiftsansvariges räkning, inklusive information om den underentreprenör som används²⁰ och en beskrivning av den behandling som anförtros underentreprenören²¹.
30. Andra rättsliga skäl motiverar behovet av att den personuppgiftsansvarige identifierar alla personuppgiftsbiträden och underentreprenörer. Personuppgiftsbiträden till vilka uppgifter lämnas ut eller överförs betraktas som "mottagare"²².
 - För att uppfylla öppenhetskraven enligt artiklarna 13.1 e och 14.1 e i dataskyddsförordningen bör personuppgiftsansvariga informera de registrerade om uppgiftsmottagarna eller kategorierna av uppgiftsmottagare och vara så specifika och konkreta som möjligt²³. Uppgifter om "kategorier av mottagare" måste också ingå i registren över behandling (artikel 30.1 d).
 - I artikel 15 i dataskyddsförordningen föreskrivs rätten till tillgång till bland annat information om de mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats ut eller kommer att lämnas ut²⁴. EU-domstolen klargjorde att denna bestämmelse innebär en skyldighet för den personuppgiftsansvarige att förse den registrerade med mottagarnas faktiska identitet²⁵. Bortsett från den typ av fall där den personuppgiftsansvarige endast får

²⁰ EDPB:s riktlinjer 7/2020, punkt 143.

²¹ Se t.ex. bilaga IV till kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och bilaga II till kommissionens standardavtalsklausuler för internationella överföringar.

²² Artikel 4.9 i dataskyddsförordningen; artikel 29-gruppens riktlinjer om öppenhet enligt förordning 2016/679, antagna den 29 november 2017, senast reviderade och antagna den 11 april 2018, WP260 rev.01, godkända av EDPB (nedan kallade *artikel 29-gruppens riktlinjer om öppenhet*), s. 37.

²³ Artikel 29-gruppens riktlinjer om öppenhet, s. 37 ("*Enligt rättvisepincipen måste de personuppgiftsansvariga ge sådan information om mottagarna som är mest relevant för de registrerade. I praktiken är detta mottagarnas namn, så att de registrerade vet exakt vem som har deras personuppgifter. Om de personuppgiftsansvariga väljer att ange kategorier av mottagare bör informationen vara så specifik som möjligt och innehålla uppgift om typen av mottagare (dvs. med hänvisning till den verksamhet som denne bedriver), bransch, sektor, undersektor och mottagarnas belägenhet*"; EDPB:s riktlinjer 01/2022 om registrerades rättigheter – Rätt till tillgång, version 2.1, antagna den 28 mars 2023, (nedan kallade *EDPB:s riktlinjer 01/2022 (rätt till tillgång)*), punkt 117 ("*[information om mottagarna eller kategorierna av mottagare] redan enligt artiklarna 13 och 14 i dataskyddsförordningen bör vara så konkret som möjligt när det gäller principerna om insyn och rättvisa*". se EU-domstolens dom av den 12 januari 2023, *RW mot Österreichische Post AG*, C-154/21, punkt 25, AG:s yttrande om EU-domstolens dom C-154/21, punkt 36 ("*artiklarna 13 och 14 i dataskyddsförordningen [...] föreskriver en skyldighet för den personuppgiftsansvarige att förse den registrerade med information om kategorierna av mottagare eller de specifika mottagarna av personuppgifter som rör honom eller henne när personuppgifter samlas in från den registrerade och om personuppgifterna inte har erhållits från den registrerade*").

²⁴ Artikel 15.1 c i dataskyddsförordningen. EDPB:s riktlinjer 01/2022 (rätt till tillgång), punkterna 116–117.

²⁵ EU-domstolens dom av den 12 januari 2023, *RW mot Österreichische Post AG*, C-154/21, punkt 51: "*Artikel 15.1 c i dataskyddsförordningen ska tolkas så, att rätten för den registrerade att få tillgång till personuppgifter som rör honom eller henne, vilken föreskrivs i denna bestämmelse, innebär – när uppgifterna har lämnats ut eller ska lämnas ut till mottagare – att den personuppgiftsansvarige är skyldig att ge den registrerade den faktiska identiteten på dessa mottagare, såvida det inte är omöjligt att identifiera mottagarna eller den personuppgiftsansvarige visar att den registrerades begäran om tillgång är uppenbart ogrundad eller orimlig i*

ange kategorierna av mottagare för den registrerade, bör det i princip alltid vara möjligt för den personuppgiftsansvarige att utan onödigt dröjsmål inhämta namnen på mottagarna och lämna nödvändig information till de registrerade.

- I artikel 19 i dataskyddsförordningen föreskrivs att den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. EU-domstolen klargjorde att den andra meningen i artikel 19 uttryckligen ger den registrerade rätt att få information om de specifika mottagarnas identitet²⁶.

31. Även om det inte uttryckligen framgår av dessa bestämmelser anser dataskyddsstyrelsen att personuppgiftsansvariga, vid tillämpningen av artikel 28.1 och 28.2 i dataskyddsförordningen, alltid bör ha information om identiteten på alla personuppgiftsbiträden, underbiträden och andra eventuella mellanhänder lätt tillgänglig²⁷, så att de på bästa sätt kan fullgöra sina skyldigheter enligt de bestämmelser som nämns ovan. Att säkerställa sådan tillgång är också nödvändigt för att personuppgiftsansvariga ska kunna samla in och bedöma all den information som krävs för att uppfylla kraven i dataskyddsförordningen, bland annat så att de utan onödigt dröjsmål kan besvara begäranden om tillgång enligt artikel 15 i dataskyddsförordningen och snabbt kan reagera vid eventuella dataintrång längs behandlingskedjan. Detta bör gälla oberoende av den risk som är förknippad med behandlingen.
32. I detta syfte bör personuppgiftsbiträdet proaktivt förse²⁸ den personuppgiftsansvarige med all information om identiteten på alla personuppgiftsbiträden, underentreprenörer osv. som behandlar uppgifter för den personuppgiftsansvariges räkning, och bör hålla informationen om alla involverade underentreprenörer ständigt uppdaterad. Den personuppgiftsansvarige och personuppgiftsbiträdet kan i avtalet lägga till ytterligare detaljer om hur och i vilket format personuppgiftsbiträdet ska tillhandahålla denna information, med tanke på att den personuppgiftsansvarige kan vilja begära ett specifikt format som gör det lättare för denne att hämta och organisera informationen.

2.1.2 Den personuppgiftsansvariges verifiering och dokumentation av att de garantier som tillhandahålls av alla personuppgiftsbiträden i behandlingskedjan är tillräckliga

33. Frågorna 1.1.b.i, 1.1.b.iii och 1.3 syftar till att klargöra i vilken utsträckning och på vilken detaljnivå den personuppgiftsansvarige bör kontrollera och dokumentera att de skyddsåtgärder som tillhandahålls av

den mening som avses i artikel 12.5 i dataskyddsförordningen. I sådant fall är det tillräckligt att den personuppgiftsansvarige informerar den registrerade om de aktuella kategorierna av mottagare”.

Domstolen meddelade att den registrerade också kan ”välja att endast begära upplysningar om kategorierna av mottagare”. EU-domstolens dom av den 12 januari 2023, *RW mot Österreichische Post AG*, C-154/21, punkt 43. EDPB:s riktlinjer 01/2022 (rätt till tillgång), punkt 117.

²⁶ EU-domstolens dom av den 12 januari 2023, *RW mot Österreichische Post AG*, C-154/21, punkt 41.

²⁷ Denna information är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra sina skyldigheter även om underbiträdenas behandlingskedja bryts på grund av att ett personuppgiftsbiträde (eller en underentreprenör) inte kan nå, vägrar att medverka eller är insolvent och ett annat personuppgiftsbiträde (eller en underentreprenör) måste kontaktas.

²⁸ I syfte att uppfylla kraven i artikel 28.2 i dataskyddsförordningen, för att göra det möjligt för den personuppgiftsansvarige att besluta om tillägg av underbiträden, samt i syfte att följa artikel 28.1 i den förordningen, för att göra det möjligt för den personuppgiftsansvarige att kontrollera om personuppgiftsbiträdena (eller underentreprenörerna) ger tillräckliga garantier för att genomföra de tekniska och organisatoriska åtgärderna.

alla personuppgiftsbiträden i behandlingskedjan är tillräckliga och i vilken utsträckning skyldigheterna enligt artiklarna 28.1 och 28.2 i dataskyddsförordningen lästa tillsammans med artiklarna 5.2 och 24 i den förordningen varierar beroende på den risk som är förknippad med behandlingen. När det gäller dessa frågor understryker dataskyddsstyrelsen följande element.

34. I artikel 5.2 i dataskyddsförordningen stadfästs principen om ansvarsskyldighet genom att den personuppgiftsansvarige görs ansvarig för efterlevnaden av dataskyddsprinciperna i artikel 5.1 i dataskyddsförordningen och för att kunna påvisa denna efterlevnad. Artikel 5.2 i dataskyddsförordningen gäller för alla de allmänna principer som anges i artikel 5.1 i samma förordning.
35. Artikel 24.1 i dataskyddsförordningen omfattar den personuppgiftsansvariges skyldighet att visa att behandlingen utförs i enlighet med dataskyddsförordningen men i den artikeln vidareutvecklas en av de uppgifter som principen om ansvarsskyldighet är tillämplig på, nämligen genomförandet av "lämpliga tekniska och organisatoriska åtgärder"²⁹. I artikel 24.1 i dataskyddsförordningen hänvisas till att begreppet "risk"³⁰ är relevant för dess tillämpning, då risknivån är ett av de kriterier som den personuppgiftsansvarige måste beakta vid bedömningen av huruvida sådana åtgärder är lämpliga³¹. I artikel 24.1 i dataskyddsförordningen anges också att dessa åtgärder ska ses över och uppdateras vid behov.

²⁹ Dom av den 25 januari 2024, *BL mot MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, punkt 36: "I artikel 24 i dataskyddsförordningen föreskrivs en allmän skyldighet för den personuppgiftsansvarige att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter sker i överensstämmelse med förordningen, och att kunna visa detta".

³⁰ I skäl 75 i dataskyddsförordningen anges några exempel på risker: "behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel". I skäl 76 anges vidare: "Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk". Som EU-domstolen sammanfattat saken "framgår det av skäl 76 i förordningen att sannolikheten för att riskerna ska förverkligas och hur allvarliga de är beror på omständigheterna kring den aktuella personuppgiftsbehandlingen och att risken bör bedömas objektivt". (EU-domstolens dom av den 14 december 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punkt 36).

³¹ EU-domstolen anförde följande: "För detta ändamål anges i artikel 24.1 ett antal faktorer som ska beaktas vid bedömningen av huruvida de vidtagna åtgärderna är lämpliga, nämligen behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter", dom av den 14 december 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, punkt 25. I samma dom preciserade EU-domstolen att "Bedömningen av om sådana åtgärder är lämpliga ska ske utifrån de konkreta omständigheterna i det enskilda fallet. I bedömningen ingår att ta ställning till om den personuppgiftsansvarige vid genomförandet av åtgärderna har beaktat de olika faktorer som avses [...] och de skyddsbehov som särskilt gör sig gällande i samband med den aktuella personuppgiftsbehandlingen samt därmed förenade risker", punkt 30; om detta erinrades det också om i dom C-687/21 av den 25 januari 2024, *BL/MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72, punkt 38: "Det framgår således av ordalydelsen i artiklarna 24 och 32 i dataskyddsförordningen att lämpligheten av de åtgärder som den personuppgiftsansvarige vidtar ska bedömas på ett konkret sätt, med beaktande av de olika faktorer som avses i nämnda artiklar och de skyddsbehov som särskilt gör sig gällande i samband med den aktuella personuppgiftsbehandlingen samt därmed förenade risker, och detta särskilt som den personuppgiftsansvarige måste kunna visa att dessa åtgärder är förenliga med förordningen, vilket den personuppgiftsansvarige inte skulle ha möjlighet att göra om det ansågs föreligga en sådan icke motbevisbar presumtion". Det måste noteras att EU-domstolens analys även avser artikel 32 i dataskyddsförordningen.

36. EU-domstolen konstaterade att "[...] artiklarna 5.2 och 24 i allmänna dataskyddsförordningen innebär att de personuppgiftsansvariga åläggs generella krav avseende ansvarsskyldighet och efterlevnad. Dessa bestämmelser kräver särskilt att de personuppgiftsansvariga, för att garantera rätten till dataskydd, ska vidta lämpliga åtgärder för att förhindra eventuella åsidosättanden av reglerna i allmänna dataskyddsförordningen"³².
37. Ansvarsskyldighetsprincipen gäller för den personuppgiftsansvarige, även när den personuppgiftsansvarige har anförtrott personuppgiftsbiträden eller underbiträden att behandla personuppgifter för deras räkning.
38. Enligt artikel 28.1 i dataskyddsförordningen måste en personuppgiftsansvarig, när den anlitar ett personuppgiftsbiträde för att utföra behandling av personuppgifter för dess räkning, endast använda ett personuppgiftsbiträde som ger *"tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven"* i dataskyddsförordningen *"och säkerställer att den registrerades rättigheter skyddas"*³³. Såsom anges i EDPB:s riktlinjer 07/2020 återspeglas också principen om ansvarsskyldighet i artikel 28 i dataskyddsförordningen³⁴.
39. I detta avseende framhåller EDPB att tillsynsmyndigheterna i syfte att bedöma efterlevnaden av artiklarna 24.1 och 28.1 i dataskyddsförordningen bör beakta att **anlitande av personuppgiftsbiträden inte får medföra ett sämre skydd för de registrerades rättigheter** än om behandlingen skulle utföras direkt av den personuppgiftsansvarige. Detta avser anlitandet av det ursprungliga personuppgiftsbiträdet, men också anlitande av andra personuppgiftsbiträden längs behandlingskedjan, t.ex. underentreprenörer och deras eventuella underentreprenörer i sin tur. Artiklarna 24.1 och 28.1 i dataskyddsförordningen bör tolkas som att den personuppgiftsansvarige måste se till att behandlingskedjan endast består av personuppgiftsbiträden och underentreprenörer (i alla förekommande led) som ger *"tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder"*. Dessutom bör den personuppgiftsansvarige kunna bevisa att den har tagit vederbörlig hänsyn till alla relevanta delar av dataskyddsförordningen³⁵. Dessa överväganden gäller även om behandlingskedjan kan vara lång och komplex med olika personuppgiftsbiträden, underentreprenörer osv. inblandade i olika skeden av uppgiftsbehandlingsaktiviteterna. Den personuppgiftsansvarige bör utöva tillbörlig aktsamhet vid valet av och kontrollen över sina personuppgiftsbiträden.
40. När det gäller valet av **ursprungligt personuppgiftsbiträde** bör den personuppgiftsansvarige från fall till fall kontrollera att de garantier som tillhandahålls är tillräckliga, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter, på grundval av den typ av behandling som personuppgiftsbiträdet anförtrotts³⁶. I enlighet med artikel 28.5 i dataskyddsförordningen får ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod som avses i artikel 40 i dataskyddsförordningen eller en godkänd certifieringsmekanism som avses i artikel 42 i samma förordning användas för att visa att tillräckliga garantier tillhandahålls.

