Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR

Version 2.0

Antaget den 7 juli 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versionshistorik

Version 2.0	7 juli 2021	Antagande av riktlinjerna efter offentligt samråd
Version 1.0	2 september 2020	Antagande av riktlinjerna inför offentligt samråd

SAMMANFATTNING

Begreppen personuppgiftsansvarig, gemensamt personuppgiftsansvarig och personuppgiftsbiträde spelar en viktig roll i tillämpningen av den allmänna dataskyddsförordningen 2016/679 (GDPR), eftersom de fastställer vem som ska ansvara för efterlevnaden av olika dataskyddsbestämmelser och hur registrerade personer kan utöva sina rättigheter i praktiken. Den exakta innebörden av dessa begrepp och kriterierna för korrekt tolkning av dessa måste vara tillräckligt tydliga och konsekventa inom hela det Europeiska ekonomiska samarbetsområdet (EES).

Begreppen personuppgiftsansvarig, gemensamt personuppgiftsansvarig och personuppgiftsbiträde är *funktionella* begrepp eftersom de syftar till att tilldela ansvarsskyldigheter i enlighet med parternas faktiska roller och *autonoma* begrepp i den bemärkelse att de i huvudsak bör tolkas i enlighet till EU:s dataskyddsbestämmelser.

Personuppgiftsansvarig

I princip finns det ingen begränsning vad gäller typen av enhet som kan åta sig rollen som personuppgiftsansvarig, men i praktiken är det vanligen själva organisationen och inte en individ inom organisationen (som exempelvis vd:n, en anställd eller en styrelsemedlem) som fungerar som personuppgiftsansvarig.

En personuppgiftsansvarig är ett organ som *beslutar* vissa nyckelelement för behandlingen. Personuppgiftsansvar kan definieras av lagstiftning eller kan härledas från en analys av de faktiska elementen eller omständigheterna för respektive fall. Vissa behandlingsaktiviteter kan ses som naturligt förknippade till en enhets roll (en arbetsgivare till anställda, en utgivare till prenumeranter eller en förening till sina medlemmar). I många fall kan villkoren i ett avtal hjälpa till att identifiera den personuppgiftsansvarige, även om de inte är avgörande under alla omständigheter.

En personuppgiftsansvarig fastställer behandlingsändamålet och behandlingssättet, dvs. *varför* och *hur* en behandling ska utföras. Den personuppgiftsansvarige måste besluta angående både ändamål och behandlingssätt. Dock kan vissa mera praktiska aspekter av implementeringen (”icke-väsentliga medel”) överlåtas till personuppgiftsbiträdet. Det är inte nödvändigt att den personuppgiftsansvarige har åtkomst till uppgifterna som behandlas för att vara kvalificerad som personuppgiftsansvarig.

Gemensamt personuppgiftsansvariga

Kvalificeringen som gemensamt personuppgiftsansvariga kan uppstå när mer än en aktör är involverad i behandlingen. GDPR har infört särskilda regler för gemensamt personuppgiftsansvariga och stipulerar ett ramverk för att styra relationen mellan parterna. Det övergripande kriteriet för att gemensamt personuppgiftsansvar ska föreligga är gemensamt deltagande av två eller flera enheter i fastställandet av behandlingsändamål och behandlingssätt. Gemensamt deltagande kan ske i form av ett *gemensamt beslut* som fattas av två eller flera enheter eller som är ett resultat av *konvergerande beslut* av två eller flera enheter där besluten kompletterar varandra och är nödvändiga för att behandlingen ska kunna ske på ett sådant sätt att de har en påtaglig inverkan på fastställandet av behandlingsändamål och behandlingssätt. Ett viktigt kriterium är att behandlingen inte skulle vara möjlig utan båda parternas deltagande i betydelsen att behandlingen från varje part är oskiljbar, dvs. den är oupplösligt sammanflätad. Det gemensamma deltagandet måste inkludera fastställandet av behandlingsändamålet å ena sidan och fastställandet av behandlingssättet å andra sidan.

Personuppgiftsbiträde

Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det finns två grundläggande villkor för att kvalificeras som personuppgiftsbiträde: att man är en separat enhet i relation till den personuppgiftsansvarige och att man behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgiftsbiträdet får inte behandla uppgifterna på annat sätt än i enlighet med den personuppgiftsansvariges instruktioner. Den personuppgiftsansvariges instruktioner kan fortfarande tillåta viss handlingsfrihet angående hur man bäst försvarar den personuppgiftsansvariges intressen genom att tillåta personuppgiftsbiträdet att välja de mest lämpliga tekniska och organisationsmässiga behandlingssätten. Ett personuppgiftsbiträde bryter dock mot GDPR om man avviker från den personuppgiftsansvariges instruktioner och börjar att fastställa sina egna behandlingsändamål och behandlingssätt. Personuppgiftsbiträdet kommer då att betraktas som en personuppgiftsansvarig för denna behandling och kan vara föremål för sanktioner för att ha avvikit från den personuppgiftsansvariges instruktioner.

Relationen mellan personuppgiftsansvarig och personuppgiftsbiträde

En personuppgiftsansvarig får endast använda personuppgiftsbiträden som kan tillhandahålla tillräckliga garantier för implementering av lämpliga tekniska och organisationsmässiga åtgärder så att behandlingen uppfyller kraven för GDPR. Element som bör beaktas kan vara personuppgiftsbiträdets expertkunskaper (t.ex. teknisk expertis vad gäller säkerhetsåtgärder och dataintrång), personuppgiftsbiträdets tillförlitlighet, personuppgiftsbiträdets resurser och personuppgiftsbiträdets efterlevnad av en godkänd uppförandekod eller certifieringsmekanism.

All behandling av personuppgifter av ett personuppgiftsbiträde måste styras av ett avtal eller annan juridisk handling som ska vara skriftlig, inklusive i elektroniskt format och vara bindande. Den personuppgiftsansvarige och personuppgiftsbiträdet kan välja att förhandla fram sitt eget avtal som inkluderar alla obligatoriska element eller helt eller delvis förlita sig på ett standardavtal.

GDPR anger elementen som bör ingå i behandlingsavtalet. Behandlingsavtalet bör dock inte bara upprepa bestämmelserna i GDPR utan bör snarare inkludera mera specifik och konkret information angående hur kraven kommer att uppfyllas och vilken säkerhetsnivå som krävs för behandlingen av personuppgifterna som är föremål för behandlingsavtalet.

Relationen mellan gemensamt personuppgiftsansvariga

Gemensamt personuppgiftsansvariga ska på ett öppet sätt fastställa och kommer överens om sina respektive ansvarsområden för efterlevnad av kraven enligt GDPR. Fastställandet av deras respektive ansvarsområden måste i synnerhet behandla utövandet av de registrerade personernas rättigheter och skyldigheterna att tillhandahålla information. Utöver detta bör fördelningen av ansvarsområden täcka andra skyldigheter för den personuppgiftsansvarige som allmänna dataskyddsprinciper, juridisk grund, säkerhetsåtgärder, skyldighet att avisera vid dataintrång, konsekvensanalys för dataskydd, användning av personuppgiftsbiträden, överföring till tredjeland och kontakter med registrerade personer och tillsynsmyndigheter.

Varje gemensamt personuppgiftsansvarig är skyldig att säkerställa att de har en juridisk grund för behandlingen och att informationen inte vidarebehandlas på ett sätt som är inkompatibelt med

ändamålet för vilket informationen ursprungligen samlades in av den personuppgiftsansvarige som delar informationen.

Den juridiska formen för arrangemanget mellan gemensamt personuppgiftsansvariga specificeras inte av GDPR. För rättssäkerhetens skull och för att garantera insyn och ansvar, rekommenderar EDPB att en sådan överenskommelse görs i form av ett bindande dokument, som ett avtal eller annan juridiskt bindande handling under EU-lagstiftning eller nationell lagstiftning som de personuppgiftsansvariga är underställda.

Arrangemanget ska vederbörligen återspegla respektive roller och relationer för de gemensamt personuppgiftsansvariga gentemot de registrerade personerna och det väsentliga innehållet i arrangemanget ska göras tillgänglig för den registrerade personen.

Oavsett villkoren i arrangemanget kan registrerade personer utöva sina rättigheter i anslutning till och mot vardera av de gemensamt personuppgiftsansvariga. Tillsynsmyndigheterna är inte bundna av villkoren i avtalet vare sig det gäller frågan om kvalificering av parterna som gemensamt personuppgiftsansvariga eller den utsedda kontaktpunkten.

INNEHÅLLSFÖRTECKNING

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e 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 (nedan kallad ”GDPR” eller ”förordningen”),

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

med beaktande av artikel 12 och artikel 22 i arbetsordningen,

med beaktande av att det förberedande arbetet med dessa riktlinjer innefattat insamling av bidrag från intressenter, både skriftliga och vid ett intressentevenemang, för att identifiera de mest brådskande utmaningarna.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

INLEDNING

1. Detta dokument syftar till att ge vägledning om begreppen personuppgiftsansvarig och personuppgiftsbiträde baserat på GDPR:s regler om definitioner i artikel 4 och bestämmelserna om skyldigheter i kapitel IV. Huvudsyftet är att förtydliga begreppens innebörd och tydliggöra de olika rollerna och ansvarsfördelningen mellan dessa aktörer.

2. Begreppet personuppgiftsansvarig och dess samverkan med begreppet personuppgiftsbiträde spelar en viktig roll i tillämpningen av GDPR eftersom de fastställer vem som ska ansvara för efterlevnaden av olika dataskyddsbestämmelser och hur registrerade personer kan utöva sina rättigheter i praktiken. GDPR inför uttryckligen ansvarighetsprincipen, dvs. att den personuppgiftsansvarige ska ansvara för och kunna uppvisa att principerna för behandling av personuppgifter i artikel 5 efterlevs. Dessutom introducerar GDPR även mer specifika regler för användning av personuppgiftsbiträde(n) och vissa av bestämmelserna om behandling av personuppgifter riktas inte bara till personuppgiftsansvariga utan även till personuppgiftsbiträden.

3. Det är därför av yttersta vikt att den exakta innebörden av dessa begrepp och kriterierna för korrekt användning är tillräckligt tydliga och delas inom hela EU och EES.

4. Artikel 29-arbetsgruppen utfärdade vägledning angående begreppen personuppgiftsansvarige/personuppgiftsbiträdet enligt deras yttrande 1/2010 (WP 169)[2] för att tillhandahålla förtydliganden och konkreta exempel angående dessa begrepp. Sedan GDPR trädde i kraft, har många frågor väckts angående i vilken utsträckning GDPR medförde ändringar av begreppen personuppgiftsansvarig och personuppgiftsbiträde och deras respektive roller. Frågor väcktes särskilt om innehållet och konsekvenserna av begreppet gemensamt personuppgiftsansvar (t.ex. enligt

[1] Hänvisningar till ”medlemsstater” som görs i hela detta dokument ska förstås som hänvisningar till ”EES-medlemsstater”.

[2] Artikel 29-arbetsgruppens yttrande 1/2010 angående begreppen ”personuppgiftsansvarig” och ”personuppgiftsbiträde” som antogs den 16 februari 2010, 264/10/EN, WP 169.

artikel 26 i GDPR) och om de särskilda skyldigheterna för personuppgiftsbiträden som fastställs i kapitel IV (t.ex. enligt artikel 28 i GDPR). Därför, och eftersom EDPB inser att den konkreta tillämpningen av begreppen behöver ytterligare förtydliganden, anser EDPB det nu nödvändigt att tillhandahålla mer utvecklad och specifik vägledning för att säkerställa en konsekvent och harmoniserad strategi inom hela EU och EES. De nuvarande riktlinjerna ersätter arbetsgrupp 29:s tidigare yttrande om dessa begrepp (WP 169).

5. I del I av dessa riktlinjer diskuteras definitionerna av de olika begreppen personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och tredje part/mottagare. I del II ges ytterligare vägledning om konsekvenserna som förknippas med de olika rollerna personuppgiftsansvarig, gemensamt personuppgiftsansvarig och personuppgiftsbiträde.

DEL I – BEGREPP

1 ALLMÄNNA OBSERVATIONER

6. I artikel 5.2 i GDPR står det uttryckligen att principen om ansvarsskyldighet innebär att

   - den personuppgiftsansvarige *ansvarar för efterlevnaden* av principerna som beskrivs i artikel 5.1 i GDPR, och att
   - den personuppgiftsansvarige ska kunna *bevisa efterlevnaden* av principerna som beskrivs i artikel 5.1 i GDPR.

   Denna princip har beskrivits i ett yttrande från artikel 29-arbetsgruppen[3] och kommer inte att diskuteras i detalj här.

7. Syftet med att införliva ansvarsskyldighetsprincipen i GDPR och göra den till en central princip var att betona att personuppgiftsansvariga måste införa lämpliga och effektiva åtgärder och kunna bevisa att de efterlever kraven. [4]

8. Ansvarsskyldighetsprincipen har vidareutvecklats i artikel 24, där det står att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och **kunna bevisa** att behandlingen utförs i enlighet med GDPR. Dessa åtgärder ska ses över och uppdateras vid behov. Ansvarsskyldighetsprincipen återspeglas också i artikel 28, som fastställer den personuppgiftsansvariges skyldigheter när man anlitar ett personuppgiftsbiträde.

9. Ansvarsskyldighetsprincipen riktas direkt till den personuppgiftsansvarige. Några av de mer specifika reglerna riktar sig dock till både personuppgiftsansvariga och personuppgiftsbiträden, till exempel reglerna om tillsynsmyndigheters befogenheter i artikel 58. Både personuppgiftsansvariga och personuppgiftsbiträden kan få böter om de skyldigheter enligt GDPR som är relevanta för dem inte efterlevs och båda är direkt ansvariga gentemot tillsynsmyndigheterna vad gäller skyldigheterna att underhålla och tillhandahålla lämplig dokumentation på begäran, samarbeta i händelse av utredning och följa administrativa beslut. Samtidigt bör man komma ihåg att personuppgiftsbiträden alltid måste efterleva och endast följa instruktionerna från den personuppgiftsansvarige.

[3] Artikel 29-arbetsgruppens yttrande 3/2010 angående principen för ansvarsskyldighet som antogs den 13 juli 2010, 00062/10/EN, WP 173.
[4] Skäl 74 i GDPR.

10. Ansvarsskyldighetsprincipen, tillsammans med de övriga, mera specifika reglerna för hur man följer GDPR och ansvarsfördelning, gör det därför nödvändigt att definiera olika roller för flera aktörer som är involverade i en personuppgiftsbehandling.

11. En allmän observation när det gäller begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR är att de inte har förändrats jämfört med direktiv 95/46/EG och att i stort sett förblir kriterierna för hur de olika rollerna ska tillskrivas desamma.

12. Begreppen personuppgiftsansvarig och personuppgiftsbiträde är *funktionella* begrepp: de syftar till att fördela ansvar enligt parternas faktiska roller.[5]Detta innebär att en aktörs rättsliga status som antingen ”personuppgiftsansvarig” eller ”personuppgiftsbiträde” i princip måste fastställas av deras faktiska aktiviteter i en specifik situation, snarare än vid den formella tilldelningen av en aktör som antingen en ”personuppgiftsansvarig” eller ett ”personuppgiftsbiträde” (t.ex. i ett avtal).[6] Detta innebär att rollfördelningen vanligtvis bör härröra från en analys av ärendets faktiska element eller omständigheter och är som sådan inte förhandlingsbar.

13. Begreppen personuppgiftsansvarig och personuppgiftsbiträde är även *autonoma* begrepp i den meningen att även om externa juridiska källor kan hjälpa till att identifiera vem som är personuppgiftsansvarig, bör det i huvudsak tolkas i enlighet med EU:s dataskyddslag. Begreppet personuppgiftsansvarig bör inte påverkas av andra, ibland kolliderande eller överlappande, begrepp inom andra rättsområden, såsom skaparen eller rättighetsinnehavaren när det gäller immateriella rättigheter eller konkurrenslagstiftning.

14. Eftersom det underliggande syftet med att tilldela rollen som personuppgiftsansvarig är att säkerställa ansvarsskyldighet och ett effektivt och omfattande skydd av personuppgifterna, bör begreppet ”personuppgiftsansvarig” tolkas på ett tillräckligt brett sätt, som så mycket som möjligt gynnar ett effektivt och fullständigt skydd av de registrerade personerna[7] för att säkerställa full tillämpning av EU:s dataskyddslagstiftning, för att undvika brister och för att förhindra potentiellt kringgående av reglerna, samtidigt som det inte förminskar personuppgiftsbiträdets roll.

2 DEFINITION AV PERSONUPPGIFTSANSVARIG

2.1 Definition av personuppgiftsansvarig

15. Personuppgiftsansvarig definieras enligt artikel 4.7 i GDPR som

> *”**en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ** som **ensamt eller tillsammans med andra fastställer ändamålen och medlen** för **behandlingen av personuppgifter**; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller*

[5] Artikel 29-gruppens yttrande 1/2010, WP 169, s. 9.

[6] Se även generaladvokaten Mengozzis förslag till avgörande, i *Jehovas vittnen*, C-25/17, ECLI:EU:C:2018:57, punkt 68 (”*I syfte att bestämma registeransvarig i den mening som avses i direktiv 95/46, anser jag [….] att alltför höga formella krav skulle möjliggöra ett kringgående av bestämmelserna i direktiv 95/46 och, att bedömningen [...] bör grundas på en faktabaserad snarare än en formell analys*.”

[7] EU-domstolen, mål C-131/12, Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González, domslut av den 13 maj 2014, punkt 34; EU-domstolen, mål C-210/16, Wirtschaftsakademie Schleswig-Holstein, domslut av den 5 juni 2018, punkt 28; EU-domstolen, mål C-40/17, Fashion ID GmbH & Co.KG mot Verbraucherzentrale NRW eV, domslut av den 29 juli 2019, punkt 66.

medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses ***föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt****"*.

16. Definitionen för personuppgiftsansvarig innehåller fem huvudsakliga byggstenar som kommer att analyseras separat i dessa riktlinjer. De är följande:

- "fysisk eller juridisk person, offentlig myndighet, institution eller annat organ"
- "fastställer"
- "ensamt eller tillsammans med andra"
- "ändamålen och medlen"
- "för behandlingen av personuppgifter".

2.1.1 "Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ"

17. Den första byggstenen behandlar typen av enhet som kan vara personuppgiftsansvarig. Enligt GDPR kan en personuppgiftsansvarig vara "*en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ*". Detta innebär att det i princip inte finns någon begränsning vad gäller vilken typ av enhet som kan ha rollen som personuppgiftsansvarig. Det kan vara en organisation, men kan även vara en individ eller en grupp av individer.[8] I praktiken är det emellertid vanligtvis organisationen som sådan, och inte en individ inom organisationen (som vd:n, en anställd eller en styrelseledamot), som fungerar som personuppgiftsansvarig inom betydelsen för GDPR. När det gäller databehandling inom en företagskoncern måste särskild uppmärksamhet ägnas åt frågan om en anläggning kan fungera som personuppgiftsansvarig eller personuppgiftsbiträde, t.ex. vid behandling av uppgifter för moderbolagets räkning.