³² Dom C-129/21 av den 27 oktober 2022, *Proximus NV (Allmänna elektroniska abonnentförteckningar) mot Gegevensbeschermingsautoriteit*, ECLI:EU:C:2022:833, punkt 81. Se även EDPB:s riktlinjer 07/2020, punkt 9.

³³ EDPB:s riktlinjer 07/2020, punkt 94.

³⁴ EDPB:s riktlinjer 07/2020, punkt 8.

³⁵ EDPB:s riktlinjer 07/2020, punkt 94.

³⁶ EDPB:s riktlinjer 07/2020, punkt 96.

41. Såsom tidigare nämnts av EDPB bör den personuppgiftsansvarige ta hänsyn till flera faktorer vid kontrollen av de garantier som tillhandahålls av personuppgiftsbiträdena³⁷, och ett utbyte av relevant dokumentation kan ofta krävas³⁸. Under alla omständigheter gäller att "[g]arantierna "som tillhandahålls" av personuppgiftsbiträdet är de som personuppgiftsbiträdet kan uppvisa för att tillfredsställa den personuppgiftsansvariges krav eftersom de är de enda som effektivt kan beaktas av den personuppgiftsansvarige vid bedömningen av efterlevnaden av sina skyldigheter"³⁹. Varken artikel 28.1 i dataskyddsförordningen i sig eller tidigare EDPB-dokument innehåller någon uttömmande förteckning över dokument eller åtgärder som personuppgiftsbiträdet ska uppvisa, eftersom detta i stor utsträckning beror på de specifika omständigheterna för behandlingen⁴⁰. Den personuppgiftsansvarige kan till exempel välja att ta fram ett frågeformulär som ett sätt att samla in information från sitt personuppgiftsbiträde för att kontrollera de relevanta garantierna eller begära relevant dokumentation. Den personuppgiftsansvarige kan också förlita sig på offentligt tillgänglig information och/eller certifieringar eller granskningsrapporter från tillförlitliga tredje parter och/eller utföra granskningar på plats.
42. EDPB har redan angett att skyldigheten att endast använda personuppgiftsbiträden som "ger tillräckliga garantier" enligt artikel 28.1 i dataskyddsförordningen är en kontinuerlig förpliktelse och att den personuppgiftsansvarige med lämpliga mellanrum bör verifiera personuppgiftsbiträdets garantier⁴¹.
43. Mot bakgrund av fråga 1.3 i den danska tillsynsmyndighetens begäran, om risken som är kopplad till behandlingen, betonar EDPB att begreppet risk spelar en viktig roll i många av dataskyddsförordningens bestämmelser, särskilt de som rör kapitel IV i dataskyddsförordningen⁴².
44. Det är viktigt att betona att hänvisningen till risk i artikel 24.1 och skäl 74 i dataskyddsförordningen inte bör tolkas som att den personuppgiftsansvarige kan åsidosätta eller avvika från sina skyldigheter enligt dataskyddsförordningen på grundval av enbart det faktum att den anser att risken för registrerades rättigheter och friheter är liten. Skyldigheten att genomföra "lämpliga tekniska och organisatoriska åtgärder" för att säkerställa efterlevnaden av dataskyddsförordningen i linje med artikel 24.1 i den förordningen gäller alltid, men de åtgärder som krävs för att uppnå detta resultat kan variera beroende på risken⁴³.

³⁷ EDPB:s riktlinjer 07/2020, punkterna 97–98 (om personuppgiftsbiträdets expertkunskap, tillförlitlighet och resurser, liksom personuppgiftsbiträdets rykte på marknaden och efterlevnaden av en godkänd uppförandekod eller certifieringsmekanism).

³⁸ EDPB:s riktlinjer 07/2020, punkt 95 (där några exempel nämns: integritetspolicy, användarvillkor, register över behandlingsaktiviteter, registerhanteringspolicy, informationssäkerhetspolicy, rapporter om externa dataskyddsgranskningar, erkända internationella certifieringar, som ISO 27000-serien).

³⁹ EDPB:s riktlinjer 07/2020, punkt 95.

⁴⁰ EDPB:s riktlinjer 07/2020, punkt 96 ("*Den personuppgiftsansvariges bedömning av om garantierna är tillräckliga är en form av riskbedömning, som i hög grad beror på vilken typ av behandling som anförtrots personuppgiftsbiträdet och måste göras från fall till fall, med hänsyn till karaktär, omfattning, sammanhang och syften med behandlingen samt riskerna för fysiska personers rättigheter och friheter. Som en konsekvens kan EDPB inte tillhandahålla en uttömmande lista över de dokument eller åtgärder som personuppgiftsbiträdet behöver uppvisa eller inge i ett givet scenario, eftersom detta i hög grad beror på de specifika omständigheterna för behandlingen*").

⁴¹ EDPB:s riktlinjer 07/2020, punkt 99: "*genom granskningar och inspektioner där så är lämpligt*".

⁴² Begreppet risk behandlas i artiklarna 24, 25, 27, 30, 32, 33, 34, 35, 36 och 39 i dataskyddsförordningen.

⁴³ EU-domstolens dom C-340/21 av den 14 december 2023, *Natsionalna agentsia za prihodite*, EU:C:2023:986, punkt 35: "*I skäl 74 i dataskyddsförordningen betonas dessutom att den personuppgiftsansvarige bör vara skyldig att vidta lämpliga och effektiva åtgärder och kunna visa att den aktuella personuppgiftsbehandlingen är*

45. Artikel 28.1 i dataskyddsförordningen innehåller visserligen inte några specifika hänvisningar till begreppet risk, men av den följer ändå att risknivån för de registrerades rättigheter och friheter måste beaktas. Kravet i artikel 28.1 att endast använda personuppgiftsbiträden som ger "tillräckliga garantier" för att genomföra "lämpliga tekniska och organisatoriska åtgärder" bör tolkas som att det innebär att man måste överväga personuppgiftsbiträdenas tillhandahållande av tillräckliga garantier för att genomföra sådana åtgärder mot bakgrund av riskerna med behandlingen, eftersom till exempel nivån på de säkerhetsåtgärder som ska genomföras också styrs av riskerna.
46. Den risk som är förknippad med behandlingen spelar en viktig roll för att avgöra om de tekniska och organisatoriska åtgärderna är lämpliga, tillsammans med de övriga kriterier som anges i artikel 24.1 i dataskyddsförordningen⁴⁴. Beroende på risknivån som kan tillskrivas behandlingen (t.ex. om särskilda kategorier av personuppgifter behandlas) kan den personuppgiftsansvarige fastställa strängare eller mer omfattande tekniska och organisatoriska åtgärder. Varje personuppgiftsbiträde bör därför ge tillräckliga garantier för att effektivt kunna genomföra de "lämpliga" åtgärder som fastställts av den personuppgiftsansvarige.
47. Dataskyddsstyrelsen anser att **den personuppgiftsansvariges skyldighet att kontrollera huruvida personuppgiftsbiträdena (eller underentreprenörerna) ger tillräckliga garantier för att genomföra de åtgärder som den personuppgiftsansvarige har fastställt ska gälla oavsett risken för de registrerades rättigheter och friheter.**
48. **Omfattningen** av en sådan kontroll kommer dock i praktiken att variera beroende på arten av de organisatoriska och tekniska åtgärder som fastställs av den personuppgiftsansvarige på grundval av, bland annat, den risk som är förknippad med behandlingen. Om behandlingsaktiviteterna innebär en lägre risk för de registrerades rättigheter och friheter kommer t.ex. motsvarande "lämpliga åtgärder" att vara mindre strikta. Därför kan omfattningen av den personuppgiftsansvariges verifiering vara mindre omfattande i praktiken. Om behandlingen i fråga medför en högre risk kan det vara viktigare att den personuppgiftsansvarige inriktar sin kontroll på att verifiera att tillräckliga garantier ges genom hela behandlingskedjan, med tanke på att de "lämpliga åtgärder" som ska genomföras för att hantera riskerna för de registrerade då är mer omfattande och robusta.
49. I detta avseende kan den personuppgiftsansvarige, beroende på risknivån som gäller för behandlingen, öka sin verifieringsnivå genom att själv kontrollera underleverantörsavtalen och/eller ålägga det ursprungliga personuppgiftsbiträdet en utökad verifiering och dokumentation.
50. I enlighet med ansvarsskyldighetsprincipen bör alla åtgärder som anses vara nödvändiga för att uppfylla kraven i dataskyddsförordningen, även på grundval av den risk som behandlingen medför, dokumenteras på lämpligt sätt av den personuppgiftsansvarige⁴⁵. En sådan skyldighet underlättas av,

förenlig med förordningen, vilket även inbegriper att åtgärderna är effektiva. Valet av åtgärder ska göras utifrån omständigheterna kring den aktuella personuppgiftsbehandlingen och de risker som den medför, vilket är faktorer som också anges i artiklarna 24 och 32 i förordningen".

⁴⁴ Artikel 24.1 hänvisar till "behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter".

⁴⁵ Vad gäller den personuppgiftsansvariges bevisbörda, se EU-domstolens dom *Natsionalna agentsia za prihodite* av den 14 december 2023, C-340/21, EU:C:2023:986, punkt 52: "Det framgår klart av ordalydelsen i artiklarna 5.2, 24.1 och 32.1 i dataskyddsförordningen att det är den personuppgiftsansvarige som har bevisbördan för att personuppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, i den mening som avses i artikel 5.1 f och artikel 32 i förordningen"; se även EU-domstolens dom *BL mot MediaMarktSaturnn Hagen-Iserlohn GmbH* av den 25 januari 2024, C-687/21, ECLI:EU:C:2024:72, punkt 42 "Det framgår av artiklarna 5, 24 och 32 i dataskyddsförordningen, jämförda med skäl 74 i samma förordning, att det vid en talan om

å ena sidan, de **assistans- och granskningsskyldigheter** som åläggs personuppgiftsbiträdena och, å andra sidan, den **information som det ursprungliga personuppgiftsbiträdet** tillhandahåller den personuppgiftsansvarige innan andra personuppgiftsbiträden anlitas.

51. För det första noterar dataskyddsstyrelsen att personuppgiftsbiträden har en skyldighet att hjälpa den personuppgiftsansvarige att uppfylla vissa krav i dataskyddsförordningen (enligt artikel 28.3 e och f)⁴⁶. Mer allmänt har personuppgiftsbiträdet en skyldighet att för den personuppgiftsansvarige göra all information tillgänglig som är nödvändig för att bevisa att artikel 28 (artikel 28.3 h) efterlevs⁴⁷. Den personuppgiftsansvarige bör vara fullständigt informerad om de detaljer i behandlingen som är relevanta för att påvisa efterlevnad av de skyldigheter som fastställs i artikel 28 i dataskyddsförordningen, och personuppgiftsbiträdet bör tillhandahålla all information om hur behandlingen utförs för den personuppgiftsansvariges räkning⁴⁸. I avtalet bör det anges hur ofta och på vilket sätt detta informationsflöde ska ske⁴⁹.
52. Den personuppgiftsansvarige kan därför förlita sig på den information som personuppgiftsbiträdet lämnat i enlighet med artikel 28.3 h i dataskyddsförordningen, för att fullgöra sin skyldighet att dokumentera de åtgärder som vidtagits, förutsatt att den information som personuppgiftsbiträdet lämnat faktiskt visar att kraven är uppfyllda. Eftersom personuppgiftsbiträdet på grund av sin roll torde vara väl förtroget med detaljerna i den behandling som det utför och den behandling som utförs av underbiträdena, bör det proaktivt göra all relevant information tillgänglig för den personuppgiftsansvarige⁵⁰.
53. Ovanstående gäller även för underentreprenörer. Personuppgiftsbiträdena är nämligen skyldiga att överföra skyldigheterna nedåt i behandlingskedjan (artikel 28.4 i dataskyddsförordningen).
54. För det andra är **anlitande av underentreprenörer**, såsom nämnts ovan, endast möjligt med den personuppgiftsansvariges skriftliga förhandstillstånd, som kan vara specifikt eller allmänt. Om den personuppgiftsansvarige väljer att ge sitt allmänna tillstånd bör det *"kompletteras med kriterier för att styra personuppgiftsbiträdets valalternativ (t.ex. garantier när det gäller tekniska och organisatoriska åtgärder, expertkunskap, tillförlitlighet och resurser)"*⁵¹.

ersättning med stöd av artikel 82 i förordningen är den personuppgiftsansvarige som har bevisbördan för att personuppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, i den mening som avses i artikel 5.1 f och artikel 32 i förordningen. En sådan fördelning av bevisbördan är inte bara ägnad att uppmuntra de personuppgiftsansvariga att vidta de säkerhetsåtgärder som krävs enligt dataskyddsförordningen, utan även att säkerställa den ändamålsenliga verkan av rätten till ersättning enligt artikel 82 i förordningen och respektera unionslagstiftarens avsikter som nämns i skäl 11 i förordningen".

⁴⁶ Se EDPB:s riktlinjer 07/2020, punkterna 130–138.

⁴⁷ Se EDPB:s riktlinjer 07/2020, punkterna 143–145.

⁴⁸ EDPB:s riktlinjer 07/2020, punkt 143.

⁴⁹ EDPB:s riktlinjer 07/2020, punkt 143.

⁵⁰ EDPB:s riktlinjer 07/2020, punkt 143, med hänvisning till artikel 28.3 h: *"Till exempel kan de relevanta delarna av personuppgiftsbiträdets register över behandlingsaktiviteter delas med den personuppgiftsansvarige. Personuppgiftsbiträdet ska tillhandahålla all information om hur behandlingen kommer att utföras för den personuppgiftsansvariges räkning. Sådan information bör inkludera uppgifter om hur systemen som används fungerar, säkerhetsåtgärder, hur datalagringskraven uppfylls, datalokalisering, överföring av data, vem som har tillgång till uppgifterna och vilka som är mottagare av data, underbiträden som används, etc."* Möjligheten för den personuppgiftsansvarige att utföra en granskning specificeras också i punkt 144: *"Målet med sådana revisioner är att säkerställa att den personuppgiftsansvarige har all information om den utförda behandlingen för dennes räkning och de garantier som tillhandahålls av personuppgiftsbiträdet."*

⁵¹ EDPB:s riktlinjer 07/2020, punkt 156.