18. Ibland utser företag och offentliga organ en specifik person som ansvarar för genomförandet av behandlingsaktiviteten. Även om en specifik fysisk person utses för att säkerställa att dataskyddsreglerna följs kommer denna person inte att vara personuppgiftsansvarig utan agerar för den juridiska personens (företagets eller det offentliga organets) räkning som kommer att vara ytterst ansvarig vid överträdelse av reglerna i egenskap av personuppgiftsansvarig. I samma anda, även om en viss avdelning eller enhet i en organisation har ett operativt ansvar för att säkerställa efterlevnad för viss behandlingsaktivitet, betyder det inte att denna avdelning eller enhet (snarare än organisationen som helhet) blir personuppgiftsansvarig.

Exempel:

Företaget ABC:s marknadsföringsavdelning lanserar en reklamkampanj för att marknadsföra ABC:s produkter. Marknadsföringsavdelningen bestämmer kampanjens natur, metoderna som ska användas (e-post, sociala medier etc.), vilka kunder man ska rikta in sig på och vilka data som ska användas för att göra kampanjen så framgångsrik som möjligt. Även om marknadsföringsavdelningen agerade med stor självständighet, kommer företaget ABC i princip att betraktas som personuppgiftsansvarig eftersom reklamkampanjen lanseras av företaget och äger rum innanför deras affärsverksamhet och i enlighet med deras ändamål.

[8] Till exempel ansåg EU-domstolen i sin dom för *Jehovas vittnen*, C-25/17, ECLI:EU:C:2018:551, punkt 75, att ett religiöst samfund av Jehovas vittnen fungerade som personuppgiftsansvarig, tillsammans med sina enskilda medlemmar. Domslut för *Jehovas vittnen*, C-25/17, ECLI:EU:C:2018:551, punkt 75.

19. I princip kan all behandling av personuppgifter av anställda som sker inom ramen för en organisations verksamhet betraktas som att den sker under den organisationens kontroll.[9] I undantagsfall kan det dock hända att en anställd beslutar att använda personuppgifter för sina egna ändamål och därigenom olagligt överskrider de befogenheter som han eller hon fick (t.ex. för att starta sitt eget företag eller liknande). Det är därför organisationens skyldighet som personuppgiftsansvarig att se till att det finns tillräckliga tekniska och organisatoriska åtgärder, inklusive t.ex. utbildning och information för anställda för att säkerställa att GDPR följs.[10]

2.1.2 ”Fastställer”

20. Den andra byggstenen i begreppet personuppgiftsansvarig avser den personuppgiftsansvariges *inflytande* över behandlingen, i kraft av ett *utövande av beslutanderätt*. En personuppgiftsansvarig är ett organ som *beslutar* vissa nyckelelement i anslutning till behandlingen. Detta personuppgiftsansvar kan definieras av lagstiftning eller kan härledas från en analys av de faktiska elementen eller omständigheterna för respektive fall. Man bör titta på de specifika behandlingsoperationerna i fråga och förstå vem som fastställer dem genom att först beakta följande frågor: *”varför sker denna behandling?”* och *”vem bestämde att behandlingen skulle ske för ett visst ändamål?”*.

Omständigheter som ger upphov till kontroll

21. Eftersom begreppet personuppgiftsansvarig är ett funktionellt begrepp, baseras det därför på en **faktisk, snarare än formell analys**. För att underlätta analysen kan vissa tumregler och praktiska antaganden användas för att styra och förenkla processen. I de flesta situationer kan det ”beslutande organet” identifieras enkelt och tydligt med hänvisning till vissa rättsliga och/eller faktiska omständigheter från vilka ”inflytande” normalt kan härledas, om inte andra element tyder på motsatsen. Två situationskategorier kan särskiljas: (1) kontroll som härrör från *lagbestämmelser*, och (2) kontroll som härrör från *faktiskt inflytande*.

1) *Kontroll som härrör från lagbestämmelser*

22. Det finns fall där kontroll kan utläsas av uttrycklig juridisk kompetens, t.ex. när den personuppgiftsansvarige eller de specifika kriterierna för nominering av denne fastställs av nationell lagstiftning eller unionsrätt. Faktum är att i artikel 4.7 anges det att ”*om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.*” Även om artikel 4.7 endast hänvisar till ”den personuppgiftsansvarige” i singularis, anser EDPB att det även är möjligt för unionslagstiftningen eller medlemslandets lagstiftning att utse mer än en personuppgiftsansvarig, potentiellt även som gemensamt personuppgiftsansvariga.

23. Där den personuppgiftsansvarige har identifierats specifikt av denna lagstiftning, kommer detta att vara fastställande för etablerandet av vem som fungerar som personuppgiftsansvarig. Detta förutsätter att lagstiftaren har utsett den enhet som har en verklig förmåga att utöva kontroll till personuppgiftsansvarig. I vissa länder föreskriver den nationella lagen att offentliga myndigheter är ansvariga för behandling av personuppgifter inom ramen för sina uppgifter.

[9] Anställda som har tillgång till personuppgifter inom en organisation betraktas i allmänhet inte som ”personuppgiftsansvariga” eller ”personuppgiftsbiträden”, utan snarare som ”personer som agerar under den personuppgiftsansvariges eller personuppgiftsbiträdets befogenhet” i den mening som avses i artikel 29 i GDPR.
[10] Artikel 24.1 i GDPR.

24. Men vanligare är att istället för att direkt utse den personuppgiftsansvarige eller fastställa kriterierna för utnämnandet, kommer lagen att fastställa en uppgift eller ålägga någon skyldighet att samla in och behandla vissa uppgifter. I sådana fall fastställs ändamålet med behandlingen ofta av rådande lagstiftning. Den personuppgiftsansvarige kommer normalt att vara den som utses av rådande lagstiftning för utförande av detta syfte, detta offentliga åtagande. Till exempel skulle detta vara fallet där en enhet som har anförtrotts vissa offentliga uppgifter (t.ex. Socialstyrelsen) som inte kan fullgöras utan att samla in åtminstone en del personuppgifter, inrättar en databas eller ett register för att fullgöra dessa offentliga uppgifter. I så fall anger lagen, om än indirekt, vem som är personuppgiftsansvarig. Mer allmänt kan lagen också ålägga antingen offentliga eller privata enheter att behålla eller tillhandahålla vissa uppgifter. Dessa enheter skulle då normalt betraktas som personuppgiftsansvariga med avseende på den behandling som är nödvändig för att fullgöra denna skyldighet.

Exempel: Lagbestämmelser

Den nationella lagstiftningen i landet A fastställer en skyldighet för kommunala myndigheter att tillhandahålla sociala förmåner, som exempelvis månatliga utbetalningar till medborgare beroende på deras ekonomiska situation. För att kunna genomföra dessa utbetalningar måste den kommunala myndigheten samla in och behandla data om de ansökandes ekonomiska situation. Även om lagen inte uttryckligen anger att den kommunala myndigheten är personuppgiftsansvarig för denna behandling, är detta underförstått enligt lagbestämmelserna.

2) *Kontroll som härleds från faktiskt inflytande*

25. I avsaknad av kontroll som följer av lagbestämmelser måste en parts kvalificering som personuppgiftsansvarig fastställas på grundval av en bedömning av de faktiska omständigheterna kring behandlingen. Alla relevanta faktiska omständigheter måste beaktas för att nå en slutsats om huruvida en viss enhet utövar ett avgörande inflytande när det gäller behandlingen av personuppgifterna i fråga.

26. Behovet av sakbedömning innebär också att en personuppgiftsansvarigs roll inte härrör från den databehandlande enhetens natur utan från dess konkreta verksamhet i ett specifikt sammanhang. Med andra ord kan samma enhet fungera som personuppgiftsansvarig för vissa behandlingsoperationer och som personuppgiftsbiträde för andra samtidigt, och kvalifikationen som personuppgiftsansvarig och personuppgiftsbiträde måste bedömas med avseende på varje specifik databehandlingsaktivitet.

27. I praktiken kan vissa behandlingsaktiviteter betraktas som naturligt förknippade med rollen eller aktiviteterna för en enhet som omfattar ansvar ur en dataskyddssynvinkel. Detta kan bero på mer allmänna lagbestämmelser eller en etablerad rättspraxis inom olika områden (civilrätt, handelsrätt, arbetsrätt etc.). I det här fallet kommer befintliga traditionella roller och professionell expertis som normalt innebär ett visst ansvar att hjälpa till att identifiera den personuppgiftsansvarige, till exempel: en arbetsgivare i samband med behandling av personuppgifter om sina anställda, en utgivare som behandlar personuppgifter om sina prenumeranter eller en förening som behandlar personuppgifter om sina medlemmar eller bidragsgivare. När ett företag engagerar sig i behandling av personuppgifter som en del av sin samverkan med sina egna anställda, kunder eller medlemmar, är det i allmänhet detta företag som bestämmer behandlingssyfte och behandlingssätt och fungerar därför som personuppgiftsansvarig i den mening som avses i GDPR.

Exempel: Advokatbyråer

Företaget ABC anlitar en advokatbyrå för att företräda dem i en tvist. För att kunna utföra denna uppgift måste advokatbyrån behandla personuppgifter relaterade till ärendet. Anledningarna till behandlingen av personuppgifterna är advokatbyråns mandat att företräda klienten i domstol. Detta mandat riktar sig dock inte specifikt till behandling av personuppgifter. Advokatbyrån agerar med en betydande grad av oberoende, till exempel för att besluta vilken information som ska användas och hur den ska användas, och det finns inga instruktioner från kundföretaget angående behandlingen av personuppgifter. Behandlingen som advokatbyrån utför för att fullgöra uppgiften som juridiskt ombud för företaget är därför kopplad till advokatbyråns funktionella roll och advokatbyrån bör därför betraktas som personuppgiftsansvarig för denna behandling.

Exempel: Telekomoperatörer[11]:

Att tillhandahålla en elektronisk kommunikationstjänst som exempelvis en elektronisk posttjänst innebär behandling av personuppgifter. Leverantören av sådana tjänster kommer normalt att betraktas som en personuppgiftsansvarig för behandling av personuppgifter som är nödvändiga för driften av tjänsten som sådan (t.ex. trafik- och faktureringsuppgifter). Om leverantörens enda syfte och roll är att möjliggöra överföring av e-postmeddelanden, kommer leverantören inte att betraktas som den personuppgiftsansvarige för personuppgifterna i själva meddelandet. Den personuppgiftsansvarige för alla personuppgifter som finns i meddelandet anses normalt vara den person från vilken meddelandet kommer, snarare än den tjänsteleverantör som erbjuder överföringstjänsten.

28. I många fall kan en bedömning av avtalsvillkoren mellan de olika berörda parterna underlätta fastställandet av vilken eller vilka parter som fungerar som personuppgiftsansvariga. Även om ett avtal inte anger vem som är den personuppgiftsansvarige kan det innehålla tillräcklig information för att göra det möjligt att utläsa vem som utövar en beslutande roll med avseende på behandlingsändamål och behandlingssätt. Det kan även vara fallet att avtalet innehåller ett uttryckligt uttalande om den personuppgiftsansvariges identitet. Om det inte finns någon anledning att tvivla på att detta återspeglar verkligheten på rätt sätt, finns det inget som hindrar att man följer avtalsvillkoren. Avtalsvillkoren är emellertid inte avgörande under alla omständigheter, eftersom detta helt enkelt skulle göra det möjligt för parterna att fördela ansvaret efter eget tycke. Det är inte möjligt att antingen bli personuppgiftsansvarig eller att undkomma skyldigheterna som personuppgiftsansvarig genom att helt enkelt utforma avtalet på ett visst sätt där de faktiska omständigheterna säger något annat.

29. Om en part faktiskt bestämmer varför och hur personuppgifter behandlas kommer den parten att vara personuppgiftsansvarig även om ett avtal säger att de är ett personuppgiftsbiträde. På samma sätt är det inte för att ett kommersiellt avtal använder termen ”underleverantör” som en enhet ska betraktas som ett personuppgiftsbiträde ur dataskyddslagens perspektiv.[12]

30. I linje med det faktiska tillvägagångssättet betyder ordet ”bestämmer” att den enhet som faktiskt utövar ett avgörande inflytande på behandlingsändamålet och behandlingssättet är den personuppgiftsansvarige. Normalt fastslår ett processoravtal vem som är den bestämmande parten (personuppgiftsansvarig) och den instruerade parten (personuppgiftsbiträde). Även om

[11] EDPB anser att detta exempel, som tidigare ingick i skäl 47 i direktiv 95/46/EG, fortfarande är relevant även enligt GDPR.

[12] Se t.ex. artikel 29-gruppens yttrande 10/2006 angående behandling av personuppgifter av Society for Worldwide Interbank Financial Telecommunication (SWIFT) av den 22 november 2006, WP 128, s. 11.

personuppgiftsbiträdet erbjuder en tjänst som är preliminärt definierad på ett specifikt sätt måste den personuppgiftsansvarige förses med en detaljerad beskrivning av tjänsten och måste fatta det slutliga beslutet att aktivt godkänna hur behandlingen utförs och begära ändringar om det behövs. Vidare kan personuppgiftsbiträdet inte ändra de väsentliga delarna i behandlingen i ett senare skede utan den personuppgiftsansvariges godkännande.

Exempel: standardiserad molnlagringstjänst

En stor molnlagringsleverantör erbjuder sina kunder möjligheten att lagra stora personuppgiftsvolymer. Tjänsten är fullständigt standardiserad och kunderna har liten eller ingen förmåga att anpassa tjänsten personligt. Avtalsvillkoren bestäms och utarbetas ensidigt av molntjänstleverantören, och tillhandahålls kunden enligt devisen ”passar det inte, så låt bli”. Företaget X beslutar sig för att använda molnleverantören för att lagra personuppgifter för sina kunder. Företaget X kommer fortfarande att betraktas som personuppgiftsansvarig, på grund av beslutet att använda denna särskilda molntjänstleverantör för behandling av personuppgifter för sin räkning. I den mån molntjänstleverantören inte behandlar personuppgifterna för egna ändamål och lagrar uppgifterna enbart för sina kunders räkning och i enlighet med instruktionerna kommer tjänsteleverantören att betraktas som personuppgiftsbiträde.

2.1.3 ”Ensamt eller tillsammans med andra”

31. I artikel 4.7 fastställs att ”ändamål och medel” för behandlingen kan bestämmas av mer än en aktör. Här förklaras att den personuppgiftsansvarige är den aktör som ”ensam eller tillsammans med andra” bestämmer behandlingsändamål och behandlingssätt. Detta innebär att flera olika enheter kan fungera som personuppgiftsansvariga för samma behandling, där var och en av dem då är underställda gällande dataskyddsbestämmelser. På motsvarande sätt kan en organisation fortfarande vara personuppgiftsansvarig även om den inte fattar alla beslut angående behandlingsändamål och behandlingssätt. Kriterierna för gemensamt personuppgiftsansvar och i vilken utsträckning två eller flera aktörer gemensamt utövar kontroll kan anta olika former, vilket klargörs senare.[13]

2.1.4 ”Behandlingsändamål och behandlingssätt”

32. Den fjärde byggstenen för definitionen av personuppgiftsansvarig hänvisar till ändamålet med den personuppgiftsansvariges inflytande, nämligen ”ändamål och medel” för behandlingen. Den representerar substantivdelen för konceptet personuppgiftsansvarig: vad en part bör bestämma för att kvalificera sig som personuppgiftsansvarig.

33. Ordböcker definierar ”ändamål” som ”ett förväntat resultat som är avsett eller som styr dina planerade handlingar” och ”medel” som ”hur ett resultat eller ett mål uppnås”.

34. GDPR fastställer att data måste samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte vidarebehandlas på ett sätt som är oförenligt med dessa ändamål. Det är därför särskilt viktigt att bestämma ”ändamålen” för behandlingen och ”medlen” för att uppnå dem.

35. Att bestämma ändamålen och medlen innebär att man bestämmer ”varför” respektive ”hur” behandlingen sker:[14] för en särskild behandlingsoperation är det den personuppgiftsansvarige aktören som har bestämt *varför* behandlingen sker (dvs. ”i vilket syfte” eller ”varför”) och *hur* detta mål ska uppnås (dvs. vilka medel som ska användas för att uppnå målet). En fysisk eller juridisk person som

[13] Se del I, avsnitt 3 (”Definition av gemensamt personuppgiftsansvariga”).
[14] Se även generaladvokat Bots åsikt i *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, punkt 46.

utövar ett sådant inflytande över behandlingen av personuppgifter deltar därmed i fastställandet av ändamålen och medlen för behandlingen i enlighet med definitionen i artikel 4.7 i GDPR.[15]

36. Den personuppgiftsansvarige måste bestämma både behandlingsändamål och behandlingssätt enligt vad som beskrivs nedan. Därmed kan den personuppgiftsansvarige inte nöja sig med att enbart fastställa ändamålet. Man måste även ta beslut angående behandlingssätt. Omvänt kan den part som agerar som personuppgiftsbiträde aldrig bestämma ändamålet med behandlingen.

37. Om en personuppgiftsansvarig anlitar ett personuppgiftsbiträde för att utföra behandlingen för sin räkning, innebär det ofta i praktiken att personuppgiftsbiträdet ska kunna ta vissa beslut på egen hand angående hur behandlingen bör genomföras. EDPB instämmer i att viss handlingsmarginal kan tillåtas för att personuppgiftsbiträdet också ska kunna fatta vissa beslut i anslutning till behandlingen. Ur detta perspektiv finns det ett behov av att ge vägledning om vilken **grad av inflytande** i anslutning till ”varför” och ”hur” ska innebära att en enhet kvalificerar sig som personuppgiftsansvarig och i vilken utsträckning ett personuppgiftsbiträde kan fatta egna beslut.

38. När en enhet tydligt bestämmer ändamål och medel och anlitar en annan enhet för att utföra behandlingsaktiviteterna i enlighet med deras detaljerade instruktioner, är situationen okomplicerad och det råder ingen tvekan om att den andra enheten ska betraktas som ett personuppgiftsbiträde, medan den första enheten är personuppgiftsansvarig.

Väsentliga kontra icke-väsentliga medel

39. Frågan är var man ska dra linjen mellan beslut som är reserverade för den personuppgiftsansvarige och beslut som kan lämnas till personuppgiftsbiträdets gottfinnande. Beslutet angående ändamålet med behandlingen åligger utan tvekan alltid den personuppgiftsansvarige.

40. När det gäller fastställandet av medel, kan väsentliga och icke-väsentliga medel hållas isär. ”Väsentliga medel” är traditionellt och i sig förbehållna den personuppgiftsansvarige. Även om icke-väsentliga medel även kan fastställas av personuppgiftsbiträdet, måste väsentliga medel fastställas av den personuppgiftsansvarige. ”Väsentliga medel” är medel som är nära kopplade till behandlingens ändamål och omfattning, till exempel vilken typ av personuppgifter som behandlas (”*vilka uppgifter ska behandlas?*”), behandlingens varaktighet (”*hur länge ska de behandlas?*”), mottagarkategorierna (”*vem ska ha åtkomst till dem?*”) och kategorierna av registrerade personer (”*vars personuppgifter behandlas?*”). Tillsammans med ändamålet med behandlingen är de väsentliga medlen också nära kopplade till frågan om huruvida behandlingen är laglig, nödvändig och proportionell. ”Icke-väsentliga medel” gäller mer praktiska aspekter av implementeringen, till exempel valet av en viss typ av maskin- eller programvara eller de detaljerade säkerhetsåtgärder som kan överlåtas till personuppgiftsbiträdet att besluta om.

Exempel: Löneadministration

Arbetsgivaren A anlitar ett annat företag för att hantera löneutbetalningarna till sina anställda. Arbetsgivare A ger tydliga instruktioner om vem som ska betalas, vilka belopp, vid vilket datum, av vilken bank, hur länge uppgifterna ska lagras, vilka uppgifter som ska lämnas ut till skattemyndigheten etc. I detta fall sker behandlingen av uppgifter i enlighet med företag A:s syfte att betala löner till sina anställda och löneadministratören får inte använda uppgifterna för något eget syfte. Det sätt på vilket löneadministratören ska utföra behandlingen är i huvudsak klart och tydligt definierat. Trots detta kan löneadministratören besluta om vissa detaljerade frågor kring behandlingen, till exempel vilken programvara som ska användas, hur man distribuerar åtkomst inom sin egen organisation etc. Detta

[15] Domslut för *Jehovas vittnen*, C-25/17, ECLI:EU:C:2018:551, punkt 68.

ändrar inte rollen som personuppgiftsbiträde så länge som administratören inte går emot eller bortom instruktionerna från företag A.

Exempel: Bankbetalningar

Som en del av instruktionerna från arbetsgivare A överför löneadministrationen information till bank B så att de kan utföra den faktiska betalningen till anställda hos arbetsgivare A. Denna aktivitet inkluderar behandling av personuppgifter av bank B som den utför för ändamålet att utföra bankverksamhet. Inom denna verksamhet beslutar banken oberoende av arbetsgivare A om vilka uppgifter som måste behandlas för att tillhandahålla tjänsten, hur länge uppgifterna måste lagras etc. Arbetsgivare A kan inte ha något inflytande över ändamålet och medlen som bank B använder för databehandlingen. Bank B ska därför betraktas som en personuppgiftsansvarig för denna behandling och överföringen av personuppgifter från löneadministrationen är att betrakta som ett utlämnande av information mellan två personuppgiftsbiträden, från arbetsgivare A till bank B.

Exempel: Revisorer

Arbetsgivare A anlitar också redovisningsföretag C för att utföra revisioner av deras bokföring och överför därför uppgifter om finansiella transaktioner (inklusive personuppgifter) till C. Bokföringsföretag C behandlar dessa uppgifter utan detaljerade instruktioner från A. Redovisningsföretag C beslutar själv, i enlighet med lagbestämmelserna som reglerar revisionsverksamheten som utförs av C, att uppgifterna som de samlar in endast kommer att behandlas i syfte att revidera A och de fastställer vilka uppgifter de behöver, vilka kategorier av personer som behöver registreras, hur länge uppgifterna ska lagras och vilka tekniska medel som ska användas. Under dessa omständigheter är redovisningsföretaget C att betrakta som en egen personuppgiftsansvarig vid utförandet av sina revisionstjänster för A. Men denna bedömning kan vara annorlunda beroende på instruktionsnivån från A. I en situation där lagen inte fastställer specifika skyldigheter för redovisningsföretaget och kundföretaget ger mycket detaljerade instruktioner om behandlingen, skulle bokföringsföretaget dock fungera som ett personuppgiftsbiträde. En åtskillnad skulle kunna göras mellan en situation där behandlingen, i enlighet med lagarna som reglerar detta yrke, utförs som en del av redovisningsbyråns kärnverksamhet och där behandlingen är en mera begränsad, kompletterande uppgift som utförs som en del av kundföretagets verksamhet.

Exempel: Hostingtjänster

Arbetsgivaren A anlitar hostingtjänsten H för att lagra krypterade data på H:s servrar. Hostingtjänsten H fastställer inte huruvida informationen man är host för är personuppgifter och man behandlar inte heller data på något annat sätt än att lagra den på sina servrar. Eftersom lagring är ett exempel på en behandlingsaktivitet för personuppgifter, behandlar hostingtjänsten H personuppgifter för arbetsgivaren A:s räkning, och är därmed ett personuppgiftsbiträde. Arbetsgivaren A måste ge H nödvändiga instruktioner och ett databehandlingsavtal i enlighet med artikel 28 måste ingås, som kräver att H implementerar tekniska och organisatoriska säkerhetsåtgärder. H måste assistera A när det gäller att säkerställa att nödvändiga säkerhetsåtgärder vidtas och avisera i händelse av eventuella dataintrång.

41. Även om beslut om icke-väsentliga medel kan överlåtas till personuppgiftsbiträdet, måste den personuppgiftsansvarige fortfarande ange vissa delar i behandlingsavtalet, till exempel i förhållande till säkerhetskravet, t.ex. en instruktion om att vidta alla åtgärder som krävs enligt artikel 32 i GDPR.

Avtalet måste också ange att personuppgiftsbiträdet ska assistera den personuppgiftsansvarige när det gäller efterlevnad av exempelvis artikel 32. Under alla omständigheter förblir den personuppgiftsansvarige ansvarig för genomförandet av lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen (artikel 24). Därvid måste den personuppgiftsansvarige ta hänsyn till behandlingens art, omfattning, sammanhang och ändamål såväl som riskerna för fysiska personers rättigheter och friheter. Av denna anledning måste den personuppgiftsansvarige vara välinformerad om behandlingssätten som används så att man kan ta ett välgrundat beslut i anslutning till detta. För att den personuppgiftsansvarige ska kunna påvisa lagligheten i behandlingen är det lämpligt att dokumentera minst de nödvändiga tekniska och organisatoriska åtgärderna i avtalet eller andra juridiskt bindande instrument mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

Exempel: Callcenter

Företaget X beslutar sig för att lägga ut en del av sin kundtjänst på entreprenad till ett callcenter. Callcentret tar emot identifierbara uppgifter om kundköp, såväl som kontaktuppgifter. Callcentret använder sin egen programvara och it-infrastruktur för att hantera personuppgifterna som berör företag X kunder. Företag X tecknar ett behandlingsavtal med leverantören av callcentret i enlighet med artikel 28 i GDPR, efter att ha fastställt att de tekniska och organisatoriska säkerhetsåtgärder som föreslås av callcentret är lämpliga för de berörda riskerna och att callcentret endast kommer att behandla personuppgifterna för företagets ändamål och i enlighet med dess instruktioner. Företag X ger inga ytterligare instruktioner till callcentret angående specifik programvara som ska användas eller detaljerade instruktioner om de specifika säkerhetsåtgärder som ska genomföras. I detta exempel förblir företag X personuppgiftsansvarig, trots att callcentret har bestämt vissa icke-väsentliga behandlingsmetoder.

2.1.5 ”Avseende behandling av personuppgifter”

42. Ändamålen och medlen som fastställs av den personuppgiftsansvarige måste relatera till ”behandlingen av personuppgifter”. I artikel 4.2 i GDPR definieras behandling av personuppgifter som ”*varje operation eller uppsättning operationer som utförs på personuppgifter eller på uppsättningar av personuppgifter*”. Som ett resultat kan begreppet personuppgiftsansvarig länkas till antingen en enskild behandlingsoperation eller flera operationer. I praktiken kan detta innebära att kontrollen som utövas av en viss enhet kan sträcka sig till hela den aktuella behandlingen men också kan vara begränsad till ett visst steg i behandlingen.[16]

43. I praktiken kan behandlingen av personuppgifter som involverar flera aktörer delas in i flera mindre behandlingsoperationer för vilka varje aktör kan övervägas för att bestämma ändamålet och medlen individuellt. Å andra sidan kan en sekvens eller uppsättning behandlingsoperationer som involverar flera aktörer också ske för samma eller flera ändamål, i vilket fall det är möjligt att behandlingen involverar en eller flera gemensamt personuppgiftsansvariga. Med andra ord är det möjligt att på ”mikronivå” verkar de olika behandlingsoperationerna i kedjan vara åtskilda från varandra, eftersom var och en av dem kan ha olika ändamål. Det är dock nödvändigt att dubbelkontrollera om dessa

[16] Domslut i *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, punkt 74: ”*Härav följer, såsom generaladvokaten angett, [...] att en fysisk eller juridisk person endast betraktas som ansvarig, i den mening som avses i artikel 2 d i direktiv 95/46, tillsammans med andra, för de behandlingar av personuppgifter för vilken den tillsammans bestämt medlen och ändamålen för. Däremot [...] kan denna fysiska eller juridiska person inte anses vara ansvarig i den mening som avses i denna bestämmelse för de tidigare eller senare åtgärderna i den övergripande behandlingskedjan, som denna varken fastställer ändamålen eller medlen för.*”

behandlingar på ”makronivå” inte ska betraktas som en ”uppsättning operationer” som strävar efter ett gemensamt syfte med gemensamt definierade medel.

44. Den som bestämmer sig för att behandla data måste överväga om detta inkluderar personuppgifter och, om så är fallet, vilka skyldigheter som gäller enligt GDPR. En aktör kommer att betraktas som en ”personuppgiftsansvarig” även om man inte medvetet riktar in sig på personuppgifter som sådana eller har felbedömt att man inte behandlar personuppgifter.

45. Det är inte nödvändigt att den personuppgiftsansvarige har faktisk åtkomst till uppgifterna som behandlas.[17] Någon som lägger ut en behandling på entreprenad och därigenom har ett avgörande inflytande på ändamålet och (väsentliga) medel för behandlingen (t.ex. genom att justera parametrar för en tjänst på ett sådant sätt att den påverkar vems personuppgifter som ska behandlas), är att betrakta som personuppgiftsansvarig även om han eller hon aldrig kommer att ha faktisk tillgång till uppgifterna.

Exempel: Marknadsundersökning 1

Företaget ABC vill ta reda på vilka typer av konsumenter som mest sannolikt är intresserade av deras produkter och anlitar tjänsteleverantören XYZ för att inhämta relevant information.

Företaget ABC förklarar för XYZ vilken typ av information man är intresserad av och tillhandahåller en lista med frågor som ska ställas till dem som deltar i marknadsundersökningen.

Företaget ABC tar endast emot statistisk information (t.ex. identifiering av konsumenttrender per region) från XYZ och har inte tillgång till själva personuppgifterna. Dock beslutade företaget ABC att behandlingen skulle äga rum, behandlingen utförs för deras ändamål och deras verksamhet och man har försett XYZ med detaljerade instruktioner om vilken information som ska samlas in. Företaget ABC bör därför fortfarande betraktas som personuppgiftsansvarig när det gäller behandlingen av personuppgifterna som genomförs för att tillhandahålla informationen man har begärt. XYZ får endast behandla informationen i det syfte som företag ABC har angett och i enlighet med deras detaljerade instruktioner och är därmed att betrakta som ett personuppgiftsbiträde.

Exempel: Marknadsundersökning 2

Företaget ABC vill ta reda på vilken typ av konsumenter som mest sannolikt är intresserade av deras produkter. Tjänsteleverantören XYZ är ett marknadsundersökningsföretag som har samlat in information om konsumentintressen genom en mängd olika som rör en mängd olika produkter och tjänster. Tjänsteleverantören XYZ har samlat in och analyserat dessa data självständigt och enligt sin egen metod utan att ha tagit emot några instruktioner från företaget ABC. För att hantera företaget ABC:s begäran kommer tjänsteleverantören XYZ att generera statistisk information, men gör detta utan att ta emot några ytterligare instruktioner om vilka personuppgifter som ska behandlas eller hur de ska behandlas för att generera denna statistik. I det här exemplet fungerar tjänsteleverantören XYZ som den enda personuppgiftsansvarige, som behandlar personuppgifter i marknadsundersökningssyfte och bestämmer självständigt sätten för att göra det. Företaget ABC har ingen särskild roll eller något ansvar enligt dataskyddslagstiftningen i samband med dessa behandlingar, eftersom företaget ABC tar emot anonymiserad statistik och inte är inblandat i att fastställa ändamålen och medlen för behandlingen.

[17] Domslut i *Wirtschaftsakademie*, C-201/16, ECLI:EU:C:2018:388, punkt 38.

3 DEFINITION AV GEMENSAMT PERSONUPPGIFTSANSVARIGA

3.1 Definition av gemensamt personuppgiftsansvariga

46. Kvalificeringen som gemensamt personuppgiftsansvariga kan uppstå när mer än en aktör är involverad i behandlingen.

47. Även om begreppet inte är nytt och redan finns enligt direktiv 95/46/EG, inför GDPR i artikel 26 särskilda regler för gemensamt personuppgiftsansvariga och sätter upp ett ramverk för att styra deras förhållande. Dessutom har EU-domstolen i de senaste domarna lagt fram förtydliganden om detta begrepp och dess konsekvenser.[18]

48. Som närmare beskrivs i del II, avsnitt 2, kommer kvalificeringen av gemensamt personuppgiftsansvariga huvudsakligen att få konsekvenser när det gäller fördelning av skyldigheter för efterlevnad av dataskyddsregler och i synnerhet med avseende på individers rättigheter.

49. I detta perspektiv syftar följande avsnitt till att ge vägledning om begreppet gemensamt personuppgiftsansvariga i enlighet med GDPR och EU-domstolens rättspraxis för att hjälpa enheter att avgöra var de kan fungera som gemensamt personuppgiftsansvariga och tillämpa begreppet i praktiken.

3.2 Förekomst av gemensamt personuppgiftsansvar

3.2.1 Allmänna överväganden

50. Definitionen av en personuppgiftsansvarig i artikel 4.7 i GDPR utgör utgångspunkten för att fastställa gemensam kontroll. Övervägandena i detta avsnitt är således direkt relaterade till och kompletterar övervägandena i avsnittet om begreppet personuppgiftsansvarig. Som en konsekvens bör utvärderingen av gemensam kontroll spegla bedömningen av ”enskild” kontroll som utvecklats ovan.

51. Artikel 26 i GDPR, som återspeglar definitionen i artikel 4.7 i GDPR, föreskriver att *”Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga.”* I stora drag existerar gemensam kontroll när det gäller en specifik behandling när olika parter *gemensamt* fastställer ändamålet och medlen för denna behandling. Därför kräver bedömningen av förekomsten av gemensamt personuppgiftsansvariga att man undersöker om bestämmande av ändamål och medel som kännetecknar en personuppgiftsansvarig beslutas av mer än en part. ”Gemensamt” måste tolkas i betydelsen ”tillsammans med” eller ”inte ensam”, i olika former och kombinationer, enligt vad som förklaras nedan.

52. Bedömningen av den gemensamma kontrollen bör utföras utifrån en saklig, snarare än en formell, analys av det faktiska inflytandet över ändamålen och medlen för behandlingen. Alla befintliga eller planerade arrangemang bör kontrolleras mot de faktiska omständigheterna kring förhållandet mellan

[18] Se i synnerhet *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein mot Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu mot Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG mot Verbraucherzentrale NRW eV (*C-40/17). Det bör noteras att även om dessa domar utfärdades av EU-domstolen angående tolkningen av begreppet gemensamt personuppgiftsansvariga enligt direktiv 95/46/CE, förblir de giltiga i samband med GDPR, med tanke på att de element som bestämmer detta begrepp enligt GDPR förblir samma som enligt direktivet.

parterna. Ett rent formellt kriterium skulle inte vara tillräckligt av minst två skäl: i vissa fall skulle den formella utnämningen av en gemensam personuppgiftsansvarig, som till exempel anges i lag eller i ett avtal, saknas; i andra fall kan det vara så att den formella utnämningen inte återspeglar arrangemangets verklighet, genom att formellt överlåta rollen som personuppgiftsansvarig till en enhet som i själva verket inte har möjlighet att ”fastställa” ändamålet och medlen för behandlingen.

53. All behandling där flera enheter är inblandade innebär inte alltid gemensam kontroll. Det övergripande kriteriet för att gemensamt personuppgiftsansvar ska föreligga är **gemensamt deltagande av två eller flera enheter i fastställandet av behandlingsändamål och behandlingssätt**. Det gemensamma deltagandet måste mera specifikt inkludera fastställandet av behandlingsändamålet å ena sidan och fastställandet av behandlingssättet å andra sidan. Om vart och ett av dessa element bestäms av alla berörda enheter bör de betraktas som gemensamt personuppgiftsansvariga för den aktuella behandlingen.

3.2.2 Bedömning av gemensamt deltagande

54. Gemensamt deltagande i fastställandet av ändamål och medel innebär att mer än en enhet har ett avgörande inflytande över huruvida och hur behandlingen sker. I praktiken kan gemensamt deltagande ske på flera olika sätt. Till exempel kan gemensamt deltagande anta formen av ett **gemensamt beslut** som fattas av två eller flera enheter eller härrör från **konvergerande beslut** från två eller flera enheter angående ändamål och väsentliga medel.

55. Gemensamt deltagande via ett *gemensamt beslut* innebär att besluta tillsammans och innebär en gemensam avsikt i enlighet med den vanligaste förståelsen av termen ”gemensamt” som avses i artikel 26 i GDPR.

Situationen för gemensamt deltagande genom *konvergerande beslut* beror framför allt på EU-domstolens rättspraxis om begreppet gemensamt personansvariga. Beslut kan betraktas som konvergerande angående ändamål och medel **om de kompletterar varandra och är nödvändiga för att behandlingen ska ske på ett sådant sätt att de har en påtaglig inverkan på fastställandet av ändamålen och medlen för behandlingen**. Det bör framhållas att begreppet konvergerande beslut måste beaktas i förhållande till ändamålen och medlen för behandlingen men inte andra aspekter av det kommersiella förhållandet mellan parterna.[19] Ett viktigt kriterium för att identifiera konvergerande beslut i detta sammanhang är **huruvida behandlingen inte skulle vara möjlig utan båda parters deltagande i ändamålen och medlen i den meningen att varje parts behandling är oskiljbar, det vill säga oupplösligt länkad**. Situationen för gemensamt personuppgiftsansvariga som agerar på grundval av konvergerande beslut bör dock särskiljas från fallet med ett personuppgiftsbiträde, eftersom den senare, även om denna deltar i utförandet av en behandling, inte behandlar uppgifterna för egna ändamål utan utför behandlingen för den personuppgiftsansvariges räkning.

56. Att en av parterna inte har tillgång till personuppgifter som behandlas är inte tillräckligt för att utesluta gemensam kontroll.[20] Till exempel, i *Jehovas vittnen*, ansåg EU-domstolen att ett religiöst samfund måste betraktas som en personuppgiftsansvarig, tillsammans med sina medlemmar som engagerar sig i att predika, av behandlingen av personuppgifter som utförs av de senare i samband med predikande från dörr till dörr.[21] EU-domstolen ansåg att det inte var nödvändigt att gemenskapen hade tillgång till de aktuella uppgifterna eller att fastställa att samfundet hade gett sina medlemmar skriftliga riktlinjer

[19] Alla kommersiella arrangemang innebär konvergerande beslut som en del av processen genom vilken en överenskommelse träffas.
[20] Domslut i *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punkt 38.
[21] Domslut i *Jehovah’s witnesses*, C-25/17, ECLI:EU:C:2018:551, punkt 75.

eller instruktioner i samband med databehandlingen.[22] Samfundet deltog i fastställandet av ändamål och medel genom att organisera och samordna sina medlemmars aktiviteter, vilket bidrog till att uppnå de frikyrkliga målsättningarna för Jehovas Vittnen.[23] Dessutom var samfundet generellt medvetet om att sådan behandling utfördes för att sprida sitt budskap.[24]

57. Det är också viktigt att understryka, som klargjorts av EU-domstolen, att ett företag endast kommer att betraktas som gemensamt personuppgiftsansvarigt med de andra för de verksamheter för vilka det bestämmer medel och ändamål för samma databehandling tillsammans med de andra, i synnerhet vid konvergerande beslut. Om en av dessa enheter ensam beslutar vilka ändamål och medel att använda i verksamheten som föregår eller efterföljs i behandlingskedjan, måste denna enhet betraktas som den enda personuppgiftsansvarige av denna föregående eller efterföljande verksamhet.[25]

58. Förekomsten av gemensamt ansvar innebär inte nödvändigtvis lika ansvar för de olika operatörer som är involverade i behandlingen av personuppgifter. Tvärtom har EU-domstolen förtydligat att dessa operatörer kan vara inblandade i olika skeden av behandlingen och i olika grad så att ansvaret för var och en av dem måste bedömas med hänsyn till alla relevanta omständigheter i det särskilda fallet.