55. EDPB förklarar att "[f]ör att genomföra bedömningen och ta beslutet om att godkänna underentreprenad måste en lista över avsedda underbiträden (där det anges för vardera: deras plats, vad de ska göra och bevis på vilka skyddsåtgärder som har genomförts) överlämnas till den personuppgiftsansvarige av personuppgiftsbiträdet"⁵². Denna information behövs så att den personuppgiftsansvarige kan efterleva ansvarsprincipen enligt artiklarna 5.2 och 24 och bestämmelserna i artiklarna 28.1, 32 och kapitel V i dataskyddsförordningen⁵³. När det gäller överföringar av personuppgifter utanför EES hänvisar dataskyddsstyrelsen till den danska tillsynsmyndighetens svar på fråga 1.2 nedan.
56. Såsom EDPB har påpekat bör det ursprungliga personuppgiftsbiträdet säkerställa att det föreslår underbiträden som ger tillräckliga garantier⁵⁴. Behovet av att det ursprungliga personuppgiftsbiträdet tillhandahåller ovanstående information visar att **det ursprungliga personuppgiftsbiträdet har en roll när det gäller att välja underbiträden och kontrollera de garantier som de tillhandahåller, och bör förse den personuppgiftsansvarige med tillräcklig information**. Detta är också förenligt med det faktum att personuppgiftsbiträdet förblir fullt ansvarigt gentemot den personuppgiftsansvarige för utförandet av underbiträdenas skyldigheter, oavsett vilka kriterier som den personuppgiftsansvarige föreslår för att välja underleverantörer (artikel 28.4 i dataskyddsförordningen).
57. I detta avseende gäller att, även om det enligt artikel 28.4 i dataskyddsförordningen åligger det personuppgiftsbiträde som anlitar en underleverantör att se till att samma skyldigheter i fråga om dataskydd som fastställs i det ursprungliga avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet även gäller för det ytterligare personuppgiftsbiträdet, upphäver detta inte den personuppgiftsansvariges ansvar för att säkerställa efterlevnad av kraven i artiklarna 28.1 och 24.1 i dataskyddsförordningen och dennes skyldighet att kunna bevisa denna efterlevnad.
58. **Det slutliga beslutet om att anlita ett visst underbiträde (eller en underentreprenör till detta underbiträde) och det därmed sammanhängande ansvaret, inklusive när det gäller att kontrollera att de garantier som underbiträdet lämnar är tillräckliga, åligger den personuppgiftsansvarige.** När det gäller generiska eller särskilda tillstånd är det, såsom redan påpekats, alltid upp till den personuppgiftsansvarige att besluta om huruvida den ska godkänna eller invända mot att ett visst underbiträde anlitas.
59. När tillsynsmyndigheterna bedömer efterlevnaden av artiklarna 24.1 och 28.1 i dataskyddsförordningen bör de bedöma om den personuppgiftsansvarige kan bevisa att den kontrollerat att de garantier som ges av dess underentreprenörer är tillräckliga och tillfredsställande för den personuppgiftsansvarige. Detta innebär att den personuppgiftsansvarige kan välja att förlita sig på den information som den fått från sitt personuppgiftsbiträde och vid behov komplettera den med mer information. Om den information som tillhandahållits den personuppgiftsansvarige tycks ofullständig, felaktig eller ger upphov till tvivel, eller när så är lämpligt på grundval av omständigheterna i ärendet, inbegripet den risk som är förknippad med behandlingen, bör den personuppgiftsansvarige begära ytterligare information och/eller kontrollera informationen och vid behov komplettera eller korrigera den.
60. Mer konkret bör den personuppgiftsansvarige vid behandling som innebär en hög risk för de registrerades rättigheter och friheter öka sin kontrollnivå när det gäller verifiering av informationen rörande de garantier som de olika personuppgiftsbiträdena i behandlingskedjan lämnar.

⁵² EDPB:s riktlinjer 07/2020, punkt 152.

⁵³ EDPB:s riktlinjer 07/2020, fotnot 69.

⁵⁴ EDPB:s riktlinjer 07/2020, punkt 159.

2.1.3 Verifiering av avtalet mellan det ursprungliga personuppgiftsbiträdet och de ytterligare personuppgiftsbiträdena

61. Den danska tillsynsmyndighetens frågor rör i huvudsak huruvida och i vilken utsträckning den personuppgiftsansvarige är skyldig att kontrollera och dokumentera att avtalen med underentreprenörerna innehåller samma skyldigheter för de ytterligare personuppgiftsbiträdena.
62. I artikel 28.4⁵⁵ föreskrivs en direkt skyldighet för personuppgiftsbiträden i detta avseende. Dessutom krävs det enligt artikel 28.3 d att den personuppgiftsansvarige och personuppgiftsbiträdet ska "föreskriva" en skyldighet för personuppgiftsbiträdet att i sitt avtal respektera de villkor som avses i artikel 28.4, vilket gör detta krav till en avtalsenlig skyldighet för personuppgiftsbiträdet. Med andra ord är **det ursprungliga personuppgiftsbiträdet rättsligt och avtalsmässigt skyldigt att överföra samma dataskyddsskyldigheter i de underbiträdesavtal som det ingår med ytterligare personuppgiftsbiträden.**

⁵⁵ Artikel 28.4 i dataskyddsförordningen: "*I de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar ska det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt punkt 3, och särskilt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning.*"

63. På samma sätt kommer de ytterligare personuppgiftsbiträdena att vara avtalsenligt förpliktade (gentemot det ursprungliga personuppgiftsbiträdet) att införa samma dataskyddsskyldigheter för sina egna personuppgiftsbiträden (eller underentreprenörer) och så vidare längs behandlingskedjan⁵⁶. Det är inte nödvändigt att underbiträdesavtalet har exakt samma lydelse som det uppgiftsbehandlingsavtal som ingåtts med det ursprungliga personuppgiftsbiträdet⁵⁷.
64. Dataskyddsstyrelsen påminner om att i fall där en underentreprenör underlåter att fullgöra sina skyldigheter är det den personuppgiftsansvarige som har det yttersta ansvaret för att detta underbiträde fullgör sina skyldigheter. Det ursprungliga personuppgiftsbiträdet kommer dock att förbli ansvarigt gentemot den personuppgiftsansvarige, vilket innebär att den personuppgiftsansvarige har möjlighet att göra ett avtalsenligt anspråk gentemot sitt ursprungliga personuppgiftsbiträde om detta personuppgiftsbiträde underlåter att överföra samma skyldigheter avseende dataskydd i kontrakten med sina underentreprenörer.
65. Personuppgiftsbiträden är skyldiga att ge den personuppgiftsansvarige tillgång till all information som är nödvändig för att visa att artikel 28.3 h i dataskyddsförordningen efterlevs. Därför måste det ursprungliga personuppgiftsbiträdet på begäran av den personuppgiftsansvarige tillhandahålla avtalen mellan det ursprungliga personuppgiftsbiträdet och de underentreprenörer som det anlitar.
66. I detta avseende ger Europeiska kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden⁵⁸ och standardavtalsklausuler för överföring av personuppgifter till tredjeländer⁵⁹ den personuppgiftsansvarige möjlighet att begära en kopia av

⁵⁶ I EDPB:s och EDPS gemensamma yttrande 2/2021 om Europeiska kommissionens genomförandebeslut om standardavtalsklausuler för överföring av personuppgifter till tredjeländer, betonade EDPB och EDPS att kravet i artikel 28.4 i dataskyddsförordningen måste beaktas vid kontraktsförhållanden där båda parterna är personuppgiftsbiträden (punkt 66).

⁵⁷ EDPB:s riktlinjer 07/2020, punkt 160: "Att ålägga "samma" skyldigheter bör tolkas mera funktionellt än på ett formellt sätt: det är inte nödvändigt att avtalet innehåller exakt samma ord som de som används i avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet, men det bör se till att förpliktelserna i sak är desamma.". EDPB noterar också att när två personuppgiftsbiträden använder sig av modul tre (avtalsförhållanden där båda parterna är personuppgiftsbiträden) i kommissionens standardavtalsklausuler för internationella överföringar, lämnas en ytterligare garanti av det ursprungliga personuppgiftsbiträdet. Enligt klausul 8.1 d i standardavtalsklausulerna för internationella överföringar intygar uppgiftsutföraren (det ursprungliga personuppgiftsbiträdet) att denne har ålagt uppgiftsföraren (underentreprenören) samma dataskyddsskyldigheter som anges i avtalet eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan den personuppgiftsansvarige och uppgiftsutföraren.

⁵⁸ I kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden föreskrivs följande i klausul 7.7 c, Användning av underleverantörer: "På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet tillhandahålla den personuppgiftsansvarige en kopia av ett sådant underleverantörsavtal och eventuella senare ändringar. I den mån det är nödvändigt för att skydda affärshemligheter eller annan konfidentiell information, inbegripet personuppgifter, får personuppgiftsbiträdet redigera avtalstexten innan kopian delas". Kommissionens genomförandebeslut 2021/915 av den 4 juni 2021 om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i förordning (EU) 2016/679 och artikel 29.7 i förordning (EU) 2018/1725 ("standardavtalsklausulerna mellan personuppgiftsansvariga och personuppgiftsbiträden").

⁵⁹ I modul två (från personuppgiftsansvarig till personuppgiftsbiträde), klausul 9 c i kommissionens standardavtalsklausuler för internationella överföringar anges följande: "Uppgiftsföraren ska, på uppgiftsutförarens begäran, tillhandahålla en kopia av avtalet med underentreprenören och eventuella senare ändringar till uppgiftsutföraren. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsföraren redigera texten i avtalet innan en kopia tillhandahålls." I modul tre (från personuppgiftsbiträde till personuppgiftsbiträde) föreskrivs dessutom att "Uppgiftsföraren ska, på uppgiftsutförarens eller den personuppgiftsansvariges begäran, tillhandahålla en

avtalet mellan det ursprungliga personuppgiftsbiträdet och de ytterligare personuppgiftsbiträdena. Denna möjlighet föreskrivs också i de tre standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden som antagits av olika tillsynsmyndigheter⁶⁰. Denna möjlighet följer av den personuppgiftsansvariges rätt till granskning enligt artikel 28.3 h i dataskyddsförordningen. På begäran av den personuppgiftsansvarige ska personuppgiftsbiträdet tillhandahålla en sådan kopia.

67. EDPB noterar dock att standardavtalsklausulerna inte reglerar huruvida en personuppgiftsansvarig *måste* begära en sådan kopia för att uppfylla kraven i artikel 28.1 i dataskyddsförordningen.
68. I det avseendet kan den personuppgiftsansvariges ansvar inte avgöras av om den denne väljer att begära en sådan kopia eller inte. Under alla omständigheter har personuppgiftsbiträdet också en rättslig och avtalsmässig skyldighet att införa samma dataskyddskrav som i det ursprungliga avtalet.
69. Med detta sagt är den **personuppgiftsansvarige inte skyldig att systematiskt begära in underleverantörsavtal för att kontrollera huruvida de dataskyddsskyldigheter som föreskrivs i det ursprungliga avtalet har överförts nedåt i behandlingskedjan**. Den personuppgiftsansvarige bör bedöma från fall till fall huruvida det är nödvändigt att begära en kopia av sådana avtal eller att när som helst granska dem för att kunna visa efterlevnad mot bakgrund av principen om ansvarsskyldighet. I samband med utövandet av sin rätt till granskningar enligt artikel 28.3 h bör den personuppgiftsansvarige ha infört ett förfarande för att genomföra granskningskampanjer för att genom stickprovskontroller kontrollera att avtalen med underleverantörerna innehåller de skyldigheter avseende dataskydd som krävs.
70. Behovet av att begära en kopia av underleverantörsavtalet beror således på omständigheterna i det enskilda fallet. Om det till exempel råder tvivel om personuppgiftsbitrådets eller underleverantörens efterlevnad av kraven i artiklarna 28.1 och 28.4, eller om tillsynsmyndigheten så begär, bör den personuppgiftsansvarige be om tillgång till avtalet för granskningsändamål (t.ex. i händelse av att det ytterligare personuppgiftsbiträdet påverkas av en personuppgiftsincident, eller i händelse av annan offentligt tillgänglig information eller annan information som är tillgänglig för den personuppgiftsansvarige). Det kan till exempel hända att det förekommer mallar för underleverantörers databehandlingsavtal som inte uppfyller kraven i artikel 28.3 i dataskyddsförordningen.
71. För att säkerställa efterlevnad av artikel 28.1 med beaktande av ansvarsprincipen kan en kopia av underbiträdesavtalen göra det möjligt för den personuppgiftsansvarige att bevisa att dess personuppgiftsbiträden och deras underentreprenörer ger tillräckliga garantier, inklusive att personuppgiftsbiträdena följer artikel 28.4 i dataskyddsförordningen. EDPB noterar att en personuppgiftsansvarig kanske inte kan bedöma om de garantier som ges i förhållande till en underentreprenör är tillräckliga om den personuppgiftsansvarige inte får tillgång till underbiträdesavtalet och kan bedöma innehållet i det. Även om garantier kan inkluderas skriftligen i

kopia av avtalet med underentreprenören och eventuella senare ändringar till uppgiftsutföraren. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsinföraren redigera texten i avtalet innan en kopia tillhandahålls." Kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 ("kommissionens standardavtalsklausuler för internationella överföringar").

⁶⁰ Den danska tillsynsmyndighetens standardavtalsklausuler för efterlevnad av artikel 28 i dataskyddsförordningen, särskilt klausul 7.5, den litauiska tillsynsmyndighetens standardavtalsklausuler för efterlevnad av artikel 28 i dataskyddsförordningen, särskilt klausul 18, och den slovenska tillsynsmyndighetens standardavtalsklausuler för efterlevnad av artikel 28 i dataskyddsförordningen, särskilt klausul 6.5.

avtalet kan avtalsklausuler inte i sig visa att de tillräckliga garantierna faktiskt tillhandahålls av avtalsparterna.

2.2 Om tolkningen av artikel 28.1 i dataskyddsförordningen läst tillsammans med artikel 44 i dataskyddsförordningen (överföringar i behandlingskedjan – frågorna 1.2 och 1.3)

72. I fråga 1.2 i begäran efterlyser myndigheten klargöranden i fråga om fall av överföringar eller vidareöverföringar från ett personuppgiftsbiträde (eller underentreprenör) till ett annat personuppgiftsbiträde ((eller underentreprenör), samt i vilken utsträckning den personuppgiftsansvarige, som en del av sin skyldighet enligt artikel 28.1 i dataskyddsförordningen, jämförd med artikel 44 i den förordningen, bör bedöma dokumentationen från personuppgiftsbiträden (eller underentreprenörer) för att kontrollera att dataskyddsnivån inte äventyras av de inledande överföringarna eller vidareöverföringarna.
73. Syftet med fråga 1.3 är att klargöra huruvida omfattningen av skyldigheterna enligt artikel 28.1 i dataskyddsförordningen, läst tillsammans med artikel 5.2 och artikel 24 i samma förordning och som förklarades under fråga 1.2, varierar beroende på den risk som är förknippad med behandlingen. Den danska tillsynsmyndigheten begärde att få veta hur omfattande sådana skyldigheter är, i förekommande fall, för behandling med låg risk respektive hög risk.

Inledande förtydliganden

74. För tydlighetens skull ges några inledande klargöranden avseende dessa frågor inom ramen för detta yttrande.
75. För det första förstår dataskyddsstyrelsen termen "överföring" i den mening som avses i EDPB:s riktlinjer 05/2021 om samspelet mellan artikel 3 och kapitel V i dataskyddsförordningen⁶¹ (nedan kallade *EDPB:s riktlinjer 05/2021 (samspel)*), vilka även hänvisar till EDPB:s riktlinjer 3/2018 om dataskyddsförordningens territoriella tillämpningsområde⁶². Som EDPB betonat tidigare ingår fjärråtkomst från ett tredjeland i begreppet överföring om åtkomsten uppfyller de kriterier som anges i EDPB:s riktlinjer 05/2021 (samspel)⁶³. Under alla omständigheter innebär förekomsten av en överföring att kapitel V i dataskyddsförordningen börjar tillämpas.
76. För det andra, eftersom fråga 1.2 avser en situation där ett personuppgiftsbiträde (eller en underentreprenör) utför en inledande överföring eller en vidareöverföring till ett annat personuppgiftsbiträde (eller en annan underentreprenör), är den personuppgiftsansvarige inte uppgiftsutföraren. Uppgiftsutföraren är i stället ett personuppgiftsbiträde som överför personuppgifterna till ett annat personuppgiftsbiträde i kedjan, för den personuppgiftsansvariges räkning, och inte till en separat personuppgiftsansvarig. Frågan utesluter därför personuppgifter som överförs till separata personuppgiftsansvariga, däribland tribunaler, domstolar eller administrativa myndigheter i tredjeländer. Tolkningen av artikel 48 i dataskyddsförordningen omfattas därför inte av dessa frågor.
77. För det tredje noterar EDPB att fråga 1.2 avser överföringar som sker längs databehandlingskedjan i enlighet med den personuppgiftsansvariges dokumenterade instruktioner enligt artikel 28.3 a i dataskyddsförordningen. Det är värt att betona att det är upp till den personuppgiftsansvarige att besluta om huruvida en överföring av personuppgifter utanför EES är möjlig som en del av den behandlingsverksamhet som anförts trots personuppgiftsbiträdena (eller deras underentreprenörer). Personuppgiftsbiträdet bör avstå från att utföra inledande överföringar eller vidareöverföringar som faller utanför den personuppgiftsansvariges instruktioner⁶⁴. Den personuppgiftsansvariges dokumenterade instruktioner avseende inledande överföringar eller vidareöverföringar av personuppgifter ska föras vidare nedåt i behandlingskedjan⁶⁵.
78. För det fjärde klargör EDPB att begreppet risk, som det hänvisas till i fråga 1.3, bör förstås som risken för rättigheterna och friheterna för de registrerade vars personuppgifter behandlas, i den mening som avses i skäl 75 och 76 i dataskyddsförordningen (se punkt 35 ovan).

⁶¹ EDPB:s riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, antagna den 14 februari 2023, där punkt 9 anger de tre kumulativa kriterierna för att en uppgiftsbehandling ska betraktas som en överföring och där dessa kriterier beskrivs mer allmänt i avsnitt 2.

⁶² EDPB:s riktlinjer 05/2021 (samspel), punkt 12, som hänvisar till EDPB:s riktlinjer 3/2018 om dataskyddsförordningens territoriella tillämpningsområde, version 2.1, antagna den 12 november 2019 (med rättelse daterad den 7 januari 2020), s. 5 och avsnitt 1–3. Se särskilt "d) Personuppgiftsbiträde utan verksamhetsställe inom unionen" under avsnitt 2.

⁶³ EDPB:s riktlinjer 05/2021 (samspel), punkt 16.

⁶⁴ Artikel 29 i dataskyddsförordningen. Såsom EDPB erinrar om bör avtalet "*specificera kraven för överföringar till tredjeländer eller internationella organisationer, med beaktande av bestämmelserna i kapitel V i GDPR*" (EDPB:s riktlinjer 07/2020, punkt 119). Den personuppgiftsansvarige kan till exempel välja att förbjuda överföringar eller att endast tillåta dem till specifika länder.

⁶⁵ Artikel 28.4 i dataskyddsförordningen.

Den personuppgiftsansvariges ansvar gäller även om personuppgiftsbiträdena (eller underentreprenörerna) genomför den inledande överföringen eller vidareöverföringen

79. När det gäller innehållet i begäran har EDPB redan angett att det kommer *"att uppstå en överföringssituation när ett personuppgiftsbiträde (antingen enligt artikel 3.1 eller artikel 3.2 för en viss behandling, såsom förklaras ovan) skickar uppgifter till ett annat personuppgiftsbiträde eller till och med en annan personuppgiftsansvarig i tredjeland, enligt instruktioner från sin personuppgiftsansvarige. I dessa fall agerar personuppgiftsbiträdet som uppgiftsutförare för den personuppgiftsansvariges räkning och måste säkerställa att bestämmelserna i kapitel V efterlevs för den aktuella överföringen enligt den personuppgiftsansvariges instruktioner, vilket inbegriper användning av ett lämpligt överföringsverktyg. Eftersom överföringen är en behandling som utförs för den personuppgiftsansvariges räkning kan den personuppgiftsansvarige dessutom hållas ansvarig enligt kapitel V och måste även säkerställa att personuppgiftsbiträdet ger tillräckliga garantier enligt artikel 28."*⁶⁶
80. Vid en överföring, även om den inte utförs direkt av den personuppgiftsansvarige utan av ett personuppgiftsbiträde för den personuppgiftsansvariges räkning, är den personuppgiftsansvarige med andra ord fortfarande föremål för skyldigheter som härrör från både artikel 44 och artikel 28.1 i dataskyddsförordningen^{67 68}.

Det ansvar som följer av artikel 44 i dataskyddsförordningen

81. Skyldigheterna i artikel 44 i dataskyddsförordningen⁶⁹ omfattar både personuppgiftsbiträden (som inom ramen för yttrandet fungerar som uppgiftsutförare) och personuppgiftsansvariga⁷⁰. Både personuppgiftsbiträden och personuppgiftsansvariga bör därför säkerställa att skyddsnivån för personuppgifterna inte undergrävs av den inledande överföringen eller vidareöverföringen, oavsett vilken grund som överföringen baseras på⁷¹. I princip förblir både den personuppgiftsansvarige och personuppgiftsbiträdet till exempel ansvariga enligt kapitel V i dataskyddsförordningen vid en olaglig inledande överföring eller vidareöverföring⁷² och kan hållas ansvariga individuellt eller gemensamt vid en överträdelse.

⁶⁶ EDPB:s riktlinjer 05/2021 (samspel), punkt 19, fetstil tillagd.

⁶⁷ Det är också relevant att påpeka att artikel 28.1 i dataskyddsförordningen hänvisar till uppfyllande av kraven i dataskyddsförordningen och därför bör tolkas som att den omfattar bestämmelserna i kapitel V om inledande överföringar eller vidareöverföringar av personuppgifter till tredjeländer. Detta omfattar både inledande överföringar och vidareöverföringar, se artikel 44 i dataskyddsförordningen.

⁶⁸ I detta avsnitt av yttrandet behandlas de skyldigheter som följer av artiklarna 44 och 28.1 i dataskyddsförordningen, och det specificeras att den personuppgiftsansvarige fortsätter att omfattas av alla skyldigheter som gäller för personuppgiftsansvariga enligt dataskyddsförordningen.

⁶⁹ I artikel 44 i dataskyddsförordningen hänvisas till bestämmelserna i kapitel V i samma förordning.

⁷⁰ Artikel 44 i dataskyddsförordningen riktar sig till både "den personuppgiftsansvarige och personuppgiftsbiträdet" för efterlevnad av kapitel V, se även skäl 101. EDPB:s rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, version 2.0, antagna den 18 juni 2021 (nedan kallade *EDPB:s rekommendationer 01/2020*) är därför tillämpliga på "uppgiftsutförare" (oavsett om dessa är personuppgiftsansvariga eller personuppgiftsbiträden/underleverantörer som behandlar personuppgifter).

⁷¹ EU-domstolens dom C-311/18 av den 16 juli 2020, *Data Protection Commissioner mot Facebook Ireland Ltd och Maximilian Schrems* (nedan kallad *EU-domstolens dom i målet Schrems II*) ECLI:EU:C:2020:559, punkt 92.

⁷² Den personuppgiftsansvarige kan kräva ersättning från sitt personuppgiftsbiträde motsvarande dennes del av ansvaret, förutsatt att de villkor som anges i artikel 82.5 i dataskyddsförordningen är uppfyllda.

Det ansvar som följer av artikel 28.1 i dataskyddsförordningen

82. Enligt ansvarsskyldighetsprincipen är personuppgiftsansvariga skyldiga att vidta "lämpliga åtgärder" för att förhindra eventuella överträdelser av de regler som fastställs i dataskyddsförordningen, i syfte att säkerställa rätten till skydd av personuppgifter⁷³, vilket inbegriper förhindrande av överträdelser avseende kapitel V i dataskyddsförordningen. Detta ansvar gäller innan överföringen påbörjas och så länge som de överförda personuppgifterna behandlas i tredjelandet.
83. Såsom förklaras i punkterna 47–48 ovan bör *den personuppgiftsansvariges skyldighet* att kontrollera huruvida personuppgiftsbiträdena (eller underentreprenörerna) lämnar tillräckliga garantier för att genomföra de åtgärder som den personuppgiftsansvarige fastställt enligt artikel 28.1 i dataskyddsförordningen⁷⁴ gälla oavsett hur stor risken är för de registrerades rättigheter och friheter. *Omfattningen* av denna kontroll kommer dock i praktiken att variera beroende på den typ av organisatoriska och tekniska åtgärder som den personuppgiftsansvarige fastställer på grundval av, bland annat, den risk som är förenad med uppgiftsbehandlingen⁷⁵. I detta avseende kan förekomsten av en inledande överföring eller vidareöverföring till tredjeländer i behandlingskedjan öka de risker som behandlingen medför och därmed påverka de "lämpliga åtgärder" som fastställs av den personuppgiftsansvarige⁷⁶.
84. På begäran bör den personuppgiftsansvarige – med stöd från det ursprungliga personuppgiftsbiträdet och dennes underleverantörer – kunna visa för den behöriga tillsynsmyndigheten att den uppfyller kraven i artikel 28.1 i dataskyddsförordningen. Den lämpliga dokumentationen skulle bland annat kunna baseras på den information som mottagits från personuppgiftsbiträdena i samband med anlitaandet av personuppgiftsbiträden (eller underentreprenörer)⁷⁷ (se punkterna 54–56), men bör

⁷³ Se avsnittet ovan om artiklarna 5.2 och 24.1 lästa tillsammans med artikel 28.1 i dataskyddsförordningen.

⁷⁴ För att undvika missförstånd bör det klargöras att de "lämpliga tekniska och organisatoriska åtgärder" som avses i artiklarna 24.1 och 28.1 i dataskyddsförordningen inte ska förväxlas med de "kompletterande åtgärder" som nämns i EDPB:s rekommendationer 01/2020 (punkt 50: "*Kompletterande åtgärder*" är per definition kompletterande till de skyddsåtgärder som överföringsverktyget i artikel 46 i dataskyddsförordningen redan tillhandahåller och till alla andra tillämpliga säkerhetskrav (t.ex. tekniska skyddsåtgärder) i dataskyddsförordningen", med hänvisning till skäl 109 i dataskyddsförordningen och EU-domstolens dom i målet Schrems II, punkt 133).

⁷⁵ Se definitionen av risk i punkterna 35 och 78.

⁷⁶ I skäl 116 i dataskyddsförordningen föreskrivs följande: "*När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskydds rättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information.*"

⁷⁷ Se även klausul 9 a i modul tre (överföring från personuppgiftsbiträde till personuppgiftsbiträde) i kommissionens standardavtalsklausuler för internationella överföringar och dess bilaga III, se även klausul 9 a i modul två (överföring från personuppgiftsansvarig till personuppgiftsbiträde) och klausul 7.7 a i kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och dess bilaga IV, "Förteckning över underleverantörer". Både bilaga II till kommissionens standardavtalsklausuler för internationella överföringar och bilaga IV till kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden ska kompletteras med följande information om underleverantörerna i händelse av ett särskilt tillstånd från den personuppgiftsansvarige: namn, adress, kontaktpersonens namn, befattning, kontaktuppgifter samt en beskrivning av databehandlingen. Dessutom innehåller bilaga I till kommissionens standardavtalsklausuler för internationella överföringar, avsnitt B, "Beskrivning av överföringen" följande: "Vid överföringar till personuppgiftsbiträden/underentreprenörer, ange även föremålet för behandlingen liksom dess karaktär och varaktighet". På liknande sätt innehåller bilaga II till standardavtalsklausulerna mellan personuppgiftsansvariga och personuppgiftsbiträden följande: "För behandling som utförs av personuppgiftsbiträden (eller underleverantörer), ange även föremålet för behandlingen, behandlingens art och dess varaktighet".

även kunna skaffas fram med hjälp av de berörda personuppgiftsbiträdena i enlighet med artikel 28.3 h i dataskyddsförordningen (se punkterna 51–52).