3.2.2.1 Gemensamt fastställande av ändamål

59. Gemensam kontroll föreligger när enheter som är involverade i samma behandling utför behandlingen för gemensamt definierade ändamål. Detta kommer att vara fallet om de berörda enheterna behandlar uppgifterna för samma eller gemensamma ändamål.

60. När enheterna inte har samma ändamål med behandlingen kan dessutom gemensamt personuppgiftsansvar, mot bakgrund av EU-domstolens rättspraxis, ha inrättats när de berörda enheterna eftersträvar ändamål som är nära sammankopplade eller kompletterande. Så kan exempelvis vara fallet när det uppstår en ömsesidig nytta av samma behandling, förutsatt att var och en av de inblandade enheterna deltar i fastställandet av ändamål och medel för den relevanta behandlingen. Men begreppet ömsesidig nytta är inte avgörande och kan bara vara en indikation. I *Fashion ID*, till exempel, klargjorde EU-domstolen att en webbplatsoperatör deltar i fastställandet av ändamål (och medel) för behandlingen genom att bädda in ett socialt tilläggsprogram på en webbplats för att optimera marknadsföringen av sina varor genom att göra dem mer synliga på det sociala nätverket. EU-domstolen ansåg att de aktuella behandlingarna utfördes med ekonomiskt intresse för både webbplatsoperatören och leverantören av det sociala tilläggsprogrammet.[26]

61. På samma sätt, som nämnts av EU-domstolen i *Wirtschaftsakademie*, har behandlingen av personuppgifter genom statistik över besökare på en fan-sida för avsikt att göra det möjligt för Facebook att förbättra sitt reklamsystem som överförs via deras nätverk och att göra det möjligt för administratören för fan-sidan att få statistik för att hantera marknadsföringen av sin verksamhet.[27] I detta fall agerar varje enhet i sitt eget intresse men båda parterna deltar i fastställandet av ändamålen (och medlen) för behandling av personuppgifter när det gäller besökarna på fan-sidan.[28]

---

[22] Ibid.
[23] Ibid, punkt 71.
[24] Ibid.
[25] Domslut i *Fashion ID*, C-40/17, ECLI:EU:2018:1039, punkt 74 *"Däremot, och utan att det påverkar eventuellt civilrättsligt ansvar enligt nationell lagstiftning i detta avseende, kan denna fysiska eller juridiska person inte anses vara ansvarig i den mening som avses i denna bestämmelse för de tidigare eller senare åtgärderna i den övergripande behandlingskedjan, som denna varken fastställer ändamålen eller medlen för."*.
[26] Domslut i *Fashion ID,* C-40/17, ECLI:EU:2018:1039, punkt 80.
[27] Domslut i *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punkt 34.
[28] Domslut i *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punkt 39.

62. I detta avseende är det viktigt att lyfta fram att enbart en ömsesidig nytta (till exempel kommersiell) som uppstår från en behandling, inte ger upphov till gemensamt personuppgiftsansvar. Om enheten som är inblandad i behandlingen inte har något eget syfte i förhållande till behandlingen, utan bara betalas för tillhandahållna tjänster, fungerar den som ett personuppgiftsbiträde snarare än som en gemensam personuppgiftsansvarig.

3.2.2.2 Gemensamt fastställda medel

63. Gemensamt personuppgiftsansvar kräver även att två eller flera enheter har haft inflytande över behandlingssätten. Detta innebär inte att varje involverad enhet alltid måste besluta alla behandlingssätt för att gemensamt personuppgiftsansvar ska föreligga. Som klargörs av EU-domstolen kan olika enheter vara involverade i olika skeden av behandlingen och i olika grad. Olika gemensamt personuppgiftsansvariga kan därför definiera behandlingsmedlen i olika omfattning, beroende på vem som effektivt kan göra detta.

64. Det kan också vara så att en av de inblandade enheterna tillhandahåller medlen för behandlingen och gör dem tillgängliga för behandling av personuppgifter av andra enheter. Enheten som beslutar att använda dessa medel så att personuppgifter kan behandlas för ett visst ändamål deltar också i fastställandet av behandlingsmedlen.

65. Detta scenario kan särskilt uppstå om plattformar, standardiserade verktyg eller annan infrastruktur gör det möjligt för parterna att behandla samma personuppgifter och som har konfigurerats på ett visst sätt av en av parterna för att kunna användas av andra som också kan bestämma hur det ska konfigureras.[29] Användningen av ett redan befintligt tekniskt system utesluter inte gemensamt personuppgiftsansvar när användare av systemet kan besluta om behandling av personuppgifter som ska utföras i detta sammanhang.

66. Som ett exempel på detta ansåg EU-domstolen i fallet *Wirtschaftsakademie* att administratören för en fan-sida (som hostas på Facebook) genom att definiera parametrar baserat på dess målgrupp och med målsättningen att hantera och marknadsföra dess verksamhet, måste anses ha deltagit i beslutet om medel för behandling av personuppgifter relaterade till besökarna på denna fan-sida.

67. Vidare kommer det val som görs av ett företag att använda ett verktyg eller annat system som utvecklats av en annan enhet för sina egna ändamål sannolikt att utgöra ett gemensamt beslut om hur dessa enheter ska behandlas. Detta följer av Fashion ID-fallet där EU-domstolen drog slutsatsen att genom att bädda in Facebooks gilla-knapp på sin webbsida, som Facebook gör tillgänglig för webbplatsoperatörer, har Fashion ID utövat ett avgörande inflytande när det gäller operationer som involverar insamling och överföring av personuppgifter om besökarna på sin webbplats till Facebook och hade därmed gemensamt bestämt med Facebook hur denna behandling skulle utföras.[30]

68. Det är viktigt att understryka att **användningen av ett gemensamt databehandlingssystem eller en infrastruktur kommer inte alltid att leda till att de berörda parterna kvalificeras som gemensamt personuppgiftsansvariga**, särskilt när behandlingen de utför går att hålla isär och kan utföras av en part utan ingripande från den andra eller om leverantören är ett personuppgiftsbiträde som inte har något eget ändamål (förekomsten av enbart kommersiell vinning för de inblandade parterna är inte tillräckligt för att kvalificera sig som ett behandlingsändamål).

[29] Systemleverantören kan vara en gemensamt personuppgiftsansvarig om kriterierna ovan uppfylls, det vill säga om leverantören deltar i fastställandet av ändamål och medel. Annars bör leverantören betraktas som ett personuppgiftsbiträde.

[30] Domslut i Fashion ID, C-40/17, ECLI:EU:2018:1039, punkterna 77–79.

Exempel: Resebyrå

En resebyrå skickar personuppgifter om sina kunder till flygbolaget och en hotellkedja med avsikt att göra bokningar för ett resepaket. Flygbolaget och hotellet bekräftar tillgängligheten för flygstolarna och rummen som önskas. Resebyrån utfärdar resehandlingar och kvitton åt sina kunder. Var och en av aktörerna behandlar uppgifterna för att utföra sina egna aktiviteter och använder sina egna medel. I det här fallet är resebyrån, flygbolaget och hotellet tre olika personuppgiftsansvariga som behandlar uppgifterna för sina egna och separata ändamål och det finns inget gemensamt personuppgiftsansvar.

Resebyrån, hotellkedjan och flygbolaget beslutar sedan att tillsammans skapa en internetbaserad plattform för det gemensamma ändamålet att erbjuda paketresor. De är överens om de väsentliga medlen som ska användas, till exempel vilka data som ska lagras, hur reservationer kommer att fördelas och bekräftas, och vem som kan få tillgång till den lagrade informationen. Dessutom bestämmer de sig för att dela uppgifter om sina kunder för att genomföra gemensamma marknadsföringskampanjer. I det här fallet bestämmer resebyrån, flygbolaget och hotellkedjan gemensamt varför och hur personuppgifter om deras respektive kunder behandlas och kommer därför att vara gemensamt personuppgiftsansvariga när det gäller behandling av den gemensamma internetbaserade bokningsplattformen och de gemensamma marknadsföringskampanjerna. Var och en av dem skulle dock fortfarande behålla ensam kontroll över andra behandlingar utanför den internetbaserade gemensamma plattformen.

Exempel: Forskningsprojekt av institut

Flera forskningsinstitut beslutar sig för att delta i ett specifikt gemensamt forskningsprojekt och för detta använda den befintliga plattformen för ett av instituten som deltar i projektet. Varje institut matar in personuppgifter som man redan har i plattformen för det gemensamma forskningsprojektet och använder uppgifter som har tillhandahållits av andra via plattformen för att utföra forskningen. I detta fall kvalificerar sig alla institut sig som gemensamt personuppgiftsansvariga för den personuppgiftsbehandling som utförs genom att lagra och dela information via plattformen eftersom de tillsammans har bestämt ändamålet med behandlingen och de medel som ska användas (den befintliga plattformen). Varje institut är dock separat personuppgiftsansvariga för all annan behandling som eventuellt utförs utanför plattformen för deras respektive ändamål.

Exempel: Marknadsföringskampanj

Företagen A och B har lanserat den gemensamma produkten C och vill arrangera ett event för att marknadsföra produkten. För detta ändamål beslutar de att dela data från sina respektive databaser för kunder och potentiella kunder och beslutar om listan över inbjudna till eventet på grundval av detta. De är också överens om metoderna för att skicka inbjudningarna till eventet, hur man samlar in feedback under eventet och uppföljande marknadsföringsåtgärder. Företag A och B kan betraktas som gemensamt personuppgiftsansvariga för behandlingen av personuppgifter relaterade till organiserandet av reklameventet eftersom de tillsammans beslutar om det gemensamt definierade ändamålet och väsentliga sätt för databehandlingen i detta sammanhang.

Exempel: Kliniska prövningar[31]

En vårdgivare (utredaren) och ett universitet (sponsorn) beslutar att tillsammans inleda en klinisk prövning med samma ändamål. De samarbetar för att utarbeta studieprotokollet (dvs. ändamål, metodik/utformning av studien, data som ska samlas in, kriterier för uteslutning/inkludering av försökspersoner, återanvändning av databas [vid behov] etc.). De kan betraktas som gemensamt personuppgiftsansvariga för denna kliniska prövning, eftersom de gemensamt fastställer och är överens om samma ändamål och de väsentliga metoderna för behandlingen. Insamlingen av personuppgifter från patientjournalen för forskningsändamålen ska särskiljas från lagring och användning av samma uppgifter för patientvård, för vilken vårdgivaren förblir personuppgiftsansvarig.

Om utredaren inte deltar i utarbetandet av protokollet (denna accepterar helt enkelt det protokoll som redan har utarbetats av sponsorn) och protokollet endast är utformat av sponsorn bör utredaren betraktas som ett personuppgiftsbiträde och sponsorn som personuppgiftsansvarig för denna kliniska prövning.

Exempel: Rekryterare

Företaget X hjälper företaget Y att rekrytera ny personal med sin berömda värdeskapande tjänst ”global matchz”. Företag X letar efter lämpliga kandidater både bland de CV som tas emot direkt av företag Y och de som man redan har i sin egen databas. Denna databas har skapats och hanteras enbart av företag X. Detta säkerställer att företag X förbättrar matchningen mellan jobberbjudanden och arbetssökande, vilket ökar intäkterna. Även om de inte formellt har fattat ett beslut tillsammans, deltar företag X och Y gemensamt i behandlingen i syfte att hitta lämpliga kandidater baserat på konvergerande beslut: beslutet att skapa och hantera tjänsten ”global matchz” för företag X och beslutet av företag Y att utvidga databasen med de CV som man tar emot direkt. Sådana beslut kompletterar varandra, är oskiljaktiga och nödvändiga för att behandlingen för att kunna hitta lämpliga kandidater ska kunna genomföras. I detta särskilda fall bör de därför betraktas som gemensamt personuppgiftsansvariga för sådan behandling. Företag X är dock ensamt personuppgiftsansvarigt för den behandling som är nödvändig för att hantera deras databas och företag Y är ensamt ansvarig för den efterföljande anställningsbehandlingen för sitt eget ändamål (organisation av intervjuer, ingående av avtal och hantering av personaluppgifter).

Exempel: Analys av hälsouppgifter

Företag ABC, utvecklare av en blodtrycksövervakningsapp och företag XYZ, leverantör av appar för läkare, vill båda undersöka hur blodtrycksförändringar kan hjälpa till att förutsäga vissa sjukdomar. Företagen beslutar sig för att inleda ett gemensamt projekt och kontaktar sjukhuset DEF för att även bjuda in dem att delta.

Personuppgifterna som kommer att behandlas i detta projekt består av personuppgifter som företag ABC, sjukhus DEF och företag XYZ behandlar separat som enskilda personuppgiftsansvariga. Beslutet att behandla dessa uppgifter för att bedöma blodtrycksförändringar fattas gemensamt av de tre aktörerna. Företag ABC, sjukhus DEF och företag XYZ har gemensamt fastställt ändamålen med behandlingen. Företag XYZ tar initiativet att föreslå de väsentliga behandlingsmetoderna. Både företag ABC och sjukhus DEF accepterar dessa väsentliga medel efter att de också var med och utvecklade

[31] EDPB planerar att tillhandahålla ytterligare vägledning om kliniska prövningar inom ramen för sina kommande riktlinjer för behandling av personuppgifter för medicinska och vetenskapliga forskningsändamål.

några av appens funktioner så att resultaten kan användas i tillräcklig utsträckning av dem. De tre organisationerna är alltså överens om att ha ett gemensamt ändamål för behandlingen som är bedömningen av hur blodtrycksförändringar kan hjälpa till att förutsäga vissa sjukdomar. När forskningen är klar kan företag ABC, sjukhus DEF och företag XYZ dra nytta av utvärderingen genom att använda dess resultat i sin egen verksamhet. Av alla dessa skäl kvalificerar de sig som gemensamt personuppgiftsansvariga för denna specifika gemensamma behandling.

Om företag XYZ helt enkelt hade blivit ombett av de andra att utföra denna bedömning utan att ha något eget ändamål och bara behandlat uppgifter för de andras räkning, skulle företag XYZ kvalificera sig som ett personuppgiftsbiträde även om det anförtrotts att fastställa de icke-väsentliga medlen.

3.2.3 Situationer där det inte finns gemensamt personuppgiftsansvar

69. Att flera aktörer är involverade i samma behandling betyder inte nödvändigtvis att de fungerar som gemensamt personuppgiftsansvariga för sådan behandling. Inte alla typer av partnerskap, samarbete eller samarbetsprojekt innebär kvalificering av gemensamt personuppgiftsansvariga eftersom kvalificering för detta kräver en individuell analys av varje behandling som står på spel och varje enhets exakta roll med avseende på varje behandling. Nedanstående fall ger icke-uttömmande exempel på situationer där det inte finns någon gemensamt personuppgiftsansvar.

70. Exempelvis bör utbyte av samma data eller uppsättning data mellan två enheter utan gemensamt bestämda ändamål eller gemensamt bestämda behandlingsmedel betraktas som en överföring av data mellan separata personuppgiftsansvariga.

Exempel: Överföring av anställdas uppgifter till skattemyndigheterna

Ett företag samlar in och behandlar personuppgifter om sina anställda i syfte att hantera löner, sjukförsäkringar, etc. En lag ålägger företaget en skyldighet att skicka alla uppgifter om löner till skattemyndigheterna i syfte att förstärka den finanspolitiska kontrollen.

I detta fall, även om både företaget och skattemyndigheterna behandlar samma uppgifter om löner, kommer avsaknaden av gemensamt fastställda ändamål och medel för denna databehandling att leda till att de två enheterna kvalificeras som två separata personuppgiftsansvariga.

71. Gemensamt personuppgiftsansvar kan också uteslutas i en situation där flera enheter använder en delad databas eller en gemensam infrastruktur, om varje enhet självständigt fastställer sina egna ändamål.

Exempel: Marknadsföring i en grupp företag som använder en delad databas:

En grupp företag använder samma databas för hantering av kunder och potentiella kunder. Denna databas finns på moderbolagets servrar som därför är ett personuppgiftsbiträde för företagen när det gäller lagring av uppgifterna. Varje enhet i gruppen matar in uppgifterna från sina egna kunder och potentiella kunder och behandlar endast sådana uppgifter för sina egna ändamål. Varje enhet beslutar också självständigt om åtkomst, lagringsperioder, korrigering eller radering av sina kunders och potentiella kunders uppgifter. De har inte tillgång till och kan inte använda varandras uppgifter. Bara det faktum att dessa företag använder en delad gruppdatabas innebär inte som sådant gemensamt personuppgiftsansvar. Under dessa omständigheter är varje företag därmed separat personuppgiftsansvariga.

Exempel: Självständigt personuppgiftsansvar vid användning av en delad infrastruktur

Företaget XYZ hostar en databas och gör den tillgänglig för andra företag för att behandla och hosta personuppgifter om sina anställda. Företaget XYZ är personuppgiftsansvarig i förhållande till behandling och lagring av andra företags anställda eftersom dessa operationer utförs på uppdrag och enligt instruktionerna från dessa andra företag. Dessutom behandlar de andra företagen uppgifterna utan någon inblandning från företag XYZ och för ändamål som inte på något sätt delas av företag XYZ.

72. Det kan också finnas situationer där olika aktörer successivt behandlar samma personuppgifter i en verksamhetskedja, var och en av dessa aktörer har ett oberoende syfte och oberoende medel i sin del av kedjan. I avsaknad av gemensamt deltagande i fastställandet av ändamål och medel för samma behandlingsoperation eller uppsättning operationer måste gemensamt personuppgiftsansvar uteslutas och de olika aktörerna måste betraktas som successiva oberoende personuppgiftsansvariga.

Exempel: Statistisk analys för en uppgift av allmänt intresse

En offentlig myndighet (myndighet A) har den juridiska uppgiften att genomföra relevant analys och statistik om hur landets sysselsättningsgrad utvecklas. För att göra det är många andra offentliga enheter juridiskt bundna att lämna ut specifika data till myndighet A. Myndighet A beslutar att använda ett specifikt system för att behandla uppgifterna, inklusive insamling. Detta innebär också att de andra enheterna är skyldiga att använda systemet för att lämna ut uppgifter. I detta fall, utan att det påverkar tillämpningen av roller enligt lag, kommer myndighet A att vara ensamt personuppgiftsansvarig för behandlingen för analys och statistik över sysselsättningsgraden som behandlas i systemet, eftersom myndighet A bestämmer ändamålet med behandlingen, och har bestämt hur behandlingen ska organiseras. Naturligtvis är de andra offentliga enheterna, i egenskap av personuppgiftsansvariga för sina egna behandlingar, ansvariga för att säkerställa riktigheten i de uppgifter som de tidigare har behandlat, som de sedan lämnar ut till myndighet A.