85. Den personuppgiftsansvarige behöver också ha tillgång till all relevant information för att kunna utfärda de instruktioner som krävs för att överföra personuppgifterna till respektive tredjeland och för att kunna följa principen om ansvarsskyldighet i artikel 5.2 och artikel 24 i dataskyddsförordningen samt bestämmelserna i artikel 28.1, artikel 32 och kapitel V i samma förordning⁷⁸. Den personuppgiftsansvarige får motsätta sig eller inte godkänna anlitaandet av ett ytterligare personuppgiftsbiträde om det skulle medföra en överföring av personuppgifter från det ursprungliga personuppgiftsbiträdet (som uppgiftsutförare) till det planerade ytterligare personuppgiftsbiträdet (som uppgiftsinförare) på grundval av den information som mottagits.
86. I enlighet med punkt 58 ovan är den personuppgiftsansvarige ytterst ansvarig för varje överträdelse av artikel 28.1 i dataskyddsförordningen när det gäller användning av personuppgiftsbiträden (eller underentreprenörer) och skulle kunna hållas ansvarig för en sådan överträdelse. EDPB framhåller att det faktum att personuppgiftsansvariga åberopar praktiska svårigheter när det gäller kontroll över hur deras personuppgiftsbiträden anlitar underleverantörer – vilket i sin tur kan göra det svårt för dem att kontrollera ”tillräckliga garantier”, särskilt när det gäller överföringar till tredjeländer – inte befriar de personuppgiftsansvariga från dess ansvar i samband med databehandlingen⁷⁹.
87. Nedan ges icke-uttömmande exempel på den dokumentation som den personuppgiftsansvarige ska bedöma och kunna visa för den behöriga tillsynsmyndigheten – kartläggning av överföringen, den grund för överföring som används och i tillämpliga fall ”konsekvensbedömning avseende överföring” samt kompletterande åtgärder.

Kartläggning av överföringen:

88. Som ett första steg, i fall där personuppgifter ska överföras till tredjeländer med hjälp av personuppgiftsbiträden (eller deras underleverantörer), bör den personuppgiftsansvarige bedöma och kunna visa dokumentation avseende kartläggningen av överföringen⁸⁰. Den personuppgiftsansvarige bör se till att uppgiftsutföraren (som behandlar personuppgifter för den personuppgiftsansvariges räkning) genomför en kartläggning av överföringen där uppgiftsutföraren anger vilka personuppgifter som överförs (fjärråtkomst inkluderat) samt vart och för vilka ändamål⁸¹. Den personuppgiftsansvarige kan stödja sig på en sådan kartläggning och vid behov komplettera den. Exempelvis bör den personuppgiftsansvarige begära ytterligare information, kontrollera informationen och vid behov komplettera/korrigera den om kartläggningen som erhålls förefaller ofullständig⁸², felaktig eller ger upphov till frågor.
89. Den personuppgiftsansvarige bör få denna information⁸³ innan ytterligare ett personuppgiftsbiträde anlitas. Det bör också erinras om att den personuppgiftsansvarige omfattas av särskilda krav på transparens när det gäller överföringar till tredjeländer enligt artiklarna 13.1 f, 14.1 f, 15.1 c och 15.2 i dataskyddsförordningen och kravet på att föra register över behandlingsaktiviteter enligt artikel 30.1 d

⁷⁸ EDPB:s riktlinjer 07/2020, punkt 152, fotnot 69.

⁷⁹ CEF:s rapport om molntjänster, s. 16.

⁸⁰ ”Kartläggning” avser det första steget (”Lär känna din överföring”) i EDPB:s rekommendationer 01/2020, avsnitt 2.1 ”Steg 1: Lär känna dina överföringar”. Detta första steg gäller oavsett grunden för överföringen.

⁸¹ Det bör anges att ändamålen fastställs av den personuppgiftsansvarige, tillsammans med de ”väsentliga medlen” för behandlingen (se EDPB:s riktlinjer 07/2020, punkt 40).

⁸² Till exempel om det i kartläggningen inte anges var underleverantörerna befinner sig, eller om överföringar av typen fjärråtkomst inte nämns i kartläggningen trots att de sker.

⁸³ Enligt förklaring i punkterna 54–56 ovan.

och e i dataskyddsförordningen. För att uppfylla dessa krav bör den personuppgiftsansvarige veta var underleverantörerna finns och var överföringar – inklusive fjärråtkomst – äger rum⁸⁴.

Den grund för överföring som använts och, i tillämpliga fall, konsekvensbedömningen för överföringen och de kompletterande åtgärderna:

90. Den personuppgiftsansvarige ska bedöma och kunna uppvisa dokumentation avseende grunden för överföringen⁸⁵ som uppgiftsutföraren baserar sig på i enlighet med den personuppgiftsansvariges instruktioner⁸⁶. Detta innebär att den personuppgiftsansvarige bör få denna information från personuppgiftsbiträdena (underentreprenörerna)/uppgiftsutförarna innan överföringarna äger rum. I detta sammanhang påminner EDPB om att den personuppgiftsansvarige omfattas av särskilda krav på transparens när det gäller "förekomsten eller avsaknaden av ett beslut om adekvat skyddsnivå" enligt artikel 45 i dataskyddsförordningen eller "lämpliga skyddsåtgärder" som tillhandahålls i enlighet med artikel 46 i samma förordning (artiklarna 13.1 f, 14.1 f och 15.2 i dataskyddsförordningen⁸⁷).
91. Hur omfattande den personuppgiftsansvariges skyldighet att bedöma denna dokumentation är, styrs av vilken typ av grund som används för den ursprungliga överföringen eller vidareöverföringen av personuppgiftsbiträdena/underentreprenörerna (i egenskap av uppgiftsutförare)⁸⁸:
92. Överföringar kan göras på grundval av ett **beslut om adekvat skyddsnivå** under förutsättning att kommissionen enligt artikel 45 i dataskyddsförordningen har fastställt att ett tredjeland, ett territorium, ett eller flera specificerade sektorer inom tredjelandet eller en internationell organisation uppfyller en adekvat skyddsnivå. För att bedöma om skyddsnivån är adekvat beaktar kommissionen bland annat de regler för vidareöverföring av personuppgifter till ett annat tredjeland eller en internationell organisation som följs i det landet eller av den internationella organisationen, rättspraxis samt effektiva och verkställbara rättigheter för registrerade och effektiva administrativa och rättsliga prövningsmöjligheter för de registrerade vars personuppgifter överförs⁸⁹.
93. Mot denna bakgrund gäller att om en överföring utförs av ett personuppgiftsbiträde/en underentreprenör (på den personuppgiftsansvariges vägnar) på grundval av ett beslut om adekvat skyddsnivå i enlighet med artikel 45 i dataskyddsförordningen, bör den grad av kontroll som krävs av den personuppgiftsansvarige enligt artikel 28.1 i dataskyddsförordningen med avseende på att dess

⁸⁴ En sådan kartläggning är också nödvändig när parterna fyller i de relevanta bilagorna till kommissionens standardavtalsklausuler för internationella överföringar och kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden (se fotnot 80 ovan).

⁸⁵ EDPB:s rekommendationer 01/2020, avsnitt 2.2. "Steg 2: Identifiera vilka överföringsverktyg du förlitar dig på".

⁸⁶ Artikel 28.3 a i dataskyddsförordningen.

⁸⁷ EDPB:s riktlinjer 01/2022 (rätt till tillgång), punkt 122.

⁸⁸ I enlighet med den personuppgiftsansvariges dokumenterade instruktioner med avseende på överföringar av personuppgifter längs behandlingskedjan.

⁸⁹ Se artikel 45 i dataskyddsförordningen och artikel 29-arbetsgruppens referensram för adekvat skyddsnivå, antagen den 28 november 2017, WP 254, godkänd av EDPB den 25 maj 2018, s. 7: "*Vidare överföring av personuppgifter från den första mottagaren av den ursprungliga överföringen ska endast tillåtas när nästa mottagare (det vill säga mottagaren av den vidare överföringen) också omfattas av bestämmelser (inklusive avtalsbaserade bestämmelser) som ger en adekvat skyddsnivå och följer relevanta instruktioner vid behandling av uppgifter på den personuppgiftsansvariges uppdrag. Skyddsnivån för de fysiska personer vars personuppgifter överförs får inte undergrävas av den vidare överföringen. Den första mottagaren av uppgifter som överförs från EU ska vara skyldig att säkerställa att lämpliga skyddsåtgärder vidtas för vidare överföringar av uppgifter i avsaknad av ett beslut om adekvat skyddsnivå. Sådana vidare överföringar av uppgifter ska endast göras för begränsade och specificerade ändamål och bara så länge det finns en rättslig grund för behandlingen.*"

personuppgiftsbiträde (eller dennes underentreprenör) ger tillräckliga garantier när det gäller efterlevnaden av kapitel V i dataskyddsförordningen, omfatta följande:

- Huruvida beslutet om adekvat skyddsnivå är i kraft⁹⁰.

- Huruvida de överföringar som görs på den personuppgiftsansvariges vägnar omfattas av ett sådant beslut (till exempel kategorier av personuppgifter eller sektorer som faller inom ramen för tillämpningsområdet)⁹¹.

94. Om personuppgifter som överförs av ett personuppgiftsbiträde/underbiträde (för den personuppgiftsansvariges räkning) på grundval av ett beslut om adekvat skyddsnivå är föremål för en **vidareöverföring** från detta tredjeland, får den skyddsnivå för fysiska personer som garanteras genom dataskyddsförordningen för sådan vidareöverföring inte heller undergrävas⁹². I detta avseende, och i enlighet med artikel 45.2 a i dataskyddsförordningen, omfattar beslut om adekvat skyddsnivå som utfärdas av Europeiska kommissionen bland annat tredjeländernas regler för vidareöverföringar. Enligt artikel 44 i dataskyddsförordningen behöver den personuppgiftsansvarige därför inte kontrollera dessa krav på egen hand.
95. När det gäller den personuppgiftsansvariges skyldighet enligt artikel 28.1 i dataskyddsförordningen innebär detta att den personuppgiftsansvarige bör säkerställa att personuppgiftsbiträdet/underbiträdet ger "tillräckliga garantier" även när det gäller vidare överföringar som utförs av ett personuppgiftsbiträde/underbiträde från ett lämpligt land.
96. I avsaknad av ett beslut om adekvat skyddsnivå kan överföringar omfattas av "**lämpliga skyddsåtgärder**" i enlighet med **artikel 46 i dataskyddsförordningen**. I detta fall bör den personuppgiftsansvarige bedöma de lämpliga skyddsåtgärder som införts och vara uppmärksam på eventuell problematisk lagstiftning som skulle kunna hindra underbiträdet från att uppfylla de skyldigheter som fastställs i dess avtal med det ursprungliga personuppgiftsbiträdet⁹³. Mer specifikt bör den personuppgiftsansvarige säkerställa att en sådan konsekvensbedömning avseende överföringen⁹⁴ utförs, i linje med rättspraxis⁹⁵ och såsom förklaras i EDPB:s rekommendationer 01/2020. Dokumentationen som rör de lämpliga skyddsåtgärder som införts, konsekvensbedömningen avseende överföring och eventuella kompletterande åtgärder bör tas fram av personuppgiftsbiträdet/uppgiftsutföraren⁹⁶ (i tillämpliga fall i samarbete med

⁹⁰ EDPB:s rekommendationer 01/2020, punkt 19: "Om du [uppgiftsutföraren] överför personuppgifter till tredjeländer, regioner eller sektorer som omfattas av ett beslut om adekvat skyddsnivå (i tillämpliga fall), behöver du inte vidta några ytterligare av de steg som beskrivs i dessa rekommendationer. Du måste emellertid fortfarande övervaka om de beslut om adekvat skyddsnivå som är relevanta för dina överföringar återkallas eller ogiltigförklaras."

⁹¹ EDPB:s rekommendationer 01/2020, punkt 19.

⁹² Se artikel 44 i dataskyddsförordningen: "uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation".

⁹³ Se i detta avseende EU-domstolens dom i målet Schrems II, punkterna 132 och 133, där den avtalsmässiga karaktären hos kommissionens standardavtalsklausuler för internationell överföring betonas av EU-domstolen.

⁹⁴ Denna bedömning förklaras närmare i EDPB:s rekommendationer 01/2020, steg 3 "Bedöm om överföringsverktyget i artikel 46 i dataskyddsförordningen är effektivt mot bakgrund av alla omständigheter kring överföringen".

⁹⁵ EU-domstolens dom i målet Schrems II, punkt 134.

⁹⁶ Rekommendationer 01/2022 om ansökan om godkännande och om de delar och principer som ska återfinnas i bindande företagsbestämmelser för personuppgiftsansvariga (artikel 47 i dataskyddsförordningen), som antogs den 20 juni 2023, version 2.1, punkt 10: "(...) Vidare är det till exempel varje uppgiftsutförarens ansvar att för varje

personuppgiftsbiträdet/uppgiftsinföraren⁹⁷). Den personuppgiftsansvarige kan förlita sig på den bedömning som gjorts av personuppgiftsbiträdet/underleverantören och vid behov komplettera den. Om den bedömning som mottagits av den personuppgiftsansvarige till exempel förefaller ofullständig, felaktig eller ger upphov till frågor bör den personuppgiftsansvarige begära ytterligare information, verifiera informationen och vid behov komplettera/korrigera den, med beaktande av att bedömningen bör vara i linje med EDPB:s rekommendationer 01/2020 och de steg som anges däri⁹⁸. Detta innefattar identifiering av lagar och praxis som är relevanta mot bakgrund av alla omständigheter kring överföringen⁹⁹ och identifiering av lämpliga kompletterande åtgärder vid behov¹⁰⁰. I detta avseende bör den personuppgiftsansvarige ägna särskild uppmärksamhet åt huruvida uppgiftsutföraren, dvs. personuppgiftsbiträdet eller underentreprenören, har bedömt om det finns något i tredjelandets lagstiftning och/eller i praxis som kan inkräkta på effektiviteten hos lämpliga skyddsåtgärder för den grund för överföring som uppgiftsutföraren förlitar sig på¹⁰¹, särskilt i fråga om den lagstiftning och praxis som styr tredjelandets myndigheters tillgång till de överförda personuppgifterna¹⁰².

97. Dessutom, och i likhet med överföringar som grundas på beslut om adekvat skyddsnivå (artikel 45 i dataskyddsförordningen, se ovan i punkterna 94 och 95), där personuppgifter överförs av ett personuppgiftsbiträde (eller av dennes underentreprenör) på grundval av lämpliga skyddsåtgärder enligt artikel 46 i dataskyddsförordningen, omfattar den personuppgiftsansvariges skyldighet enligt artikel 28.1 i dataskyddsförordningen också att försäkra sig om att personuppgiftsbiträdet (underentreprenören) lämnar tillräckliga garantier när det gäller **vidareöverföringar**. Lämpliga skyddsåtgärder enligt artikel 46 i dataskyddsförordningen omfattar vanligtvis bestämmelser som fastställer regler som kommer att styra eventuella vidareöverföringar¹⁰³. Detta innebär att personuppgiftsansvariga inte behöver kontrollera huruvida dessa regler som sådana är förenliga med kraven i kapitel V i dataskyddsförordningen. De personuppgiftsansvariga bör dock kunna visa upp dokumentation om sådana vidareöverföringar. Detta innebär att den personuppgiftsansvarige bör få denna information från personuppgiftsbiträdena (underentreprenörerna)/uppgiftsutförarna, och

överföring, från fall till fall, bedöma om det finns ett behov av att genomföra kompletterande åtgärder för att säkerställa en skyddsnivå som i allt väsentligt motsvarar den som föreskrivs i dataskyddsförordningen."