4 DEFINITION AV PERSONUPPGIFTSBITRÄDE

73. Ett personuppgiftsbiträde definieras enligt artikel 4.8 i GDPR som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. I likhet med definitionen av personuppgiftsansvarig innefattar definitionen av personuppgiftsbiträde ett brett spektrum av aktörer. Det kan vara ”*en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ*”. Detta innebär att det i princip inte finns någon begränsning vad gäller vilken typ av aktör som kan ha rollen som personuppgiftsbiträde. Det kan vara en organisation, men också en individ.

74. I GDPR fastställs skyldigheter som är direkt tillämpliga specifikt på personuppgiftsbiträden, vilket specificeras närmare i del II, avsnitt 1, i dessa riktlinjer. Ett personuppgiftsbiträde kan hållas ansvarigt eller bötfällas om man inte efterlever sådana skyldigheter eller om man agerar utanför eller i strid med de lagstadgade instruktionerna från den personuppgiftsansvarige.

75. Behandling av personuppgifter kan involvera flera personuppgiftsbiträden. Till exempel kan en personuppgiftsansvarig själv välja att direkt anlita flera personuppgiftsbiträden genom att involvera olika personuppgiftsbiträden i separata steg i behandlingen (flera personuppgiftsbiträden). En personuppgiftsansvarig kan också besluta att anlita ett personuppgiftsbiträde, som, med tillstånd från den personuppgiftsansvarige, i sin tur anlitar ett eller flera andra personuppgiftsbiträden (”underbiträde(n)”). Behandlingsverksamheten som anförtros ett personuppgiftsbiträde kan vara

begränsad till en mycket specifik uppgift eller ett mycket specifikt sammanhang eller kan vara relativt allmän och omfattande.

76. Två grundläggande villkor för att kvalificera sig som personuppgiftsbiträde är

    a) att vara en *separat enhet* i relation till den personuppgiftsansvarige och

    b) att behandla personuppgifter för *den personuppgiftsansvariges räkning*.

77. En *separat enhet* innebär att den personuppgiftsansvarige beslutar att delegera hela eller delar av behandlingsverksamheten till en extern organisation. Inom en företagsgrupp kan ett företag vara ett personuppgiftsbiträde åt ett annat företag som fungerar som personuppgiftsansvarig, eftersom båda företagen är separata enheter. Å andra sidan kan en avdelning inom ett företag inte vara ett personuppgiftsbiträde åt en annan avdelning inom samma enhet.

78. Om den personuppgiftsansvarige bestämmer sig för att behandla uppgifterna på egen hand, med hjälp av sina egna resurser inom sin organisation, till exempel genom sin egen personal, innebär detta inte en situation med ett personuppgiftsbiträde. Anställda och andra personer som agerar under den personuppgiftsansvariges direkta befogenhet, till exempel tillfälligt anställd personal, ska inte ses som personuppgiftsbiträden eftersom de kommer att behandla personuppgifter som en del av den personuppgiftsansvariges enhet. I enlighet med artikel 29 är de även bundna av den personuppgiftsansvariges instruktioner.

79. *Behandling av personuppgifter för den personuppgiftsansvariges räkning* kräver i första hand att den separata enheten behandlar personuppgifter för den personuppgiftsanvariges räkning. I artikel 4.2 definieras behandling som ett begrepp som omfattar ett brett spektrum av åtgärder, allt från insamling, lagring och läsning till användning, spridning eller tillhandahållande på annat sätt och förstöring. Begreppet ”behandling” beskrivs ytterligare ovan under 2.1.5.

80. För det andra måste behandlingen göras för en personuppgiftsansvarigs räkning men på annat sätt än under dennes direkta befogenhet eller kontroll. Att agera ”för någons räkning” innebär att man tjänar någon annans intressen och detta påminner om det juridiska begreppet ”delegering”. När det gäller dataskyddslagen anlitas ett personuppgiftsbiträde för att implementera instruktionerna från den personuppgiftsansvarige, åtminstone med avseende på ändamålet med behandlingen och de väsentliga elementen i medlen. Laglig behandling av personuppgifter enligt artikel 6, och i förekommande fall artikel 9, i förordningen härleds från den personuppgiftsansvariges verksamhet och personuppgiftsbiträdet får inte behandla uppgifterna på annat sätt än enligt den personuppgiftsansvariges instruktioner. Trots detta, enligt vad som beskrivs ovan, kan den personuppgiftsansvariges instruktioner fortfarande tillåta viss handlingsfrihet angående hur man bäst försvarar den personuppgiftsansvariges intressen genom att tillåta personuppgiftsbiträdet att välja de mest lämpliga tekniska och organisatoriska behandlingssätten.[32]

81. Att verka ”för någons räkning” innebär även att personuppgiftsbiträdet inte får utföra någon behandling i eget syfte. Enligt vad som anges i artikel 28.10 bryter ett personuppgiftsbiträde mot GDPR om man avviker från den personuppgiftsansvariges instruktioner och börjar att fastställa sina egna behandlingsändamål och behandlingssätt. Personuppgiftsbiträdet kommer att betraktas som en personuppgiftsansvarig för denna behandling och kan vara föremål för sanktioner för att ha avvikit från den personuppgiftsansvariges instruktioner.

[32] Se del I, underavsnitt 2.1.4 som beskriver skillnaden mellan väsentliga och icke-väsentliga medel.

Exempel: Tjänsteleverantör hänvisas till som personuppgiftsbiträde men agerar som personuppgiftsansvarig

Tjänsteleverantören MarketinZ tillhandahåller reklam och direkta marknadsföringstjänster till flera olika företag. Företaget GoodProductZ ingår ett avtal med MarketinZ, enligt vilket det senare företaget tillhandahåller kommersiell reklam för GoodProductZ kunder och benämns personuppgiftsbiträde. MarketinZ beslutar dock att använda GoodProducts kunddatabas även för andra ändamål än reklam för GoodProducts, som till exempel att utveckla sin egen affärsverksamhet. Beslutet att lägga till ett ytterligare ändamål utöver det för vilket personuppgifterna överfördes omvandlar MarketinZ till en personuppgiftsansvarig för denna uppsättning behandlingsoperationer och deras behandling för detta ändamål skulle utgöra en överträdelse av bestämmelserna i GDPR.

82. EDPB påminner om att inte alla tjänsteleverantörer som behandlar personuppgifter vid tillhandahållandet av en tjänst är ett ”personuppgiftsbiträde” i den mening som avses i GDPR. En personuppgiftsansvarigs roll härrör inte från den databehandlande enhetens natur utan från dess konkreta verksamhet i ett specifikt sammanhang. Med andra ord kan samma enhet fungera som personuppgiftsansvarig för vissa behandlingsoperationer och som personuppgiftsbiträde för andra samtidigt, och kvalifikationen som personuppgiftsansvarig eller personuppgiftsbiträde måste bedömas med avseende på varje specifik databehandlingsaktivitet. Tjänstens art kommer att avgöra om behandlingsaktiviteten innebär behandling av personuppgifter för den personuppgiftsansvariges räkning i den mening som avses i GDPR. I praktiken, när den tillhandahållna tjänsten inte specifikt är inriktad på behandling av personuppgifter eller om sådan behandling inte utgör en viktig del av tjänsten, kan tjänsteleverantören självständigt bestämma ändamål och sätt för den behandling som krävs för att tillhandahålla tjänsten. I denna situation ska tjänsteleverantören ses som en separat personuppgiftsansvarig och inte som ett personuppgiftsbiträde.[33] En analys från fall till fall förblir dock nödvändig för att fastställa graden av inflytande som varje enhet effektivt har för att bestämma ändamål och medel för behandlingen.

Exempel: Taxitjänst

En taxitjänst erbjuder en onlineplattform som gör det möjligt för företag kan boka en taxi för att transportera anställda eller gäster till och från flygplatsen. När de bokar en taxi anger företaget ABC namnet på den anställde som ska hämtas från flygplatsen så att föraren kan bekräfta den anställdes identitet vid upphämtningstillfället. I detta fall behandlar taxitjänsten personuppgifter om den anställde som en del av sin tjänst till företag ABC, men behandlingen som sådan är inte målet för tjänsten. Taxitjänsten har utformat onlinebokningsplattformen som ett led i att utveckla sin egen affärsverksamhet för att tillhandahålla transporttjänster, utan några instruktioner från företag ABC. Taxitjänsten bestämmer även självständigt vilka kategorier av data den samlar in och hur länge dessa uppgifter lagras. Taxitjänsten fungerar därför som personuppgiftsansvarig i sig självt, trots att behandlingen sker efter en tjänstebegäran från företag ABC.

83. EDPB noterar att en tjänsteleverantör fortfarande kan fungera som personuppgiftsbiträde även om behandlingen av personuppgifter inte är tjänstens huvudsyfte eller primära syfte, förutsatt att kunden för tjänsten fortfarande bestämmer ändamålen och medlen för behandlingen i praktiken. När de överväger om de ska överlåta behandlingen av personuppgifter till en viss tjänsteleverantör eller inte, bör personuppgiftsansvariga noggrant bedöma om tjänsteleverantören i fråga tillåter dem att utöva

[33] Se även skäl 81 i GDPR, som hänvisar till att ”anförtro behandling åt ett personuppgiftsbiträde”, vilket indikerar att behandlingen som sådan är en viktig del av den personuppgiftsansvariges beslut att be ett personuppgiftsbiträde att behandla personuppgifter för sin räkning.

en tillräcklig grad av kontroll, med hänsyn till arten, omfattningen, sammanhanget och ändamålet med behandlingen samt de potentiella riskerna för registrerade personer.

Exempel: Callcenter

Företag X lägger ut sin kundsupport på entreprenad till företag Y som tillhandahåller ett callcenter för att hjälpa företag X:s kunder med deras frågor. Kundsupporttjänsten innebär att företag Y har tillgång till företag X:s kunddatabas. Företag Y har endast åtkomst till uppgifterna för att tillhandahålla den support som företag X har begärt och de kan inte behandla uppgifter för andra ändamål än de som anges av företag X. Företag Y ska ses som ett personuppgiftsbiträde och ett behandlingsavtal måste ingås mellan företag X och Y.

Exempel: Allmän it-support

Företag Z anlitar en it-tjänsteleverantör för att ansvara för allmän support för deras it-system, vilket inkluderar en stor mängd personuppgifter. Åtkomsten till personuppgifterna är inte huvudsyftet för supporttjänsten men det är oundvikligt att it-tjänsteleverantören systematiskt har tillgång till personuppgifter när tjänsten utförs. Företag Z drar därför slutsatsen att it-tjänsteleverantören, som är ett separat företag och oundvikligen måste behandla personuppgifter även om detta inte är tjänstens huvudsyfte, är att betrakta som ett personuppgiftsbiträde. Ett behandlingsavtal ingås därför med it-tjänsteleverantören.

Exempel: It-konsult åtgärdar ett programvarufel

Företag ABC anlitar en it-specialist från ett annat företag för att åtgärda ett fel i ett program som används av företaget. It-konsulten har inte anlitats för att behandla personuppgifter och företag ABC fastställer att all åtkomst till personuppgifter kommer endast att vara tillfällig och därför väldigt begränsad i praktiken. ABC drar därför slutsatsen att it-specialisten inte är ett personuppgiftsbiträde (och inte heller en personuppgiftsansvarig i sig självt) och att företag ABC kommer att vidta lämpliga åtgärder enligt artikel 32 i GDPR för att förhindra it-konsulten från att behandla personuppgifter på ett obehörigt sätt.

84. Som nämnts ovan finns det inget som hindrar personuppgiftsbiträdet från att erbjuda en preliminärt definierad tjänst men den personuppgiftsansvarige måste fatta det slutgiltiga beslutet att aktivt godkänna hur behandlingen utförs, åtminstone i den mån det gäller de väsentliga metoderna för behandlingen. Som nämnts ovan har ett personuppgiftsbiträde viss valfrihet när det gäller icke-väsentliga medel, se ovan under underavsnitt 2.1.4.

Exempel: Molntjänsteleverantör

En kommun har beslutat att använda en molntjänsteleverantör för att hantera information i anslutning till sina skol- och utbildningstjänster. Molntjänsten tillhandahåller meddelandetjänster, videokonferenser, lagring av dokument, kalenderhantering, ordbehandling, etc. och kommer att omfatta behandling av personuppgifter om skolbarn och lärare. Molntjänstleverantören erbjuder en standardiserad tjänst som erbjuds över hela världen. Kommunen måste dock se till att det överenskomna avtalet uppfyller kraven för artikel 28.3 i GDPR, dvs. att de personuppgifter som man är personuppgiftsansvarig för endast behandlas för kommunens ändamål. Man måste även se till att deras specifika instruktioner om lagringstider, radering av data, etc., respekteras av molntjänstleverantören oavsett vad som generellt erbjuds i den standardiserade tjänsten.

5 DEFINITION AV TREDJE PART/MOTTAGARE

85. Förordningen definierar inte bara begreppen personuppgiftsansvarig och personuppgiftsbiträde utan även begreppen mottagare och tredje part. I motsats till begreppen personuppgiftsansvarig och personuppgiftsbiträde föreskriver förordningen inte specifika skyldigheter eller ansvar för mottagare och tredje parter. Dessa kan sägas vara relativa begrepp i den meningen att de beskriver en relation till en personuppgiftsansvarig eller ett personuppgiftsbiträde ur ett specifikt perspektiv, t.ex. en personuppgiftsansvarig eller ett personuppgiftsbiträde överför uppgifter till en mottagare. En mottagare av personuppgifter och en tredje part kan även samtidigt betraktas som personuppgiftsansvarig eller personuppgiftsbiträde ur andra perspektiv. Till exempel är enheter som ska ses som mottagare eller tredje parter ur ett perspektiv, personuppgiftsansvariga för den behandling för vilken de bestämmer ändamålet och medlen.

Tredje part

86. I artikel 4.10 definieras en ”*tredje part*” som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ än

- den registrerade personen,
- den personuppgiftsansvarige,
- personuppgiftsbiträdet och
- personer som under direkt ansvar från den personuppgiftsansvarige eller personuppgiftsbiträdet har tillstånd att behandla personuppgifter.

87. Definitionen motsvarar i allmänhet den föregående definitionen av ”*tredje part*” i direktiv 95/46/EG.

88. Medan termerna ”*personuppgifter*”, ”*registrerad person*”, ”*personuppgiftsansvarig*” och ”*personuppgiftsbiträde*” definieras i förordningen, definieras begreppet ”*personer som, under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta befogenhet, har behörighet att behandla personuppgifter*” inte. Det förstås dock allmänt som att det hänvisar till personer som tillhör den personuppgiftsansvariges eller personuppgiftsbiträdets juridiska enhet (en anställd eller en befattning som är mycket jämförbar med de anställdas, t.ex. tillfällig personal som tillhandahålls via ett bemanningsföretag) men endast i den mån de är behöriga att behandla personuppgifter. En anställd som får tillgång till uppgifter som han eller hon inte är behörig att få tillgång till och för andra ändamål än arbetsgivarens tillhör inte till denna kategori. Istället bör en sådan anställd betraktas som en tredje part gentemot den behandling som utförs av arbetsgivaren. I den mån arbetstagaren behandlar personuppgifter för sina egna ändamål, som skiljer sig från arbetsgivarens, kommer han eller hon då att betraktas som en personuppgiftsansvarig och ta på sig alla följder och skyldigheter i fråga om behandling av personuppgifter.[34]

89. En tredje part hänvisar alltså till någon som i den aktuella situationen inte är en registrerad person, en personuppgiftsansvarig, ett personuppgiftsbiträde eller en anställd. Till exempel kan den personuppgiftsansvarige anlita ett personuppgiftsbiträde och instruera denne att överföra personuppgifter till en tredje part. Denna tredje part kommer då att betraktas som en separat personuppgiftsansvarig för behandlingen som den utför för sina egna ändamål. Det bör noteras att inom ett företagsgrupp är ett annat företag än den personuppgiftsansvarige eller

[34] Arbetsgivaren (som ursprunglig personuppgiftsansvarig) kan ändå behålla ett visst ansvar om den nya behandlingen inträffade på grund av en avsaknad av adekvata säkerhetsåtgärder.

personuppgiftsbiträdet en tredje part, även om det tillhör samma grupp som företaget som fungerar som personuppgiftsansvarig eller personuppgiftsbiträde.

Exempel: Städtjänster

Företag A ingår ett avtal med ett städföretag som ska städa deras kontor. Städpersonalen har inte tillgång till, eller ska behandla personuppgifter på annat sätt. Även om de ibland kan stöta på sådana uppgifter när de rör sig runt på kontoret, kan de utföra sin uppgift utan att få tillgång till uppgifter och de är avtalsenligt förbjudna att komma åt eller på annat sätt behandla personuppgifter som företag A lagrar i egenskap av personuppgiftsansvarig. Städpersonalen är inte anställda av företag A och de betraktas inte heller som direkt underställda detta företags myndighet. Det finns ingen avsikt att anlita städföretaget eller dess anställda för att behandla personuppgifter för företagets räkning. Städföretaget och dess anställda ska därför ses som en tredje part och den personuppgiftsansvarige måste se till att det finns tillräckliga säkerhetsåtgärder för att förhindra att de får tillgång till personuppgifter och införa en sekretessplikt om de av misstag skulle stöta på personuppgifter.

Exempel: Företagsgrupper – moderföretag och dotterföretag

Företagen X och Y ingår som en del i Koncern Z. Företagen X och Y behandlar båda personuppgifter om sina respektive anställda i administrationssyfte. Vid en viss tidpunkt beslutar sig moderföretaget ZZ för att begära personuppgifter för de anställda från alla dotterföretag för att sammanställa koncernövergripande statistik. Vid överföring av uppgifter från företag X och Y till ZZ är de sistnämnda att betrakta som en tredje part oavsett faktumet att alla företag ingår i samma koncern. Företag ZZ kommer att betraktas som personuppgiftsansvarig för sin behandling av uppgifterna i statistiskt syfte.

Mottagare

90. Artikel 4.9 definierar en ”*mottagare*” som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilken/vilket personuppgifter utlämnas, vare sig det rör sig om en tredje part eller inte. Offentliga myndigheter ska dock inte ses som mottagare när de tar emot personuppgifter inom ramen för en viss utredning i enlighet med unionens eller medlemsstaternas lagstiftning (t.ex. skatte- och tullmyndigheter, finansiella utredningsenheter, etc.)[35]

91. Definitionen motsvarar i allmänhet den föregående definitionen av ”*mottagare*” i direktiv 95/46/EG.

92. Definitionen omfattar alla som tar emot personuppgifter, oavsett om de är tredje part eller inte. När en personuppgiftsansvarig exempelvis skickar personuppgifter till en annan enhet, antingen ett personuppgiftsbiträde eller en tredje part, är denna enhet en mottagare. En tredjepartsmottagare ska betraktas som personuppgiftsansvarig för all behandling som man utför för sina egna ändamål efter att man har tagit emot uppgifterna.

Exempel: Överföring av uppgifter mellan företag

Resebyrån ExploreMore anordnar resor på begäran av sina individuella kunder. I anslutning till denna tjänst skickar de kundernas personuppgifter till flygbolag, hotell och utflyktsarrangörer för att de ska kunna utföra sina respektive tjänster. ExploreMore, hotellen, flygbolagen och utflyktsarrangörerna bör samtliga betraktas som personuppgiftsansvariga för behandlingen de utför i anslutning till sina

[35] Se även skäl 31 i dataskyddsförordningen

respektive tjänster. Det finns ingen relation mellan personuppgiftsansvarig och personuppgiftsbiträde. Dock bör flygbolagen, hotellen och utflyktsarrangörerna betraktas som mottagare när de tar emot personuppgifter från ExploreMore.