⁹⁷ I EU-domstolens dom Schrems II, punkt 134, fastställde EU-domstolen att en sådan kontroll kan göras i samarbete med uppgiftsinföraren när så är lämpligt. Se även EDPB:s rekommendationer 01/2020, avsnitt 4.

⁹⁸ Se särskilt "Steg 3: Bedöm om överföringsverktyget i artikel 46 i dataskyddsförordningen är effektivt mot bakgrund av alla omständigheter kring överföringen", "Steg 4: Inför kompletterande åtgärder" och "Steg 6: Omvärdera med lämpliga mellanrum", såsom förklaras i EDPB:s rekommendationer 01/2020.

⁹⁹ EU-domstolens dom i målet Schrems II, punkt 126. Se även EDPB:s rekommendationer 01/2020, avsnitt 2.3. "Steg 3: Bedöm om överföringsverktyget i artikel 46 i dataskyddsförordningen är effektivt mot bakgrund av alla omständigheter kring överföringen" och särskilt punkt 33. I EU-domstolens dom i målet Schrems II, punkt 134, fastställde domstolen att en sådan kontroll kan göras i samarbete med uppgiftsinföraren när så är lämpligt (se även EDPB:s rekommendationer 01/2020, punkt 30).

¹⁰⁰ Enligt rättspraxis ankommer det på den personuppgiftsansvarige eller personuppgiftsbiträdet att i varje enskilt fall och i förekommande fall i samarbete med mottagaren av uppgifterna, kontrollera huruvida lagstiftningen i det mottagande tredjelandet säkerställer ett lämpligt skydd med hänsyn till unionsrätten för personuppgifter som överförts med stöd av standardiserade dataskyddsbestämmelser och vid behov tillhandahålla ytterligare skyddsåtgärder utöver dem som erbjuds genom dessa bestämmelser (EU-domstolens dom i målet Schrems II, punkt 134). Se även EDPB:s rekommendationer 01/2020, avsnitt 2.4, "Steg 4: Inför kompletterande åtgärder".

¹⁰¹ Se EDPB:s rekommendationer 01/2020, avsnitt 2.3 ("Steg 3").

¹⁰² Se EDPB:s rekommendationer 01/2020, punkt 41 ff.

¹⁰³ Se t.ex. klausul 8.7 (modul ett) respektive klausul 8.8 (modulerna två och tre) i Europeiska kommissionens standardavtalsklausuler för internationella överföringar (kommissionens genomförandebeslut 2021/914) av den 4 juni 2021.

denna information ska visa att uppgiftsförarna faktiskt uppfyller de krav för vidareöverföring som fastställs i det lämpliga skyddsinstrumentet.

2.3 Om tolkningen av artikel 28.3 a i dataskyddsförordningen (fråga 2)

98. För att säkerställa en transparent fördelning av ansvar och skyldigheter både internt (mellan personuppgiftsansvariga och personuppgiftsbiträden) och externt gentemot registrerade och tillsynsmyndigheter, måste all behandling av personuppgifter som utförs av ett personuppgiftsbiträde enligt artikel 28.3 i dataskyddsförordningen regleras av ett avtal eller annan rättsakt enligt unionslagstiftningen eller medlemsstaternas nationella lagstiftning¹⁰⁴ mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Enligt artikel 28.3 a i dataskyddsförordningen ska avtalet särskilt föreskriva att personuppgiftsbiträdet *"endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"*. I denna bestämmelse fastställs även att *"i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt"*.
99. Begäran avser förekomsten av avtal som innefattar ett åtagande att behandla personuppgifter endast enligt instruktion från den personuppgiftsansvarige *"såvida inte denna behandling krävs enligt lag eller bindande beslut av ett statligt organ"* (dvs. utan hänvisning till unionsrätten eller medlemsstaternas nationella rätt). I detta avseende framfördes flera frågor till EDPB, vilka behandlas tillsammans i avsnittet nedan:

2 Måste ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt i enlighet med artikel 28.3 i dataskyddsförordningen innehålla det undantag som föreskrivs i artikel 28.3 a *"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* (antingen ordagrant eller i mycket likartade ordalag) för att vara förenliga med dataskyddsförordningen?

2a Om svaret på fråga 2 är nej och det upprättas ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt som utvidgar undantaget i artikel 28.3 a i dataskyddsförordningen så att det även omfattar tredjelandslagstiftning (t.ex. *"såvida inte detta krävs enligt lag eller bindande beslut av ett statligt organ"*), är detta i sig en överträdelse av artikel 28.3 a i dataskyddsförordningen?

¹⁰⁴ Nedan används termen **"avtal"** för att hänvisa till "ett avtal eller en annan rättsakt enligt EU:s eller medlemsstaternas lagstiftning".

100. EDPB:s riktlinjer 07/2020 påminner om *"vikten av att noggrant förhandla fram och utarbeta databehandlingsavtal"* med avseende på eventuella rättsliga krav från EU eller medlemsstaterna som personuppgiftsbiträdet omfattas av¹⁰⁵. När det gäller innehållet i avtalen anges det i EDPB:s riktlinjer 07/2020 att *"[e]tt avtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde måste efterleva kraven för artikel 28 i GDPR för att säkerställa att personuppgiftsbiträdet behandlar personuppgifter i enlighet med kraven för GDPR. Alla sådana avtal bör beakta de specifika förpliktelserna för personuppgiftsansvariga och personuppgiftsbiträden. Även om artikel 28 innehåller en förteckning över punkter som måste behandlas i alla avtal som styr förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden, lämnas utrymme för förhandlingar mellan parterna för sådana avtal."*¹⁰⁶ Utrymmet för förhandlingar begränsas av de krav som anges i artikel 28.3 i dataskyddsförordningen.

¹⁰⁵ EDPB:s riktlinjer 07/2020, punkt 121.

¹⁰⁶ EDPB:s riktlinjer 07/2020, punkt 109.

101. För det första är personuppgiftsbiträdets åtagande att endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige en central del av avtalet.
102. Enligt artikel 28.3 a i dataskyddsförordningen får dock personuppgiftsbiträden lagligen behandla personuppgifter – på annat sätt än enligt dokumenterade instruktioner från den personuppgiftsansvarige – för att uppfylla rättsliga skyldigheter enligt EU:s eller medlemsstaternas lagstiftning (nedan kallad ”**EU:s/medlemsstaternas rättsliga krav**”). Samma bestämmelse kräver också ett åtagande från personuppgiftsbiträdet att i förväg informera den personuppgiftsansvarige i fall där ett lagstadgat krav från EU/medlemsstaterna gäller vid behandling/överföring av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte lagen i fråga förbjuder sådan information med hänvisning till ett viktigt allmänintresse. I kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden¹⁰⁷ ingår detta åtagande uttryckligen med en formulering som är mycket lik den i artikel 28.3 a i dataskyddsförordningen. Det ingår även i flera andra standardavtalsklausuler, i synnerhet de standardavtalsklausuler som antagits av de danska¹⁰⁸, slovenska¹⁰⁹ och litauiska¹¹⁰ tillsynsmyndigheterna för efterlevnad av artikel 28 i dataskyddsförordningen.
103. Utöver kravet på att endast behandla uppgifter på dokumenterade instruktioner från den personuppgiftsansvarige innehåller artikel 28.3 a i dataskyddsförordningen tre huvudelement: a) en regel som styr situationer där ett lagstadgat krav tvingar personuppgiftsbiträdet att utföra behandling

¹⁰⁷ Se särskilt klausul 7.1 a och 7.8 a:

– Klausul 7.1 a: *Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida detta inte är förbjudet med hänvisning till ett viktigt allmänintresse enligt denna rätt. Den personuppgiftsansvarige får även ge efterföljande instruktioner under hela den tid som personuppgifterna behandlas. Dessa instruktioner ska alltid dokumenteras.* (understrykning tillagd). I sitt gemensamma yttrande om utkastet till kommissionens standardavtalsklausuler rekommenderade EDPB och EDPS införande av den fullständiga ordalydelsen i artikel 28.3 a (dvs. att en hänvisning läggs till om personuppgiftsbiträdets skyldighet att informera den personuppgiftsansvarige om det rättsliga kravet) för att öka enhetligheten. Gemensamt yttrande 1/2021 från EDPB och 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, punkt 38. Formuleringen ”såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av” återfanns redan i utkastet till standardavtalsklausuler.

– Klausul 7.8 a: *”Personuppgiftsbiträdet får endast överföra uppgifter till ett tredjeland eller en internationell organisation på grundval av dokumenterade instruktioner från den personuppgiftsansvarige eller för att uppfylla ett särskilt krav enligt unionsrätten eller en medlemsstats lagstiftning som personuppgiftsbiträdet omfattas av, och överföringen ska genomföras i enlighet med kapitel V i förordning (EU) 2016/679 eller förordning (EU) 2018/1725.”* När det gäller klausul 7.8 a rekommenderade EDPB och EDPS att en hänvisning införs till personuppgiftsbiträdets möjlighet att göra överföringar på grundval av ett särskilt krav enligt unionsrätten eller en medlemsstats lagstiftning som personuppgiftsbiträdet omfattas av, vilket inte återfanns i utkasten till standardavtalsklausuler i ett första skede. Bilaga 2 till EDPB:s och EDPS gemensamma yttrande 1/2021, Kommentarer till klausul 7.7 a.

¹⁰⁸ Den danska tillsynsmyndighetens standardavtalsklausuler för efterlevnad av artikel 28 i dataskyddsförordningen, särskilt klausulerna 4.1 och 8.2. I sitt yttrande 14/2019 om utkastet till standardavtalsklausuler inlämnat av den danska tillsynsmyndigheten (artikel 28.8 i dataskyddsförordningen) rekommenderade EDPB att ordalydelsen i artikel 28.3 a skulle inkluderas för att säkerställa rättssäkerhet.

¹⁰⁹ Den slovenska tillsynsmyndighetens standardavtalsklausuler för efterlevnad av artikel 28 i dataskyddsförordningen, särskilt klausulerna 3.1 och 7.2.

¹¹⁰ Den litauiska tillsynsmyndighetens standardavtalsklausuler för efterlevnad av artikel 28 i dataskyddsförordningen, särskilt klausulerna 4.1, 22 och 23.

av personuppgifter som inte bygger på den personuppgiftsansvariges instruktioner, och därför inte sker på den personuppgiftsansvariges vägnar, b) behovet av att personuppgiftsbiträdet informerar den personuppgiftsansvarige¹¹¹, och c) hänvisningen till ett sådant rättsligt krav som följer av EU:s eller en medlemsstats lagstiftning.

104. I detta sammanhang påminner EDPB om den allmänna principen att avtal inte kan åsidosätta lagen. Detta innebär att oavsett om den klausul som föreskrivs i artikel 28.3 a i dataskyddsförordningen (*"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"*) ingår i ett avtal eller inte, kan den inte förhindra att rättsliga krav tillämpas utöver eller, i vissa fall, i strid med avtalskraven. I enlighet med den allmänna principen om att avtal inte medför skyldigheter gentemot tredje man kan ett avtal heller inte binda exempelvis offentliga myndigheter i en medlemsstat eller ett tredjeland¹¹².
105. Varje avtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde måste ta upp situationer där personuppgiftsbiträdet enligt lagstiftning kan åläggas att behandla personuppgifter på annat sätt än på grundval av den personuppgiftsansvariges instruktioner. Personuppgiftsbitrådets skyldighet att informera den personuppgiftsansvarige innan en databehandling utförs som inte grundar sig på dennes instruktioner är också en central del av sådana avtal, och måste ingå¹¹³.
106. För personuppgifter som behandlas utanför EES kan det hända att hänvisningen till EU:s eller medlemsstaternas lagstiftning inte är särskilt meningsfull, med tanke på att ett personuppgiftsbiträde utanför EES endast i undantagsfall kommer att omfattas av EU:s eller medlemsstaternas rättsliga krav. I detta avseende noterar EDPB att de standardavtalsklausuler för internationella överföringar som är avsedda att uppfylla kraven i artikel 28.3 och 28.4 i dataskyddsförordningen¹¹⁴ (utöver kraven i artikel 46.1 och artikel 46.2 d i samma förordning), inte innehåller en ordalydelse som liknar *"såvida inte"* i artikel 28.3 a i dataskyddsförordningen. Kravet på att endast behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte annat krävs enligt unionsrätten eller medlemsstaternas lagstiftning, behandlas dock redan indirekt genom klausul 8.1 i

¹¹¹ I artikel 28.3 a i dataskyddsförordningen föreskrivs att om unionsrätten eller en medlemsstats nationella rätt kräver att personuppgiftsbiträdet behandlar personuppgifter *"ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt"*.

¹¹² Därför innehåller kommissionens standardavtalsklausuler för internationella överföringar flera skyddsåtgärder som ålägger uppgiftsutföraren och uppgiftsinföraren att bedöma de obligatoriska kraven i ett tredjelandets lagstiftning innan de överför uppgifterna för att säkerställa att de inte går utöver vad som är nödvändigt i ett demokratiskt samhälle (klausul 14 a–d), att uppgiftsinföraren ska underrätta uppgiftsutföraren om ändringar och att denne ska agera i enlighet därmed (klausul 14 e och f), och att ålägga uppgiftsinföraren skyldigheter i händelse av tillgång för offentliga myndigheter (klausul 15). Se EU-domstolens dom i målet Schrems II, punkterna 125 och 141.

¹¹³ I EDPB:s yttrande 18/2021 om utkastet till standardavtalsklausuler som lämnats in av den litauiska tillsynsmyndigheten (artikel 28.8 i dataskyddsförordningen) rekommenderade EDPB att den sista delen av artikel 28.3 a skulle inkluderas i standardavtalsklausulerna (dvs. personuppgiftsbitrådets skyldighet att informera den personuppgiftsansvarige om det tillämpliga rättsliga kravet), EDPB:s yttrande 18/2021, punkt 19.

¹¹⁴ Se skäl 9 i kommissionens standardavtalsklausuler för internationella överföringar: *"Om behandlingen inbegriper överföringar av personuppgifter från personuppgiftsansvariga som omfattas av förordning (EU) 2016/679 till personuppgiftsbiträden som inte omfattas av dess geografiska tillämpningsområde, eller från personuppgiftsbiträden som omfattas av förordning (EU) 2016/679 till underbiträden som inte omfattas av dess geografiska tillämpningsområde, bör de standardavtalsklausuler som anges i bilagan till detta beslut också göra det möjligt att uppfylla kraven i artikel 28.3 och 28.4 i förordning (EU) 2016/679."*

kommissionens standardavtalsklausuler för internationella överföringar.¹¹⁵ Detta innebär vidare inte att informationsskyldigheten i artikel 28.3 a i dataskyddsförordningen lämnas obehandlad, med tanke på att kommissionens standardavtalsklausuler för internationella överföringar uttryckligen omfattar behovet av att uppgiftsinföraren informerar uppgiftsutföraren om den förstnämnda inte kan följa den personuppgiftsansvariges instruktioner¹¹⁶. Följaktligen är personuppgiftsbiträdet skyldigt att informera den personuppgiftsansvarige när ett rättsligt krav på behandling är tillämpligt (oavsett om det härrör från unionsrätten, medlemsstatens lagar eller tredjelandets lagstiftning). Detta följer av kommissionens standardavtalsklausuler för internationella överföringar, även om inte den exakta formuleringen *"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* i artikel 28.3 a i dataskyddsförordningen (element c ovan) används.

107. Detta är förenligt med syftet med artikel 28.3 a i dataskyddsförordningen: att säkerställa att den personuppgiftsansvarige informeras när personuppgiftsbiträdet enligt lag är skyldigt att behandla andra personuppgifter än dem som följer av den personuppgiftsansvariges instruktioner.
108. Mot bakgrund av analysen ovan anser EDPB att det undantag som föreskrivs i artikel 28.3 a i dataskyddsförordningen, *"såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"* (antingen ordagrant eller i mycket likartade ordalag), i avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet¹¹⁷ är att rekommendera starkt men inte är strikt nödvändigt för förenlighet med artikel 28.3 a i dataskyddsförordningen. Denna ståndpunkt påverkar inte behovet av en avtalsenlig skyldighet att

¹¹⁵ I klausul 8 om skyddsåtgärder för personuppgifter (modul två: Överföringar från personuppgiftsansvarig till personuppgiftsbiträde) anges följande i avsnitt 8.1 – instruktioner:

"a) Uppgiftsinföraren ska endast behandla personuppgifterna enligt dokumenterade instruktioner från uppgiftsutföraren. Uppgiftsutföraren får ge sådana instruktioner under hela avtalets giltighetstid.

b) Uppgiftsinföraren ska omedelbart informera uppgiftsutföraren vid eventuell oförmåga att följa dessa instruktioner."

På samma sätt anges i modul tre (Överföringar från personuppgiftsbiträde till personuppgiftsbiträde), klausul 8 om dataskyddsgarantier, avsnitt 8.1 – instruktioner:

"a) Uppgiftsutföraren har informerat uppgiftsinföraren om att han eller hon agerar i egenskap av personuppgiftsbiträde enligt den eller de personuppgiftsansvarigas instruktioner, vilka uppgiftsutföraren ska göra tillgängliga för uppgiftsinföraren före behandlingen.

b) Uppgiftsinföraren ska endast behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige, vilka uppgiftsutföraren ska tillhandahålla uppgiftsinföraren, och eventuella ytterligare dokumenterade instruktioner från uppgiftsutföraren. Sådana ytterligare instruktioner får inte stå i strid med den personuppgiftsansvariges instruktioner. Den personuppgiftsansvarige eller uppgiftsutföraren får ge ytterligare dokumenterade instruktioner avseende behandlingen av personuppgifter under hela avtalets giltighetstid.

c) Uppgiftsinföraren ska omedelbart informera uppgiftsutföraren vid eventuell oförmåga att följa dessa instruktioner. Om uppgiftsinföraren inte kan följa den personuppgiftsansvariges instruktioner ska uppgiftsutföraren omedelbart informera den personuppgiftsansvarige."

¹¹⁶ Utöver klausul 8.1 (se föregående fotnot) anges följande i punkt 14 e i klausul 14: *"Uppgiftsinföraren samtycker till att skyndsamt meddela uppgiftsutföraren om han eller hon, efter att ha godkänt dessa klausuler och under hela avtalets giltighetstid, har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i led a, däribland efter en ändring i lagarna i tredjelandet eller en åtgärd (såsom en begäran om utlämnande av uppgifter) som antyder att en tillämpning av sådana lagar i praktiken inte stämmer överens med kraven i led a. [För modul 3: Uppgiftsutföraren ska vidarebefordra meddelandet till den personuppgiftsansvarige.]"*

¹¹⁷ I synnerhet när den personuppgiftsansvarige och personuppgiftsbiträdet förlitar sig på ett eget avtal avseende databehandling snarare än på kommissionens standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden eller på standardavtalsklausuler som antagits av tillsynsmyndigheter i syfte att uppfylla kraven i artikel 28 i dataskyddsförordningen eller på kommissionens standardavtalsklausuler för internationella överföringar. Se även skäl 109 och artikel 28.6 i förordning (EU) 2016/679.

informera den personuppgiftsansvarige när personuppgiftsbiträdet enligt lag är skyldigt att behandla personuppgifter på annat sätt än genom att följa den personuppgiftsansvariges instruktioner, i enlighet med artikel 28.3 a i dataskyddsförordningen. Om det står klart att unionens eller medlemsstaternas rättsliga krav är relevanta för behandlingen bidrar användning av formuleringen i artikel 28.3 a i dataskyddsförordningen till att visa på efterlevnad.

109. EDPB riktar uppmärksamheten på frågan om huruvida ett avtal som innehåller ett bredare undantag som även omfattar tredjelandets lagstiftning, såsom ett undantag från skyldigheten att endast behandla personuppgifterna på dokumenterade instruktioner från den personuppgiftsansvarige *”såvida inte detta krävs enligt lag eller bindande beslut av ett statligt organ”*, i sig utgör en överträdelse av artikel 28.3 a i dataskyddsförordningen.
110. Denna formulering kan, om den inte åtföljs av ytterligare specifikationer, omfatta två olika situationer som bör analyseras var för sig mot bakgrund av det rättsliga sammanhanget:
 - Det planerade rättsliga kravet eller bindande beslutet följer av unionsrätten eller lagstiftningen i en medlemsstat (EES).
 - Det planerade rättsliga kravet eller det bindande beslutet följer av andra lagar än unionsrätten eller lagstiftningen i en medlemsstat (EES).

111. Den första situationen omfattas av de uttryckliga bestämmelserna i artikel 28.3 a i dataskyddsförordningen, där det fastställs ett avtalsenligt åtagande för personuppgiftsbiträdet att endast behandla uppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige *"såvida det inte krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av"*. Detta gäller oavsett om behandlingen av personuppgifterna sker inom eller utanför EES.
112. EU-lagstiftningen, inbegripet dataskyddsförordningen och medlemsstaternas rättsliga krav, ingår i samma konstitutionella tradition som dataskyddsförordningen, som fastställer skyddet av fysiska personer med avseende på behandling av personuppgifter som en grundläggande rättighet, enligt artikel 16.1 i fördraget om Europeiska unionens funktionssätt (**EUF-fördraget**) och artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (**stadgan**)¹¹⁸.
113. Om parterna på grundval av andra delar av sina avtal kan visa att endast den första situationen omfattas av formuleringen *"såvida inte detta krävs enligt lag eller bindande beslut av ett statligt organ"* påverkar denna formulering inte de garantier som föreskrivs i artikel 28.3 a i dataskyddsförordningen.
114. Det kommer att förekomma fall där parternas avtal går utöver denna första typ av situation, vilket innebär att en hänvisning till *"lag eller bindande beslut av ett statligt organ"* omfattar rättsliga krav/bindande föreskrifter som härrör från andra lagar än unionsrätten eller (EES-)medlemsstaternas nationella rätt (den andra typen av situation).
115. EDPB noterar att krav på behandling av uppgifter som grundar sig på annan lagstiftning än unionsrätten eller lagstiftningen i medlemsstaterna i EES inte delar den konstitutionella traditionen och inte automatiskt kan betraktas på samma sätt som krav inom EU:s rättsordning (mot bakgrund av artikel 44 i dataskyddsförordningen). I detta sammanhang erinrar EDPB om att termerna "rättslig förpliktelse", "allmänt intresse" och "offentlig myndighet" i artikel 6 i dataskyddsförordningen hänvisar till unionsrätten eller medlemsstaternas nationella lagstiftning¹¹⁹. På samma sätt noterar EDPB att artikel 29 i dataskyddsförordningen om databehandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende föreskriver att *"[p]ersonuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt."* (fetstil tillagd)

¹¹⁸ I skäl 1 i dataskyddsförordningen hänvisas till artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (stadgan). I artikel 52.1 i stadgan anges följande: *"Varje begränsning i utövandet av de rättigheter och friheter som erkänns i denna stadga ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter."*

¹¹⁹ I artikel 6.3 i dataskyddsförordningen fastställs att om den rättsliga grunden för behandlingen är en "rättslig skyldighet" (artikel 6.1 c i dataskyddsförordningen) eller om behandlingen "är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning" (artikel 6.1 e i dataskyddsförordningen), avser detta bestämmelser i unionsrätten eller i medlemsstaternas lagstiftning som den personuppgiftsansvarige omfattas av. När det gäller artikel 6 i dataskyddsförordningen förklaras i skäl 40 i dataskyddsförordningen att när den rättsliga grunden för behandlingen fastställs i lag innebär detta *"antingen i denna förordning eller i annan unionsrätt eller medlemsstaternas nationella rätt enligt denna förordning"*. Enligt artikel 49.4 i dataskyddsförordningen föreskrivs att endast ett allmänintresse som är erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av kan motivera tillämpning av detta undantag.

116. I samband med överföringar är det rimligt att anta att rättsliga krav kan uppstå även genom annan lagstiftning än EU-lagstiftning eller medlemsstaternas lagstiftning. När överföringar äger rum påminner EDPB om att kapitel V i dataskyddsförordningen är tillämpligt utöver artikel 28 i samma förordning. När det gäller personuppgifter som behandlas utanför EES anser EDPB att artikel 28.3 a i dataskyddsförordningen i princip inte hindrar att man i avtalet lägger till bestämmelser som avser krav i tredjelandets lagstiftning avseende behandling av överförda personuppgifter. Sådana bestämmelser kan i synnerhet läggas till för att säkerställa efterlevnad av kapitel V i dataskyddsförordningen, men det är mycket osannolikt att enbart tillägg av formuleringen *”såvida det inte krävs enligt lag eller bindande beslut av ett statligt organ”* skulle vara tillräckligt.
117. I detta sammanhang konstaterar EDPB att kommissionens standardavtalsklausuler för internationella överföringar specifikt behandlar *”lokala lagar och förfaranden som påverkar efterlevnaden av klausulerna”* i klausul 14 och uppgiftsförarens skyldigheter vid åtkomst av offentliga myndigheter i klausul 15. Innan parterna undertecknar standardavtalsklausuler måste de bedöma om det finns lokala lagar och förfaranden som påverkar efterlevnaden av klausulerna (klausul 14 i kommissionens standardavtalsklausuler för internationella överföringar). Enligt klausul 14 ska parterna garantera att de inte har någon anledning att misstänka att de lagar och förfaranden i det tredjeland där uppgiftsföraren är baserad skulle hindra uppgiftsföraren från att fullgöra sina skyldigheter enligt standardavtalsklausulerna för internationella överföringar, efter en bedömning från uppgiftsförarens sida av sådan lagstiftning och praxis. Enligt klausulen krävs det också att uppgiftsföraren omedelbart underrättar uppgiftsutföraren om varje ändring, med följd effekten att uppgiftsutföraren antingen identifierar lämpliga åtgärder för att hantera situationen eller avbryter överföringen med möjlighet att säga upp avtalet enligt klausul 14. I klausul 15 åläggs uppgiftsföraren vissa skyldigheter i händelse av att offentliga myndigheter i tredje land får tillgång till uppgifterna. Där fastställs ett antal åtgärder som uppgiftsföraren måste vidta när den får tillgång till uppgifter från myndigheter i tredje land (antingen på begäran eller direkt), vilka har som (slutligt) mål att säkerställa att den personuppgiftsansvarige informeras. Förutom skyldigheten att underrätta uppgiftsutföraren har uppgiftsföraren bland annat skyldighet att pröva om begäran om tillgång är laglig och dokumentera denna rättsliga bedömning, samt att i vissa fall bestrida begäran. Uppgiftsutföraren kommer då – i samråd med den personuppgiftsansvarige om uppgiftsutföraren inte är den personuppgiftsansvarige – att kunna vidta nödvändiga åtgärder, inklusive att eventuellt avbryta överföringen tillfälligt eller säga upp avtalet som innehåller standardavtalsklausulerna för internationella överföringar. Huruvida eventuella (vidare) överföringar till tredjelandets myndigheter är förenliga med dataskyddsförordningen är avhängigt en analys från fall till fall (bland annat beroende på den rättsliga grunden, personuppgiftsansvaret och efterlevnaden av kapitel V i dataskyddsförordningen). Enligt modul 3 i kommissionens standardavtalsklausuler för internationella överföringar (från personuppgiftsbiträde till personuppgiftsbiträde) är uppgiftsföraren/personuppgiftsbiträdet skyldig/skyldigt att göra den rättsliga bedömningen tillgänglig för uppgiftsutföraren. I detta avseende hänvisar EDPB även till punkterna 88–89 och 106 ovan.
118. Enligt kommissionens standardavtalsklausuler för internationella överföringar är dessutom både uppgiftsutföraren och uppgiftsföraren skyldiga att försäkra sig om att lagstiftningen i det mottagande tredjelandet gör det möjligt för uppgiftsföraren att följa kommissionens standardavtalsklausuler för internationella överföringar innan personuppgifter överförs till detta tredjeland¹²⁰. Om personuppgiftsbiträdet exporterar personuppgifter för den personuppgiftsansvariges räkning faller

¹²⁰ EU-domstolens dom i målet *Schrems II*, punkt 141. Se även kommissionens standardavtalsklausuler för internationella överföringar, klausul 14 a–d.

denna skyldighet också på den personuppgiftsansvarige (se även punkt 79 och därpå följande punkter ovan).