DEL II – KONSEKVENSER FÖR TILLDELNING AV OLIKA ROLLER

1 RELATIONEN MELLAN PERSONUPPGIFTSANSVARIG OCH PERSONUPPGIFTSBITRÄDE

93. En tydlig nyhet i GDPR är bestämmelserna som ålägger personuppgiftsbiträden direkta skyldigheter. Till exempel måste en personuppgiftsansvarig säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet (artikel 28.3). Ett personuppgiftsbiträde måste föra ett register över alla kategorier av behandling (artikel 30.2) och vidta lämpliga tekniska och organisatoriska åtgärder (artikel 32). Ett personuppgiftsbiträde måste även utnämna ett dataskyddsombud under vissa förutsättningar (artikel 37) och har en skyldighet att utan onödigt dröjsmål meddela den personuppgiftsansvarige efter att ha fått kännedom om ett dataintrång (artikel 33.2). Vidare gäller reglerna för överföring av data till tredjeländer (kapitel V) såväl för personuppgiftsbiträden som personuppgiftsansvariga. I detta avseende anser EDPB att artikel 28.3 i GDPR, samtidigt som det kräver ett specifikt innehåll för det nödvändiga avtalet mellan personuppgiftsansvarig och personuppgiftsbiträde, ålägger personuppgiftsbiträden direkta skyldigheter, inklusive skyldigheten att hjälpa den personuppgiftsansvarige att säkerställa efterlevnaden.[36]

1.1 Personuppgiftsbiträdets val

94. Den personuppgiftsansvarige har **skyldigheten att endast använda ”personuppgiftsbiträden som ger tillräckliga garantier** för att införa lämpliga tekniska och organisatoriska åtgärder”, så att behandlingen uppfyller kraven i GDPR, inklusive för behandlingens säkerhet, och säkerställer skyddet av de registrerade personernas rättigheter.[37] Den personuppgiftsansvarige är därför ansvarig för att bedöma om garantierna från personuppgiftsbiträdet är tillräckliga och bör kunna bevisa att den har tagit alla element i GDPR på allvar.

95. Garantierna ”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. Ofta kräver detta utbyte av relevant dokumentation (t.ex. integritetspolicy, användarvillkor, register över behandlingsaktiviteter, registerhanteringspolicy, informationssäkerhetspolicy, rapporter om externa dataskyddsrevisioner, erkända internationella certifieringar, som ISO 27000-serien).

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 anförtrotts

[36] Till exempel bör personuppgiftsbiträdet vid behov och på begäran bistå den personuppgiftsansvarige med att säkerställa att skyldigheterna i samband med konsekvensanalyser för dataskydd efterlevs (skäl 95 i GDPR). Detta måste återspeglas i avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt artikel 28.3 f i GDPR.
[37] Artikel 28.1 och skäl 81 i GDPR.

personuppgiftsbiträdet och måste göras från fall till fall, med hänsyn till karaktär, omfattning, sammanhang och ändamål 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 demonstrera i ett givet scenario, eftersom detta i hög grad beror på de specifika omständigheterna för behandlingen.

97. Följande element[38] bör beaktas av den personuppgiftsansvarige för att bedöma om garantierna är tillräckliga: personuppgiftsbiträdets **expertkunskap** (t.ex. teknisk expertis när det gäller säkerhetsåtgärder och dataintrång); personuppgiftsbiträdets **tillförlitlighet**; personuppgiftsbiträdets **resurser**. Personuppgiftsbiträdets rykte på marknaden kan också vara en relevant faktor som den personuppgiftsansvarige bör beakta.

98. Vidare kan efterlevnaden av en godkänd uppförandekod eller certifieringsmekanism användas som ett element genom vilket tillräckliga garantier kan demonstreras.[39] Personuppgiftsbiträdena uppmanas därför att informera den personuppgiftsansvarige om denna omständighet, samt om eventuella förändringar i sådan efterlevnad.

99. Förpliktelsen att endast använda personuppgiftsbiträden som ”ger tillräckliga garantier” enligt artikel 28.1 i GDPR är en kontinuerlig förpliktelse. Den upphör inte vid tidpunkten när den personuppgiftsansvarige och personuppgiftsbiträdet ingår i ett avtal eller annan rättsakt. Snarare bör den personuppgiftsansvarige med lämpliga mellanrum verifiera personuppgiftsbiträdets garantier, genom revisioner och inspektioner där så är lämpligt.[40]

1.2 Form för avtal eller annan rättsakt

100. All behandling av personuppgifter av ett personuppgiftsbiträde måste styras av ett avtal eller annan rättsakt mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt unionens eller medlemsstaternas lagstiftning, i enlighet med artikel 28.3 i GDPR.

101. En sådan rättsakt måste vara **skriftlig, inklusive i elektroniskt format**.[41] Därför kan icke-skriftliga avtal (oavsett hur grundliga eller effektiva de är) inte anses tillräckliga för att uppfylla kraven i artikel 28 i GDPR. För att undvika svårigheter när det gäller att uppvisa att avtalet eller den andra rättsliga handlingen verkligen har trätt i kraft rekommenderar EDPB att se till att nödvändiga underskrifter ingår i den rättsliga handlingen, i enlighet med tillämplig lag (t.ex. avtalsrätt).

102. Avtalet eller den andra rättsliga handlingen enligt unionsrätten eller medlemsstaternas lagstiftning måste dessutom vara **bindande för personuppgiftsbiträdet** gentemot den personuppgiftsansvarige, dvs. det/den måste fastställa förpliktelser för personuppgiftsbiträdet som är bindande enligt unionsrätten eller medlemsstaternas lagstiftning. Även den personuppgiftsansvariges förpliktelser bör fastställas. I de flesta fall kommer det att finnas ett avtal, men förordningen hänvisar också till ”annan rättsakt”, som exempelvis nationell lagstiftning (primär eller sekundär) eller annat rättsligt instrument. Om den rättsliga handlingen inte innehåller alla de minimikrav som krävs, måste den kompletteras med ett avtal eller en annan rättsakt som innehåller de saknade elementen.

[38] Skäl 81 i GDPR.
[39] Artikel 28.5 och skäl 81 i GDPR.
[40] Se även artikel 28.3 h i GDPR.
[41] Artikel 28.9 i GDPR.

103. Eftersom förordningen fastställer en tydlig förpliktelse att ingå ett skriftligt avtal, där ingen annan relevant rättsakt är i kraft, är avsaknaden av detta en överträdelse av GDPR.[42] Både den personuppgiftsansvarige och personuppgiftsbiträdet ansvarar för att säkerställa att det finns ett avtal eller annan rättsakt som styr behandlingen.[43] Med förbehåll för bestämmelserna i artikel 83 i GDPR kommer den behöriga tillsynsmyndigheten att kunna bötfälla både den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av omständigheterna i varje enskilt fall. Avtal som har ingåtts före datumet för tillämpningen av GDPR bör ha uppdaterats mot bakgrund av artikel 28.3. Avsaknad av en sådan uppdatering, för att få ett tidigare befintligt avtal att överensstämma med kraven i GDPR, utgör en överträdelse mot artikel 28.3.

Ett skriftligt avtal enligt artikel 28.3 i GDPR kan vara inbäddat i ett bredare avtal, till exempel ett servicenivåavtal. För att underlätta demonstrationen av överensstämmelse med GDPR rekommenderar EDPB att de delar av avtalet som syftar till att genomföra artikel 28 i GDPR tydligt identifieras som sådana på en plats (till exempel i en bilaga).

104. För att uppfylla förpliktelsen att ingå ett avtal kan **den personuppgiftsansvarige och personuppgiftsbiträdet välja att förhandla fram ett eget avtal** som inkluderar alla obligatoriska element **eller helt eller delvis förlita sig på standardavtalsklausuler i förhållande till förpliktelser enligt artikel 28**.[44]

105. En uppsättning standardavtalsklausuler kan alternativt antas av kommissionen[45] eller antas av en tillsynsmyndighet i enlighet med konsekvensmekanismen.[46] Dessa klausuler kan utgöra en del av en certifiering som beviljas den personuppgiftsansvarige eller personuppgiftsbiträdet enligt artiklarna 42 eller 43.[47]

---

[42] Förekomsten (eller frånvaron) av ett skriftligt arrangemang är emellertid inte avgörande för förekomsten av en relation mellan en personuppgiftsansvarig och ett personuppgiftsbiträde. Om det finns anledning att tro att avtalet inte överensstämmer med verkligheten när det gäller faktisk kontroll, på grundval av en saklig analys av omständigheterna kring förhållandet mellan parterna och behandlingen av personuppgifter som genomförs, kan avtalet bortses från. Omvänt kan en relation mellan en personuppgiftsansvarig och ett personuppgiftsbiträde fortfarande anses föreligga i avsaknad av ett skriftligt behandlingsavtal. Det skulle dock innebära en överträdelse av artikel 28.3 i GDPR. Under vissa omständigheter kan avsaknaden av en tydlig definition av förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet dessutom väcka problemet med bristen på rättslig grund som varje behandling bör baseras på, t.ex. när det gäller kommunikation av uppgifter mellan den personuppgiftsansvarige och den som anses vara personuppgiftsbiträde.

[43] Artikel 28.3 är inte bara tillämplig för personuppgiftsansvariga. I en situation där endast personuppgiftsbiträdet omfattas av GDPR:s territoriella tillämpningsområde, ska förpliktelsen endast vara direkt tillämplig på personuppgiftsbiträdet, se även EDPB:s riktlinjer 3/2018 angående GDPR:s territoriella tillämpningsområde, s. 12.

[44] Artikel 28.6 i GDPR. EDPB erinrar om att standardavtalsklausulerna i enlighet med artikel 28 GDPR inte är desamma som de standardavtalsklausuler som avses i artikel 46.2. Även om de föregående föreskriver och förtydligar hur bestämmelserna i artiklarna 28.3 och 28.4 kommer att uppfyllas, tillhandahåller de sistnämnda lämpliga skyddsåtgärder vid överföring av personuppgifter till ett tredjeland eller en internationell organisation i avsaknad av ett tillräcklighetsbeslut enligt artikel 45.3.

[45] Artikel 28.7 i GDPR. Artikel 28.7 i GDPR. Artikel 28.7 i GDPR. Artikel 28.7 i GDPR. Se EDPB-EDPS gemensamma yttrande 1/2021 angående standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_sv.

[46] Artikel 28.8 i GDPR. Registret för beslut som tagits av tillsynsmyndigheter och domstolar i frågor som hanteras i konsekvensmekanismen, inklusive standardavtalsklausuler för efterlevnad av artikel 28 i GDPR, kan nås här: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_sv.

[47] Artikel 28.6 i GDPR.

106. EDPB vill förtydliga att det inte finns någon skyldighet för personuppgiftsansvariga och personuppgiftsbiträden att ingå ett avtal baserat på standardavtalsklausuler och det är inte nödvändigtvis att föredra framför att förhandla fram ett individuellt avtal. Båda alternativen är gångbara för efterlevnad av dataskyddslagarna beroende på de specifika omständigheterna, så länge de uppfyller kraven i artikel 28.3.

107. Om parterna vill utnyttja standardavtalsklausuler måste dataskyddsklausulerna i deras avtal vara desamma som de i standardavtalsklausulerna. Standardavtalsklausulerna har ofta några tomma rader som kan fyllas i eller alternativ som kan väljas av parterna. Som också har nämnts ovan kommer standardavtalsklausulerna i allmänhet att vara inbäddade i ett större avtal som beskriver syftet för avtalet, dess ekonomiska villkor och andra överenskomna klausuler: det kommer att vara möjligt för parterna att lägga till ytterligare klausuler (t.ex. tillämplig lag och jurisdiktion) så länge de inte direkt eller indirekt motsäger standardavtalsklausulerna[48] och de inte undergräver det skydd som ges av GDPR och EU:s eller medlemsstaternas dataskyddslagar.

108. Avtal mellan personuppgiftsansvariga och personuppgiftsbiträden kan ibland upprättas ensidigt av en av parterna. Vilken eller vilka parter som utarbetar avtalet kan bero på flera faktorer, däribland: parternas position på marknaden och avtalsmakt, deras tekniska expertis samt tillgång till juridiska tjänster. Till exempel tenderar vissa tjänsteleverantörer att inkludera standardvillkor som inkluderar avtal om databehandling.

109. Ett 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. I vissa situationer kan en personuppgiftsansvarig eller ett personuppgiftsbiträde ha en svagare förhandlingsposition för anpassning av dataskyddsavtalet. Att förlita sig på de standardavtalsklausuler som antagits enligt artikel 28 (styckena 7 och 8) kan bidra till att balansera förhandlingspositionerna och se till att avtalen respekterar GDPR.

110. Faktumet att avtalet och dess detaljerade affärsvillkor utarbetas av tjänsteleverantören snarare än av den personuppgiftsansvarige är inte i sig problematiskt och är inte i sig en tillräcklig grund för att dra slutsatsen att tjänsteleverantören bör betraktas som en personuppgiftsansvarig. Obalansen i förhandlingspositionen hos en liten personuppgiftsansvarig jämfört med stora tjänsteleverantörer bör inte heller ses som en motivering för den personuppgiftsansvarige att acceptera klausuler och villkor som inte överensstämmer med dataskyddslagstiftningen och inte heller kan det undanta den personuppgiftsansvarige från dennes dataskyddsförpliktelser. Den personuppgiftsansvarige måste utvärdera villkoren och i den mån man frivilligt accepterar dem och använder tjänsten, har man även

[48] EDPB påminner om att samma grad av flexibilitet är tillåten när parterna väljer att använda standardavtalsklausuler som ett lämpligt skydd för överföringar till tredjeländer enligt artikel 46.2 c eller artikel 46.2 d i GDPR. Skäl 109 i GDPR klargör att *"Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausulerna [...] eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade skyddsbestämmelserna."*.

accepterat det fulla ansvaret för efterlevnad av GDPR. Varje föreslagen ändring från personuppgiftsbiträdets sida av databehandlingsavtal som ingår i standardvillkor bör direkt anmälas till och godkännas av den personuppgiftsansvarige, med beaktande av graden av spelrum som personuppgiftsbiträdet har med avseende på icke-väsentliga delar av medlen (se punkterna 40–41 ovan). Att bara publicera dessa ändringar på personuppgiftsbiträdets webbplats innebär inte efterlevnad av artikel 28.

1.3 Avtalets eller annan rättsakts innehåll

111. Innan vi fokuserar på vart och ett av de detaljerade kraven i GDPR angående innehållet i avtalet eller annan rättsakt är några allmänna kommentarer nödvändiga.

112. Även om de delar som anges i artikel 28 i förordningen utgör dess kärninnehåll, bör avtalet vara ett sätt för den personuppgiftsansvarige och personuppgiftsbiträdet att ytterligare klargöra hur sådana kärnelement kommer att genomföras med detaljerade instruktioner. **Behandlingsavtalet bör därför inte bara upprepa bestämmelserna i GDPR** utan bör snarare inkludera mera specifik och konkret information angående hur kraven kommer att uppfyllas och vilken säkerhetsnivå som krävs för behandlingen av personuppgifterna som är föremål för behandlingsavtalet. Förhandlingarna och upprättandet av avtalet, som är långt ifrån att vara en demonstrationsövning, är en chans att specificera behandlingsuppgifterna.[49] Faktum är att ”skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar [...] kräver ett tydligt fastställande av vem som bär ansvaret” enligt GDPR.[50]

113. Samtidigt bör avtalet **ta hänsyn till *”personuppgiftsbiträdets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter”*.**[51] Generellt sett bör avtalet mellan parterna utarbetas mot bakgrund av den specifika databehandlingen. Det är till exempel inte nödvändigt att införa särskilt stränga skydd och förfaranden för ett personuppgiftsbiträde som har anförtrotts en behandling från vilken endast mindre risker uppstår: även om varje personuppgiftsbiträde måste uppfylla kraven i förordningen, bör åtgärderna och förfarandena skräddarsys efter den specifika situationen. Under alla omständigheter måste alla delar av artikel 28.3 omfattas av avtalet. Samtidigt bör avtalet innehålla några element som kan hjälpa personuppgiftsbiträdet att förstå riskerna för de registrerade personernas rättigheter och friheter som härrör från behandlingen: eftersom aktiviteten utförs för den personuppgiftsansvariges räkning, har den personuppgiftsansvarige ofta en djupare förståelse för de risker som behandlingen innebär eftersom den personuppgiftsansvarige är medveten om omständigheterna under vilka behandlingen sker.

114. När det gäller det **nödvändiga innehållet** i avtalet eller annan rättsakt tolkar EDPB artikel 28.3 det som att det måste innehålla:

- **Föremålet** för behandlingen (till exempel videoövervakningsinspelningar av personer som anländer till och lämnar en högsäkerhetsanläggning). Även om föremålet för behandlingen är ett brett begrepp, måste det formuleras tillräckligt specifikt så att det är tydligt vad som är huvudsyftet med behandlingen.

[49] Se även EDPB:s yttrande 14/2019 angående utkastet till standardavtalsklausuler inlämnat av den danska tillsynsmyndigheten (artikel 28.8 i GDPR), s. 5.
[50] Skäl 79 i GDPR.
[51] Skäl 81 i GDPR.

- Behandlingens **varaktighet:**[52] den exakta tidsperioden, eller de kriterier som används för att fastställa den, bör specificeras. Till exempel kan man hänvisa till behandlingsavtalets varaktighet.
- Behandlingens **natur**: typen av åtgärder som utförs som en del av behandlingen (t.ex. ”filmning”, ”inspelning” och ”arkivering av bilder”) och behandlingens **ändamål** (t.ex. detektera otillåtet inträde). Denna beskrivning bör vara så omfattande som möjligt, beroende på den specifika behandlingen, så att externa parter (t.ex. tillsynsmyndigheter) kan förstå innehållet och riskerna med behandlingen som anförtrotts personuppgiftsbiträdet.
- **Typen av personuppgifter**: detta bör specificeras på ett så detaljerat sätt som möjligt (t.ex. videobilder av individer när de går in och ut ur anläggningen). Det vore inte tillräckligt att bara ange att det är ”personuppgifter enligt artikel 4.1 i GDPR” eller ”särskilda kategorier av personuppgifter enligt artikel 9”. Vid särskilda datakategorier bör avtalet eller rättshandlingen åtminstone specificera vilka typer av uppgifter som berörs, till exempel ”information om hälsojournaler” eller ”information angående huruvida den registrerade personen är medlem av en fackförening”.
- **Kategorierna av registrerade personer**: även detta bör anges på ett tämligen specifikt sätt (t.ex. ”besökare”, ”anställda” och ”leveranstjänster”).
- **Den personuppgiftsansvariges skyldigheter och rättigheter**: den personuppgiftsansvariges rättigheter behandlas vidare i följande avsnitt (t.ex. med avseende på den personuppgiftsansvariges rätt att utföra inspektioner och revisioner). När det gäller den personuppgiftsansvariges skyldigheter inkluderar exemplen den personuppgiftsansvariges skyldighet att förse personuppgiftsbiträdet med de uppgifter som nämns i avtalet, att tillhandahålla och dokumentera alla instruktioner som berör behandlingen av uppgifter, för att säkerställa (före och under hela behandlingen) efterlevnad av de skyldigheter som anges i GDPR från personuppgiftsbiträdets sida, att övervaka behandlingen, bland annat genom att genomföra revisioner och inspektioner med personuppgiftsbiträdet.

115. Även om GDPR anger alla de element som alltid måste ingå i avtalet, kan annan relevant information behöva inkluderas, beroende på sammanhanget och riskerna med behandlingen samt eventuella ytterligare tillämpliga krav.

1.3.1 Personuppgiftsbiträdet får endast behandla uppgifter på dokumenterade instruktioner från den personuppgiftsansvarige (artikel 28.3 a i GDPR)

116. Behovet av att specificera denna skyldighet härrör från det faktum att personuppgiftsbiträdet behandlar uppgifter för den personuppgiftsansvariges räkning. Personuppgiftsansvariga måste förse sina personuppgiftsbiträden med instruktioner i anslutning till varje behandling. Sådana instruktioner kan omfatta tillåten och oacceptabel hantering av personuppgifter, mera detaljerade förfaranden, sätt att säkra data etc. Personuppgiftsbiträdet får inte gå utöver vad som instrueras av den personuppgiftsansvarige. Det är dock möjligt för personuppgiftsbiträdet att föreslå element som, om de accepteras av den personuppgiftsansvarige, blir en del av de angivna instruktionerna.

117. När ett personuppgiftsbiträde behandlar uppgifter utanför eller bortom den personuppgiftsansvariges instruktioner, och detta innebär ett beslut som fastställer ändamål och behandlingsmedel, kommer

[52] Behandlingstiden är inte nödvändigtvis likvärdig med avtalets varaktighet (det kan finnas lagliga skyldigheter att behålla uppgifterna längre eller kortare).

personuppgiftsbiträdet att bryta mot sina skyldigheter och kommer till och med att betraktas som personuppgiftsansvarig med avseende på den behandlingen i enlighet med artikel 28.10 (se underavsnitt 1.5 nedan[53]).

118. Instruktionerna som utfärdas av den personuppgiftsansvarige måste **dokumenteras**. För detta ändamål rekommenderas att inkludera ett förfarande och en mall för att ge ytterligare instruktioner i en bilaga till avtalet eller annan rättshandling. Alternativt kan instruktionerna tillhandahållas i valfritt skriftligt format (t.ex. e-post), liksom i alla andra dokumenterade former så länge det är möjligt att föra register över sådana instruktioner. För att undvika svårigheter att bevisa att den personuppgiftsansvariges instruktioner är vederbörligen dokumenterade, rekommenderar EDPB att förvara dessa instruktioner tillsammans med avtalet eller den andra rättshandlingen.

119. Personuppgiftsbiträdets skyldighet att avstå från alla behandlingar som inte baseras på den personuppgiftsansvariges instruktioner gäller även **överföring** av personuppgifter till ett tredjeland eller en internationell organisation. Avtalet bör specificera kraven för överföringar till tredjeländer eller internationella organisationer, med beaktande av bestämmelserna i kapitel V i GDPR.

120. EDPB rekommenderar att den personuppgiftsansvarige ägnar vederbörlig uppmärksamhet åt denna specifika punkt, särskilt när personuppgiftsbiträdet ska delegera vissa behandlingsaktiviteter till andra personuppgiftsbiträden och när personuppgiftsbiträdet har avdelningar eller enheter i tredjeländer. Om instruktionerna från den personuppgiftsansvarige inte tillåter överföringar eller vidarebefordrande till tredjeländer får personuppgiftsbiträdet inte tilldela behandlingen till ett underbiträde i ett tredjeland, och han får inte heller behandla uppgifterna i någon av sina avdelningar utanför EU.

121. Ett personuppgiftsbiträde kan behandla andra uppgifter än i enlighet med dokumenterade instruktioner från den personuppgiftsansvarige **när personuppgiftsbiträdet måste behandla och/eller överföra personuppgifter på grundval av EU-lagstiftning eller lagstiftningen för den medlemsstat som personuppgiftsbiträdet omfattas av**. Denna bestämmelse avslöjar vidare vikten av att noggrant förhandla fram och utarbeta databehandlingsavtal, eftersom till exempel juridisk rådgivning kan behöva sökas av endera parten angående förekomsten av sådana lagkrav. Detta måste göras i tid, eftersom personuppgiftsbiträdet har en skyldighet att informera den personuppgiftsansvarige om detta krav innan behandlingen påbörjas. Endast när samma lagstiftning (unionsrätten eller medlemsstaternas nationella rätt) förbjuder personuppgiftsbiträdet att informera den personuppgiftsansvarige om ”viktiga allmänintressen”, finns det ingen sådan informationsskyldighet. Under alla omständigheter får överföring eller vidarebefordrande endast ske om det är tillåtet enligt unionsrätten, inklusive i enlighet med artikel 48 i GDPR.

1.3.2 Personuppgiftsbiträdet måste säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt (artikel 28.3 b i GDPR)

122. Avtalet måste ange att personuppgiftsbiträdet är skyldig att se till att alla som ges tillåtelse att behandla personuppgifterna har tystnadsplikt. Detta kan ske antingen via ett specifikt avtal eller på grund av lagstadgade skyldigheter som redan finns.

123. Det breda begreppet ”personer med behörighet att behandla personuppgifterna” inkluderar anställda och tillfälligt anställda. Generellt sett bör personuppgiftsbiträdet endast göra personuppgifterna

[53] Se del II, underavsnitt 1.5 (”Personuppgiftsbiträdet fastställer ändamål och medel för behandlingen”).

tillgängliga för de anställda som i praktiken behöver dem för att utföra uppgifter för vilka personuppgiftsbiträdet anlitades av den personuppgiftsansvarige.

124. Åtagandet eller skyldigheten för tystnadsplikt måste vara ”lämplig”, det vill säga den måste i praktiken förbjuda den behöriga personen att avslöja konfidentiell information utan tillstånd, och den måste vara tillräckligt bred för att omfatta alla personuppgifter som behandlas för den personuppgiftsansvariges räkning, såväl som villkoren för vilka personuppgifterna behandlas.

1.3.3 Personuppgiftsbiträdet måste vidta alla åtgärder som krävs enligt artikel 32 (artikel 28.3 c i GDPR)

125. Enligt artikel 32 måste den personuppgiftsansvarige och personuppgiftsbiträdet implementera lämpliga tekniska och organisatoriska säkerhetsåtgärder. Även om denna skyldighet redan åläggs ett personuppgiftsbiträde vars behandling faller inom tillämpningsområdet för GDPR, måste skyldigheten att vidta alla åtgärder som krävs enligt artikel 32 fortfarande återspeglas i avtalet angående behandlingsaktiviteter som den personuppgiftsansvarige har anförtrott.

126. Som har nämnts tidigare bör behandlingsavtalet inte bara återupprepa bestämmelserna i GDPR. Avtalet måste innehålla eller hänvisa till information om de säkerhetsåtgärder som ska vidtas, **en skyldighet för personuppgiftsbiträdet att erhålla den personuppgiftsansvariges godkännande innan ändringar görs** och en regelbunden översyn av säkerhetsåtgärderna för att säkerställa att de är lämpliga med avseende på risker som kan utvecklas med tiden. Detaljgraden för informationen angående de säkerhetsåtgärder som ska ingå i avtalet måste vara sådan att den personuppgiftsansvarige kan bedöma om åtgärderna är lämpliga enligt artikel 32.1 i GDPR. Dessutom är beskrivningen också nödvändig för att göra det möjligt för den personuppgiftsansvarige att uppfylla sin ansvarsskyldighet enligt artikel 5.2 och artikel 24 i GDPR vad gäller de säkerhetsåtgärder som åläggs personuppgiftsbiträdet. En motsvarande skyldighet för personuppgiftsbiträdet att bistå den personuppgiftsansvarige och tillgängliggöra all information som är nödvändig för att påvisa överensstämmelse kan utläsas av artikel 28.3 f och h i GDPR.

127. Instruktionsnivån som den personuppgiftsansvarige tillhandahåller personuppgiftsbiträdet om de åtgärder som ska implementeras beror på de specifika omständigheterna. I vissa fall kan den personuppgiftsansvarige tillhandahålla en tydlig och detaljerad beskrivning av de säkerhetsåtgärder som ska implementeras. I andra fall kan den personuppgiftsansvarige beskriva de minimisäkerhetsmål som ska uppnås, samtidigt som man ber personuppgiftsbiträdet att föreslå implementering av specifika säkerhetsåtgärder. Under alla omständigheter måste den personuppgiftsansvarige förse personuppgiftsbiträdet med en beskrivning av behandlingarna och säkerhetsmålen (baserat på den personuppgiftsansvariges riskbedömning), samt godkänna de åtgärder som personuppgiftsbiträdet föreslår. Detta kan inkluderas i en bilaga till avtalet. Den personuppgiftsansvarige utövar sin beslutanderätt över huvuddragen i säkerhetsåtgärderna, antingen genom att uttryckligen förteckna åtgärderna eller genom att godkänna dem som föreslagits av personuppgiftsbiträdet.

1.3.4 Personuppgiftsbiträdet måste respektera de villkor som avses i artiklarna 28.2 och 28.4 för anlitandet av ett annat personuppgiftsbiträde (artikel 28.3 d i GDPR).

128. Avtalet måste specificera att personuppgiftsbiträdet inte får anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. I händelse av ett allmänt tillstånd måste personuppgiftsbiträdet informera den personuppgiftsansvarige om alla ändringar vad gäller underbiträden genom ett skriftligt tillstånd och ge personuppgiftsbiträdet möjlighet att motsätta sig. Det rekommenderas att avtalet specificerar

processen för detta. Det bör noteras att personuppgiftsbiträdets skyldighet att informera den personuppgiftsansvarige om eventuella ändringar av underbiträden innebär att personuppgiftsbiträdet aktivt delger eller flaggar sådana ändringar gentemot den personuppgiftsansvarige.[54] Om särskilt tillstånd krävs, bör avtalet också beskriva processen för att inhämta ett sådant tillstånd.

129. När personuppgiftsbiträdet anlitar ett annat personuppgiftsbiträde måste ett avtal ingås mellan dem, som ålägger samma dataskyddskrav som de som åläggs det ursprungliga personuppgiftsbiträdet eller måste dessa skyldigheter åläggas genom en annan rättsakt enligt unionens eller medlemsstatens lagstiftning (se även punkt 160 nedan). Detta inbegriper skyldigheten i enlighet med artikel 28.3 h att tillåta och bidra till granskningar som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.[55] Personuppgiftsbiträdet är ansvarigt gentemot den personuppgiftsansvarige för de andra personuppgiftsbiträdenas efterlevnad av dataskyddskrav (för mer information om rekommenderat innehåll i avtalet, se underavsnitt 1.6 nedan[56]).

1.3.5 Personuppgiftsbiträdet måste hjälpa den personuppgiftsansvarige så att denne kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter (artikel 28.3 e GDPR).

130. Även om det är upp till den personuppgiftsansvarige att säkerställa att de registrerade personernas förfrågningar hanteras, måste avtalet föreskriva att den registeransvarige är skyldig att tillhandahålla hjälp ”genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt”. Hjälpens karaktär kan variera mycket ”med tanke på behandlingens art” och beroende på vilken typ av verksamhet som anförtros personuppgiftsbiträdet. Information om vilken hjälp som personuppgiftsbiträdet ska tillhandahålla bör anges i avtalet eller i en bilaga till detta.

131. Även om hjälpen helt enkelt kan bestå i att vidarebefordra alla mottagna förfrågningar och/eller göra det möjligt för den personuppgiftsansvarige att direkt extrahera och hantera relevanta personuppgifter, kommer personuppgiftsbiträdet under vissa omständigheter att få mer specifika, tekniska uppgifter, särskilt när personuppgiftsbiträdet är i position att extrahera och hantera personuppgifterna.

132. Det är avgörande att komma ihåg att även om den praktiska hanteringen av enskilda förfrågningar kan läggas ut på personuppgiftsbiträdet, bär den personuppgiftsansvarige ansvaret för att efterleva sådana förfrågningar. Därför bör bedömningen av huruvida förfrågningar från registrerade är tillåtna och/eller om de krav som ställs i GDPR efterlevs utföras av den personuppgiftsansvarige, antingen från fall till fall eller genom tydliga instruktioner som tillhandahålls personuppgiftsbiträdet i avtalet innan behandlingen påbörjas. De tidsfrister som anges i kapitel III kan inte förlängas av den personuppgiftsansvarige på grundval av att den nödvändiga informationen måste tillhandahållas av personuppgiftsbiträdet.

[54] I detta avseende är det däremot exempelvis inte tillräckligt för personuppgiftsbiträdet att bara ge den personuppgiftsansvarige allmän tillgång till en förteckning över underbiträden som kan uppdateras då och då, utan att peka på varje planerat nytt underbiträde. Med andra ord måste personuppgiftsbiträdet aktivt informera den personuppgiftsansvarige om alla ändringar i listan (dvs. i synnerhet varje nytt planerat underbiträde).

[55] Se även EDPB:s yttrande 14/2019 angående utkastet till standardavtalsklausuler, inlämnat av den danska tillsynsmyndigheten (artikel 28.8 i GDPR), den 9 juli 2019, punkt 44.

[56] Se del II, underavsnitt 1.6 (”Underbiträden”).

1.3.6 Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs (artikel 28.3 f i GDPR).

133. Det är nödvändigt att avtalet undviker att bara återupprepa dessa hjälpskyldigheter: **avtalet bör innehålla uppgifter om hur personuppgiftsbiträdet ombeds hjälpa den personuppgiftsansvarige att uppfylla de angivna skyldigheterna**. Till exempel kan procedurer och mallformulär läggas till i bilagorna till avtalet, så att personuppgiftsbiträdet kan förse den personuppgiftsansvarige med all nödvändig information.

134. Typen och graden av assistans som personuppgiftsbiträdet ska tillhandahålla kan variera kraftigt ”*med hänsyn till behandlingens art och informationen som personuppgiftsbiträdet har tillgång till*”. Den personuppgiftsansvarige måste informera personuppgiftsbiträdet på ett adekvat sätt om riskerna i behandlingen och om andra omständigheter som kan hjälpa personuppgiftsbiträdet att uppfylla sin plikt.

135. När det gäller de specifika skyldigheterna har personuppgiftsbiträdet till att börja med en plikt att hjälpa den personuppgiftsansvarige att uppfylla förpliktelsen att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa behandlingssäkerheten.[57] Även om detta i viss utsträckning kan överlappa kravet på att personuppgiftsbiträdet själv vidtar adekvata säkerhetsåtgärder där behandlingsverksamheten faller inom tillämpningsområdet för GDPR, förblir det två distinkta skyldigheter, eftersom den ena avser personuppgiftsbiträdets egna åtgärder och den andra hänvisar till den personuppgiftsansvariges.

136. För det andra måste personuppgiftsbiträdet hjälpa den personuppgiftsansvarige att uppfylla skyldigheten att meddela överträdelser av dataintrång till tillsynsmyndigheten och till de registrerade personerna. Personuppgiftsbiträdet måste meddela den personuppgiftsansvarige närhelst man upptäcker ett dataintrång som påverkar personuppgiftsbiträdets eller en underbiträdets anläggningar/it-system och hjälpa den personuppgiftsansvarige att sammanställa den information som måste anges i rapporten till tillsynsmyndigheten.[58] GDPR kräver att den personuppgiftsansvarige meddelar ett intrång utan onödigt dröjsmål för att minimera skadan för individer och för att maximera möjligheten att hantera överträdelsen på ett adekvat sätt. Därför bör personuppgiftsbiträdet även meddela den personuppgiftsansvarige utan onödigt dröjsmål.[59] Beroende på de specifika egenskaperna hos behandlingen som anförtrotts personuppgiftsbiträdet kan det vara lämpligt för parterna att inkludera en specifik tidsram (t.ex. antal timmar) i avtalet inom vilken personuppgiftsbiträdet ska meddela den registeransvarige, såväl som kontaktpunkten för sådana aviseringar, modalitet och minimiinnehåll som förväntas av den personuppgiftsansvarige.[60] Avtalsarrangemanget mellan den personuppgiftsansvarige och personuppgiftsbiträdet kan också innehålla ett tillstånd och ett krav för personuppgiftsbiträdet att direkt meddela ett dataintrång i enlighet med artiklarna 33 och 34, men det juridiska ansvaret för anmälan ligger hos den personuppgiftsansvarige.[61] Om personuppgiftsbiträdet meddelar ett dataintrång direkt till tillsynsmyndigheten och informerar de registrerade personerna i enlighet med artiklarna 33 och 34,

[57] Artikel 32 i GDPR.
[58] Artikel 33.3 i GDPR.
[59] För ytterligare information, se riktlinjerna angående avisering av dataintrång under förordning 2016/679, WP 250 rev. 01, den 6 februari 2018, s. 13–14.
[60] Se även EDPB:s yttrande 14/2019 om utkastet till standardavtalsklausuler, inlämnat av den danska tillsynsmyndigheten (artikel 28.8 i GDPR), den 9 juli 2019, punkt 40.
[61] Riktlinjer angående avisering av dataintrång under förordning 2016/679, WP 250rev.01, den 6 februari 2018, s. 14.

måste personuppgiftsbiträdet även informera den personuppgiftsansvarige och förse denne med kopior av anmälan och information till de registrerade personerna.

137. Vidare måste personuppgiftsbiträdet också bistå den personuppgiftsansvarige med att utföra konsekvensanalyser av dataskydd vid behov, och att konsultera tillsynsmyndigheten när resultatet visar att det finns en hög risk som inte kan mildras.

138. Biståndsplikten innebär inte en ansvarsförskjutning, eftersom dessa skyldigheter åläggs den personuppgiftsansvarige. Till exempel, även om konsekvensanalysen för dataskyddet i praktiken kan utföras av ett personuppgiftsbiträde, ansvarar den personuppgiftsansvarige för skyldigheten att utföra bedömningen[62] och personuppgiftsbiträdet är bara skyldigt att bistå den personuppgiftsansvarige ”vid behov och på begäran”.[63] Som ett resultat är det den personuppgiftsansvarige som måste ta initiativet att utföra konsekvensanalysen för dataskyddet, inte personuppgiftsbiträdet.

1.3.7 När behandlingen har avslutats måste personuppgiftsbiträdet, beroende på vad den personuppgiftsansvarige väljer, radera eller återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior (artikel 28.3 g i GDPR).

139. Avtalsvillkoren är avsedda att säkerställa att personuppgifterna är föremål för lämpligt skydd när ”tillhandahållandet av behandlingstjänster” har avslutats. Det är därför upp till den personuppgiftsansvarige att avgöra vad personuppgiftsbiträdet ska göra med personuppgifterna.

140. Den personuppgiftsansvarige kan i början avgöra huruvida personuppgifterna ska raderas eller återlämnas genom att ange detta i avtalet, genom ett skriftligt meddelande som i rimlig tid skickas till personuppgiftsbiträdet. Avtalet eller annan rättsakt bör återspegla möjligheten för den personuppgiftsansvarige att ändra det detta val innan tillhandahållandet av behandlingstjänster har avslutats. Avtalet bör specificera proceduren för tillhandahållandet av sådana instruktioner.

141. Om den personuppgiftsansvarige väljer att personuppgifterna ska raderas, bör personuppgiftsbiträdet säkerställa att raderingen utförs på ett säkert sätt som också är förenligt med artikel 32 i GDPR. Personuppgiftsbiträdet bör bekräfta för den personuppgiftsansvarige att raderingen har slutförts inom en överenskommen tidsperiod och på ett överenskommet sätt.