119. På samma sätt fastställer rekommendationerna om bindande företagsbestämmelser för personuppgiftsansvariga och referensramen om bindande företagsbestämmelser för personuppgiftsbiträden också en uppsättning skyldigheter i fall där en medlem som omfattas av de bindande företagsbestämmelserna är föremål för en konflikt mellan lokala lagar och de bindande företagsbestämmelserna¹²¹, och/eller mottar en begäran om utlämnande från en brottsbekämpande myndighet eller ett statligt säkerhetsorgan¹²². Mer specifikt anges i EDPB:s rekommendationer 1/2022¹²³ att bindande företagsbestämmelser för personuppgiftsansvariga bör innehålla klausuler som behandlar lokal lagstiftning och praxis som påverkar efterlevnaden av de bindande företagsbestämmelserna för personuppgiftsansvariga (avsnitt 5.4.1) samt uppgiftsförarens skyldigheter vid offentliga begäranden om åtkomst (avsnitt 5.4.2). Bindande företagsbestämmelser för personuppgiftsansvariga kan fungera som en överföringsmekanism för överföringar till personuppgiftsbiträden inom gruppen av företag.
120. I de fall då överföringarna omfattas av beslut om adekvat skyddsnivå är lagstiftningen om *”offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning”* en av de faktorer som Europeiska kommissionen måste ta hänsyn till när den bedömer om skyddsnivån är adekvat, enligt artikel 45.2 a i dataskyddsförordningen¹²⁴.

¹²¹ Avsnitt 5.4.1, ”Lokala lagar och förfaranden som påverkar efterlevnaden av de bindande företagsbestämmelserna för personuppgiftsansvariga”, EDPB:s rekommendationer 1/2022 om ansökan om godkännande och om de delar och principer som ska återfinnas i de bindande företagsbestämmelser för personuppgiftsansvariga (artikel 47 i dataskyddsförordningen). Avsnitt 6.3 ”Behovet av öppenhet när nationell lagstiftning hindrar koncernen från att följa de bindande företagsbestämmelserna” i artikel 29-arbetsgruppens arbetsdokument om inrättande av en tabell med de element och principer som ska finnas med i de bindande företagsbestämmelserna för personuppgiftsbiträden, WP 257 rev.01, som godkändes av EDPB den 25 maj 2018.

¹²² Avsnitt 5.4.2 ”Uppgiftsförarens skyldigheter vid begäran om tillgång från myndigheter”, EDPB:s rekommendationer 1/2022 om ansökan om godkännande och om de delar och principer som ska återfinnas i de bindande företagsbestämmelser för personuppgiftsansvariga (artikel 47 i dataskyddsförordningen); se även avsnitt 6.3 ”Behovet av öppenhet när den nationella lagstiftningen förhindrar att koncernen eller gruppen av företag efterlever de bindande företagsbestämmelserna”, i Arbetsdokument med en tabell över de element och principer som ska finnas med i bindande företagsbestämmelser för personuppgiftsbiträden, WP 257 rev.01.

¹²³ EDPB:s rekommendationer 1/2022 om ansökan om godkännande och om de delar och principer som ska återfinnas i de bindande företagsbestämmelser för personuppgiftsansvariga (artikel 47 i dataskyddsförordningen).

¹²⁴ EU-domstolen behandlade denna aspekt i sina domar i målen Schrems I och Schrems II. EU-domstolens dom av den 6 oktober 2015, *Maximillian Schrems mot Data Protection Commissioner*, (nedan kallad EU-domstolens dom i målet Schrems I), mål C-362/14, ECLI:EU:C:2015:650, punkt 91 ff. EU-domstolens dom i målet Schrems II, punkterna 141, 174–177 och 187–189.

121. Gemensamt för besluten om adekvat skyddsnivå¹²⁵, standardavtalsklausulerna för internationella överföringar¹²⁶ och rekommendationerna och referensramen för bindande företagsbestämmelser¹²⁷ är att sådana lagar och sådan praxis i ett tredjeland som respekterar det väsentliga innehållet i de grundläggande rättigheter och friheter som fastställs i EUF-fördraget, stadgan och dataskyddsförordningen och som inte går utöver vad som i ett demokratiskt samhälle är nödvändigt och proportionerligt för att skydda ett av de mål som anges i artikel 23.1 i dataskyddsförordningen, inte kommer att undergräva den skyddsnivå som säkerställs genom dataskyddsförordningen¹²⁸. Av detta skäl innehåller standardavtalsklausulerna för internationella överföringar¹²⁹ och rekommendationerna och referensramen för bindande företagsbestämmelser¹³⁰ bestämmelser som medför olika konsekvenser för lagstiftning och praxis beroende på om de undergräver den skyddsnivå som säkerställs genom dataskyddsförordningen. Ad hoc-kontrakt baserade på artikel 46.3 a i dataskyddsförordningen bör också innehålla liknande bestämmelser¹³¹.
122. Det framgår av ovanstående att när lagar i tredjelandet kräver att personuppgiftsbiträdet behandlar personuppgifter på annat sätt än enligt instruktioner från den personuppgiftsansvarige, kommer den skyddsnivå som fastställs i dataskyddsförordningen endast att respekteras om lagarna i fråga uppfyller ovannämnda villkor. Under alla omständigheter bör personuppgiftsbiträdet vidta kompletterande åtgärder om dessa villkor inte är uppfyllda, och avtalet bör säkerställa att dessa villkor är uppfyllda.
123. När personuppgiftsbiträden behandlar personuppgifter inom EES kan de under vissa omständigheter ändå ställas inför tredje lands lagstiftning. EDPB understryker att en hänvisning till tredjelandslagstiftning i avtalet inte befriar personuppgiftsbiträdet från dess skyldigheter enligt dataskyddsförordningen.
124. Mot bakgrund av analysen ovan anser EDPB att tillägget av *"såvida det inte krävs enligt lag eller bindande beslut av ett statligt organ"* eller en liknande formulering utgör en del av parternas

¹²⁵ Se artikel 45.2 a i dataskyddsförordningen, där det föreskrivs att Europeiska kommissionen ska beakta *"rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs"*. Se även artikel 29-gruppens referensram för adekvat skyddsnivå, WP 254 rev.01, som antogs den 6 februari 2018 och godkändes av EDPB den 25 maj 2018. Begreppet "adekvat skyddsnivå" har vidareutvecklats av EU-domstolen i domarna i målen Schrems I (punkterna 73 och 74) och Schrems II (punkt 94).

¹²⁶ Klausul 14 a i standardavtalsklausulerna för internationella överföringar.

¹²⁷ Detta framgår uttryckligen av EDPB:s rekommendationer 1/2022 (rekommendationerna om bindande företagsbestämmelser för personuppgiftsansvariga), version 2.1, under punkterna 5.4.1 och 5.4.2. Samma tolkning ligger implicit till grund för avsnitt 6.3, "Behovet av öppenhet när den nationella lagstiftningen förhindrar att koncernen eller gruppen av företag efterlever de bindande företagsbestämmelserna" i artikel 29-gruppens Arbetsdokument med en tabell över de element och principer som ska finnas med i bindande företagsbestämmelser för personuppgiftsbiträden, WP 257 rev.01, som godkändes av EDPB den 25 maj 2018.

¹²⁸ EDPB:s rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, v. 2.0, punkt 38, samt EDPB:s rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, punkterna 22 och 24.

¹²⁹ Klausul 14 i kommissionens standardavtalsklausuler för internationella överföringar.

¹³⁰ Se fotnot 127.

¹³¹ EDPB:s rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, v. 2.0, punkt 66.

avtalsfrihet och inte i sig utgör en överträdelse av artikel 28.3 a i dataskyddsförordningen. Detta påverkar inte skyldigheten att uppfylla kraven i dataskyddsförordningen när personuppgifter behandlas. Vidare befriar en sådan klausul inte den personuppgiftsansvarige eller personuppgiftsbiträdet från att fullgöra sina skyldigheter enligt dataskyddsförordningen, inte heller när det gäller den information som ska lämnas till den personuppgiftsansvarige och – i tillämpliga fall – villkoren för internationella överföringar av personuppgifter som behandlas på den personuppgiftsansvariges vägnar.¹³²

125. I slutet av begäran ställs en uppföljningsfråga:

Om svaret på fråga 2a är nej, ska ett sådant utvidgat undantag i stället tolkas som en dokumenterad instruktion från den personuppgiftsansvarige i den mening som avses i artikel 28.3 a i dataskyddsförordningen?

126. Mot bakgrund av svaret ovan tolkar EDPB den sista frågan som en fråga om ifall parterna kan hävda att formuleringen *”såvida de inte är skyldiga att göra detta enligt lag eller bindande beslut från ett statligt organ”* (antingen ordagrant eller i mycket likartade ordalag) i deras avtal bör tolkas som en dokumenterad instruktion från den personuppgiftsansvarige i den mening som avses i artikel 28.3 a i dataskyddsförordningen.

127. Till att börja med överväger EDPB om detta argument är hållbart när det rättsliga kravet eller det bindande föreläggandet följer av unionsrätten eller (EES-)medlemsstaternas lagstiftning.

128. EDPB noterar att begreppet *”instruktioner”* som används i artikel 28.3 a i dataskyddsförordningen specifikt avser den personuppgiftsansvariges anvisningar om vilken uppgiftsbehandling som personuppgiftsbiträdet förväntas utföra på dennes vägnar, och hur¹³³. En bestämmelse som den personuppgiftsansvarige inkluderar i avtalet med sin tjänsteleverantör/sitt personuppgiftsbiträde och som inte består av en begäran om att utföra behandling av personuppgifter för den personuppgiftsansvariges räkning kan inte heller betraktas som instruktion i den mening som avses i artikel 28.3 a i dataskyddsförordningen. Vidare skulle den personuppgiftsansvariges instruktioner behöva vara tillräckligt ingående för att täcka en specifik behandling av personuppgifter, vilket inte är fallet med den aktuella formuleringen. Dessutom skulle den personuppgiftsansvarige alltid (behöva) ha möjlighet att återkalla en sådan instruktion – och vara rättsligt skyldig att göra detta om en instruktion att behandla personuppgifter för den personuppgiftsansvariges räkning skulle strida mot dataskyddsförordningen. Personuppgiftsbiträdet ska sedan följa den personuppgiftsansvariges tillbakadragande av sin instruktion och avbryta databehandlingen.

129. Genom att tillhandahålla instruktioner till personuppgiftsbiträdet omsätter den personuppgiftsansvarige sitt fastställande av ändamål och medel för databehandling i praktiken, särskilt genom att utöva inflytande över de viktigaste delarna av behandlingen¹³⁴. I princip upphör den personuppgiftsansvariges inflytande över behandlingen av personuppgifter när EU:s eller medlemsstaternas lagstiftning innehåller krav på att personuppgiftsbiträdet ska utföra behandling av personuppgifter som den personuppgiftsansvarige inte kan styra över eller stoppa¹³⁵. Även om den

¹³² Med avseende på databehandling utanför EES, särskilt den personuppgiftsansvariges skyldighet att säkerställa att endast tredjelandslagstiftning som säkerställer en väsentligen likvärdig skyddsnivå kan kräva databehandling av personuppgiftsbiträdet. Se även punkterna 116–122 ovan.

¹³³ EDPB:s riktlinjer 07/2020, punkt 116.

¹³⁴ EDPB:s riktlinjer 07/2020, punkt 20.

¹³⁵ I detta avseende skulle situationen då kunna vara den som föreskrivs i artikel 4.7 i dataskyddsförordningen, där det anges att om ändamålen och medlen för behandlingen fastställs i unionsrätten eller i medlemsstaternas

personuppgiftsansvarige kan påminna personuppgiftsbiträdet om att följa EU:s eller medlemsstaternas lagstiftning, kan detta inte förstås som en instruktion i den mening som avses i artikel 28.3 a i dataskyddsförordningen¹³⁶. I dataskyddsförordningen erkänns detta förhållande just genom att fastställa att personuppgiftsbiträdet endast får behandla uppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, om annan behandling inte krävs enligt unionsrätten eller en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av (artikel 28.3 a i dataskyddsförordningen), och genom att föreskriva att personuppgiftsbiträdet omedelbart måste informera den personuppgiftsansvarige om en instruktion strider mot dataskyddsförordningen (artikel 28.3 sista stycket i dataskyddsförordningen).

130. EDPB anser att resonemanget ovan även är tillämpligt när det rättsliga kravet eller det bindande beslutet följer av tredjelandets lagstiftning. I denna situation begränsar lagen i fråga det inflytande som den personuppgiftsansvarige kan utöva över behandlingen av uppgifter.
131. Utöver ovanstående gäller att en klausul enligt vilken ett personuppgiftsbiträde åtar sig att behandla personuppgifter endast på dokumenterade instruktioner från den personuppgiftsansvarige *"såvida de inte är skyldiga att göra detta enligt lag eller bindande beslut från ett statligt organ"* i sig innebär att behandling på instruktion från den personuppgiftsansvarige är regeln, medan undantaget finns just för behandling som inte sker på instruktion från den personuppgiftsansvarige (vilket framgår av orden *"såvida inte"*). Vidare är det fortfarande upp till personuppgiftsbiträdet att besluta om det ska följa den rättsliga begäran eller det bindande beslutet som det omfattas av eller om det föredrar att ta de rättsliga konsekvenserna av att inte göra det.
132. På grundval av detta drar EDPB slutsatsen att *"såvida de inte är skyldiga att göra detta enligt lag eller bindande beslut från ett statligt organ"* (antingen ordagrant eller i mycket likartade ordalag) inte kan tolkas som en dokumenterad instruktion från den personuppgiftsansvarige. Den personuppgiftsansvarige förblir ansvarig för att säkerställa att personuppgiftsbiträdet (underentreprenören) endast behandlar personuppgifter på dennes dokumenterade instruktioner. Detta är dock inte tillämpligt om behandlingen krävs enligt unionsrätten eller medlemsstaternas nationella lagstiftning, eller för behandling utanför EES när behandlingen krävs enligt lagstiftning i ett tredjeland som personuppgiftsbiträdet (eller underentreprenören) omfattas av, om den lagstiftningen säkerställer en väsentligen likvärdig skyddsnivå.

För Europeiska dataskyddsstyrelsen

Ordförande

(Anu Talus)

nationella rätt får den personuppgiftsansvarige eller de särskilda kriterierna för att utse denne fastställas i unionsrätten eller i medlemsstaternas nationella rätt. Se EU-domstolens dom av den 11 januari 2024, *Belgian State (Données traitées par un journal officiel)*, mål C-231/22, ECLI:EU:C:2024:7, punkterna 28–30, 35 och 39; EDPB:s riktlinjer 07/2020, punkterna 22–24.

¹³⁶ En sådan påminnelse kommer snarare att betraktas som att den personuppgiftsansvarige inför avtalsenliga skyddsåtgärder för att säkerställa att behandlingen för den personuppgiftsansvariges räkning uppfyller alla krav i dataskyddsförordningen och säkerställer skyddet av den registrerades rättigheter.