142. Personuppgiftsbiträdet måste radera alla befintliga kopior av uppgifterna, såvida inte EU:s eller medlemsstatens lagstiftning kräver ytterligare lagring. Om personuppgiftsbiträdet eller den personuppgiftsansvarige är medveten om sådana lagkrav, bör man informera den andra parten så snart som möjligt.

1.3.8 Personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i artikel 28 har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige (artikel 28.3 h i GDPR).

143. Avtalet ska innehålla uppgifter om hur ofta och hur informationsflödet mellan personuppgiftsbiträdet och den personuppgiftsansvarige ska löpa, så att den personuppgiftsansvarige är fullständigt informerad om vilka uppgifter avseende behandlingen som är relevanta för att visa överensstämmelse

[62] Artikel 29-arbetsgruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, WP 248 rev. 01, s. 14

[63] Skäl 95 i GDPR.

med de skyldigheter som anges i artikel 28 i GDPR. 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.

144. Ytterligare uppgifter ska också anges i avtalet avseende förmågan att utföra och skyldigheten att bidra till inspektioner och revisioner av den personuppgiftsansvarige eller annan revisor på uppdrag av den personuppgiftsansvarige.

GDPR anger att inspektioner och revisioner utförs av den personuppgiftsansvarige eller av en tredje part på uppdrag av den personuppgiftsansvarige. 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. Personuppgiftsbiträdet kan föreslå val av en specifik revisor, men det slutliga beslutet måste överlåtas till den personuppgiftsansvarige enligt artikel 28.3 h i GDPR.[64] Även om inspektionen utförs av en revisor som föreslagits av personuppgiftsbiträdet, behåller den personuppgiftsansvarige rätten att bestrida inspektionens omfattning, metodik och resultat.[65]

Parterna bör samarbeta i god tro och bedöma om och när det är nödvändigt att utföra revisioner i personuppgiftsbiträdets lokaler, liksom vilken typ av revision eller inspektion (på distans/på plats/på annat sätt samla in den nödvändiga informationen) som skulle behövas och vara lämplig i det specifika fallet, även med hänsyn till säkerhetskraven. Det slutliga beslutet angående detta bör fattas av den personuppgiftsansvarige. Utifrån resultaten av inspektionen ska den personuppgiftsansvarige kunna be personuppgiftsbiträdet att vidta efterföljande åtgärder, t.ex. att korrigera brister och luckor som identifierats.[66] På samma sätt bör specifika förfaranden fastställas beträffande personuppgiftsbiträdets och den personuppgiftsansvariges inspektion av underbiträden (se underavsnitt 1.6 nedan[67]).

145. Frågan om kostnadsfördelning mellan en personuppgiftsansvarig och ett personuppgiftsbiträde rörande revisioner omfattas inte av GDPR och är föremål för kommersiella överväganden. I artikel 28.3 h krävs dock att avtalet innehåller en skyldighet för personuppgiftsbiträdet att tillgängliggöra all information som krävs för den personuppgiftsansvarige och en skyldighet att tillåta och bidra till revisioner, inklusive inspektioner, utförda av den personuppgiftsansvarige eller en annan revisor på uppdrag av den personuppgiftsansvarige. Detta innebär i praktiken att parterna inte ska infoga klausuler i avtalet som avser betalning av kostnader eller avgifter som skulle vara uppenbart oproportionerliga eller överdrivna och därmed ha en avskräckande effekt på någon av parterna. Sådana klausuler skulle verkligen innebära att de rättigheter och skyldigheter som anges i artikel 28.3 h aldrig skulle utövas i praktiken och skulle bli rent teoretiska trots att de utgör en integrerad del av de dataskyddsåtgärder som föreskrivs i artikel 28 i GDPR.

[64] Se EDPB-EDPS gemensamma yttrande 1/2021 angående standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden, punkt 43.
[65] Se yttrande 14/2019 om utkastet till standardavtalsklausuler inlämnat av den danska tillsynsmyndigheten (artikel 28.8 i GDPR), punkt 43.
[66] Se yttrande 14/2019 om utkastet till standardavtalsklausuler som lämnats in av den danska tillsynsmyndigheten (artikel 28.8 i GDPR), punkt 43.
[67] Se del II, underavsnitt 1.6 (”Underbiträden”).

1.4 Instruktioner som bryter mot dataskyddslagarna

146. Enligt artikel 28.3 ska personuppgiftsbiträdet omedelbart informera den personuppgiftsansvarige om han anser att en instruktion strider mot GDPR eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

147. Personuppgiftsbiträdet har en skyldighet att följa den personuppgiftsansvariges instruktioner, men även en allmän skyldighet att följa lagen. En instruktion som bryter mot dataskyddslagstiftningen verkar orsaka en konflikt mellan de ovannämnda två skyldigheterna.

148. Efter att ha informerats om att en av deras instruktioner kan bryta mot dataskyddslagstiftningen måste den personuppgiftsansvarige bedöma situationen och avgöra om instruktionen verkligen bryter mot dataskyddslagarna.

149. EDPB rekommenderar parterna att i avtalet förhandla fram och komma överens om konsekvenserna av aviseringen om en otillåten instruktion som skickas av personuppgiftsbiträdet och i händelse av passivitet från den personuppgiftsansvariges sida i detta sammanhang. Ett exempel skulle vara att infoga en klausul om uppsägning av avtalet om den personuppgiftsansvarige insisterar med en olaglig instruktion. Ett annat exempel skulle vara en klausul om möjligheten för personuppgiftsbiträdet att avbryta implementeringen av den berörda instruktionen tills den personuppgiftsansvarige bekräftar, ändrar eller drar tillbaka sin instruktion[68].

1.5 När personuppgiftsbiträdet fastställer ändamål och medel för behandlingen

150. Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig i fråga om den behandlingen (artikel 28.10 i GDPR).

1.6 Underbiträden

151. 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 (se ovanstående punkt 83).

152. Även om kedjan kan vara ganska lång, behåller den personuppgiftsansvarige sin avgörande roll vad gäller bestämmande av behandlingsändamål och behandlingssätt. I artikel 28.2 i GDPR föreskrivs att personuppgiftsbiträdet inte får anlita ett annat personuppgiftsbiträde utan föregående specifikt eller allmänt skriftligt tillstånd från den personuppgiftsansvarige (inklusive i elektroniskt format). Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet alltid informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. I båda fallen måste personuppgiftsbiträdet inhämta den personuppgiftsansvariges skriftliga tillstånd innan någon personuppgiftsbehandling överlåts till underbiträdet. För 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

[68] Se EDPB-EDPS gemensamma yttrande 1/2021 angående standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden, punkt 39.

bevis på vilka skyddsåtgärder som har genomförts) överlämnas till den personuppgiftsansvarige av personuppgiftsbiträdet.[69]

153. Det föregående skriftliga tillståndet kan vara specifikt, det vill säga hänvisa till ett specifikt underbiträde för en specifik behandlingsaktivitet och vid en specifik eller generell tidpunkt. Detta kan specificeras i avtalet eller en annan rättsakt som styr behandlingen.

154. I händelse av att den personuppgiftsansvarige beslutar sig för att acceptera vissa underbiträden vid tidpunkten för avtalets undertecknande, bör en lista över godkända underbiträden ingå i avtalet eller en bilaga till detta. Listan bör därefter hållas uppdaterad i enlighet med det allmänna eller specifika tillstånd som ges av den personuppgiftsansvarige.

155. Om den personuppgiftsansvarige väljer att ge sitt **specifika tillstånd** måste denne skriftligen ange vilket underbiträde och vilken behandlingsaktivitet som hänvisas till. Varje efterföljande ändring måste godkännas på nytt av den personuppgiftsansvarige innan den träder i kraft. Om personuppgiftsbiträdets begäran om ett specifikt godkännande inte besvaras inom den angivna tidsramen, bör det anses som nekat. Den personuppgiftsansvarige bör fatta sitt beslut om att bevilja eller neka sitt godkännande med beaktande av sin skyldighet att endast använda personuppgiftsbiträden som tillhandahåller ”tillräckliga garantier” (se underavsnitt 1.1 ovan[70]).

156. Alternativt kan den personuppgiftsansvarige ge sitt **allmänna tillstånd** för användning av underbiträden (i avtalet, kompletterat med en lista över sådana underbiträden i en bifogad bilaga), som bör kompletteras med kriterier för att styra personuppgiftsbiträdets valalternativ (t.ex. garantier när det gäller tekniska och organisatoriska åtgärder, expertkunskap, tillförlitlighet och resurser).[71] I detta fall måste personuppgiftsbiträdet i god tid informera den personuppgiftsansvarige om alla avsedda tillägg eller utbyten av underbiträden för att ge den personuppgiftsansvarige möjlighet att invända.

157. Därför ligger den största skillnaden mellan det specifika tillståndet och scenarierna för ett allmänt tillstånd i innebörden som ges till den personuppgiftsansvariges tystnad: i fallet för ett allmänt tillstånd kan den personuppgiftsansvariges underlåtenhet att invända inom den angivna tidsramen tolkas som ett godkännande.

158. I båda fallen bör avtalet innehålla detaljer om tidsramen för den personuppgiftsansvariges godkännande eller invändning och hur parterna tänker kommunicera angående detta ämne (t.ex. mallar). En sådan tidsram måste vara rimlig mot bakgrund av typen av behandling, komplexiteten i de aktiviteter som anförtrotts personuppgiftsbiträdet (och underbiträdena) och förhållandet mellan parterna. Dessutom bör avtalet innehålla detaljer om de praktiska stegen efter den personuppgiftsansvariges invändande (t.ex. genom att ange tidsramen inom vilken den personuppgiftsansvarige och personuppgiftsbiträdet ska besluta om behandlingen ska avslutas).

159. Oavsett de kriterier som den personuppgiftsansvarige föreslår för att välja leverantörer, är personuppgiftsbiträdet fortfarande fullt ansvarigt gentemot den personuppgiftsansvarige för

[69] Denna information behövs så att den personuppgiftsansvarige kan efterleva ansvarsprincipen enligt artikel 24 och bestämmelserna i artiklarna 28.1, 32 och kapitel V i GDPR.
[70] Se del II – underavsnitt 1.1 (”Personuppgiftsbiträdets val”).
[71] Den personuppgiftsansvariges skyldighet härrör från ansvarighetsprincipen i artikel 24 och skyldigheten att följa bestämmelserna i artiklarna 28.1, 32 och kapitel V i GDPR.

utförandet av underbiträdenas skyldigheter (artikel 28.4 i GDPR). Därför bör personuppgiftsbiträdet föreslå underbiträden som kan tillhandahålla tillräckliga garantier.

160. Vidare, när ett personuppgiftsbiträde har för avsikt att anställa ett (godkänt) underbiträde, måste denne ingå ett avtal med underbiträdet som ålägger samma skyldigheter som de som åläggs det primära personuppgiftsbiträdet av den personuppgiftsansvarige eller måste skyldigheterna åläggas genom en annan rättsakt enligt EU:s eller medlemsstaternas lagstiftning. Hela kedjan av behandlingsaktiviteter måste regleras genom skriftliga avtal. 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. Detta innebär också att om personuppgiftsbiträdet har anförtrott underbiträdet med en specifik del av behandlingen som vissa av skyldigheterna inte kan gälla för, bör sådana skyldigheter inte inkluderas ”som standard” i avtalet med underbiträdet, eftersom detta skulle bara skapa osäkerhet. Som ett exempel, när det gäller hjälp med dataintrångsrelaterade skyldigheter, kan underrättelse om ett dataintrång av ett underbiträde göras direkt till den personuppgiftsansvarige om alla tre håller med. Vid sådan direktanmälan bör dock personuppgiftsbiträdet informeras och få en kopia av meddelandet.

2 KONSEKVENSER FÖR GEMENSAMT PERSONUPPGIFTSANSVAR

2.1 Att på ett öppet sätt fastställa respektive ansvarsområden för gemensamt personuppgiftsansvariga angående efterlevnad av skyldigheterna enligt GDPR

161. I artikel 26.1 i GDPR anges att gemensamt personuppgiftsansvariga på ett öppet sätt ska fastställa och komma överens om sina respektive ansvarsområden för efterlevnad av förordningens krav.

162. Gemensamt personuppgiftsansvariga måste alltså klargöra ”vem som gör vad” genom att själva bestämma vem som ska utföra vilka uppgifter för att säkerställa att behandlingen uppfyller de tillämpliga kraven enligt GDPR i förhållande till den gemensamma behandlingen som saken gäller. Med andra ord ska ansvarsfördelningen för efterlevnad göras genom användning av termen ”*respektive*” i artikel 26.1. Detta utesluter inte det faktum att EU:s eller medlemsstaternas lagstiftning redan kan fastställa vissa ansvarsområden för respektive gemensamt personuppgiftsansvarig. Om så är fallet bör arrangemanget för gemensamt personuppgiftsansvar också behandla alla ytterligare ansvarsområden som är nödvändiga för att säkerställa att GDPR efterlevs som inte behandlas av lagbestämmelserna.[72]

163. Syftet med dessa regler är att säkerställa att ansvaret för efterlevnad av dataskyddsreglerna när flera aktörer är involverade, särskilt i komplexa databehandlingsmiljöer, tydligt fördelas för att undvika att skyddet av personuppgifter reduceras eller att en negativ kompetenskonflikt leder till kryphål där vissa skyldigheter inte efterlevs av någon av parterna som är involverade i behandlingen. Det bör klargöras här att allt ansvar måste fördelas enligt de faktiska omständigheterna för att uppnå ett operativt avtal. EDPB konstaterar att det uppstår situationer där inflytandet från en gemensam personuppgiftsansvarig och dennes faktiska inflytande försvårar uppnåendet av ett avtal. Dessa

[72] ”I vilket fall som helst bör anordnandet av det gemensamma personuppgiftsansvaret omfatta alla ansvarsområden för de gemensamt personuppgiftsansvariga, inklusive de som redan kan ha fastställts i den relevanta EU-lagstiftningen eller medlemsstatslagstiftningen och utan att det påverkar skyldigheten för gemensamt personuppgiftsansvariga att tillhandahålla kärnan i det gemensamma personuppgiftsansvaret i enlighet med artikel 26.2 i GDPR.”

omständigheter förnekar dock inte det gemensamma personuppgiftsansvaret och kan inte användas för att befria någon av parterna från sina skyldigheter enligt GDPR.

164. Närmare bestämt anges det i artikel 26.1 att fastställandet av deras respektive ansvar (dvs. uppgifter) för att uppfylla skyldigheterna enligt GDPR ska utföras av gemensamt personuppgiftsansvariga ”*i synnerhet*” när det gäller utövandet av rättigheterna för de registrerade personerna och skyldigheterna att lämna den information som avses i artiklarna 13 och 14, såvida inte och i den mån de respektive ansvarsområdena för de personuppgiftsansvariga bestäms av unionsrätten eller den medlemsstatslagstiftning som de personuppgiftsansvariga omfattas av.

165. Det framgår klart av denna bestämmelse att gemensamt personuppgiftsansvariga måste definiera vem som ska ha ansvaret för att besvara förfrågningar när registrerade personer utövar sina rättigheter som beviljas av GDPR och tillhandahålla information till dem enligt kraven i artiklarna 13 och 14 i GDPR. Detta avser endast att i sitt inbördes förhållande definiera vilken av parterna som är skyldig att svara på vilka registrerade personers förfrågningar. . Oavsett någon sådan fördelning kan den registrerade personen kontakta endera av de gemensamt personansvariga i enlighet med artikel 26.3 i GPDR. Användningen av termen ”*i synnerhet*” anger emellertid att de skyldigheter som är föremål för ansvarsfördelningen för efterlevnad av varje inblandad part enligt denna bestämmelse inte är uttömmande. Av detta följer att fördelningen av ansvaret för efterlevnad mellan gemensamt personuppgiftsansvariga inte är begränsad till de ämnen som anges i artikel 26.1 utan sträcker sig till andra skyldigheter för personuppgiftsansvariga enligt GDPR. Gemensamt personuppgiftsansvariga måste se till att hela den gemensamma behandlingen helt överensstämmer med GDPR.

166. I detta perspektiv bör överensstämmelseåtgärderna och tillhörande skyldigheter som gemensamt personuppgiftsansvariga bör beakta när de bestämmer sina respektive ansvarsområden, utöver de som specifikt anges i artikel 26.1, bland annat omfatta, utan begränsning:

- Implementering av de allmänna dataskyddsprinciperna (artikel 5)
- Juridisk grund för behandlingen[73] (artikel 6)
- Säkerhetsåtgärder (artikel 32)
- Anmälan om dataintrång till tillsynsmyndigheten och den registrerade personen[74] (artiklarna 33 och 34)
- Konsekvensanalys för dataskydd (artiklarna 35 och 36)[75]

[73] Även om GDPR inte hindrar gemensamt personuppgiftsansvariga från att använda olika juridiska grunder för olika behandlingsoperationer som de utför, rekommenderas det att när det är möjligt använda samma juridiska grund för ett visst syfte.

[74] Se även EDPB: s riktlinjer för anmälan om dataintrång i anslutning till personuppgifter enligt förordning 2016/679, WP 250 rev. 01 som föreskriver att gemensamt personuppgiftsansvar ska inkludera ”*att avgöra vilken part som kommer att ha ansvar för att uppfylla skyldigheterna enligt artiklarna 33 och 34. WP 29 rekommenderar att avtalsarrangemangen mellan gemensamt personuppgiftsansvariga innehåller bestämmelser som avgör vilken personuppgiftsansvarig som ska ta leda, eller ansvara för, efterlevnaden av GDPR:s skyldigheter att anmäla brott*” (s. 13).

[75] Se även EDPB:s riktlinjer för konsekvensanalys för dataskydd, WP 248 rev. 01 som innehåller följande: ”*När behandlingsoperationen involverar gemensamt personuppgiftsansvariga, måste de definiera sina respektive skyldigheter på ett precist sätt. Deras konsekvensanalys för dataskydd bör fastställa vilken part som ansvarar för de olika åtgärder som syftar till att hantera risker och skydda de registrerade personernas rättigheter och friheter. Varje personuppgiftsansvarig bör uttrycka sina behov och dela användbar information utan att varken*

- Användning av ett personuppgiftsbiträde (artikel 28)
- Överföring av uppgifter till tredjeland (kapitel V)
- Organisation av kontakt med registrerade personer och tillsynsmyndigheter

167. Andra ämnen som kan övervägas beroende på vilken behandling som saken gäller och parternas avsikter är till exempel begränsningarna i användningen av personuppgifter för ett annat ändamål av en av de gemensamt personuppgiftsansvariga. I detta avseende har båda de personuppgiftsansvariga alltid skyldigheten att säkerställa att de båda har en juridisk grund för behandlingen. I samband med gemensamt personuppgiftsansvar delas inland personuppgifter mellan de personuppgiftsansvariga. Varje gemensamt personuppgiftsansvarig är skyldig att säkerställa att informationen inte vidarebehandlas på ett sätt som är inkompatibelt med ändamålet för vilket informationen ursprungligen samlades in av den personuppgiftsansvarige som delar informationen.[76]

168. Gemensamt personuppgiftsansvariga kan ha en viss grad av flexibilitet vad gäller fördelning och tilldelning av skyldigheter mellan parterna, så länge som man säkerställer fullständig efterlevnad av GDPR för behandlingen i fråga. Tilldelningen bör ta hänsyn till faktorer som vem som är kompetent och i stånd att effektivt säkerställa de registrerade personernas rättigheter samt uppfylla relevanta skyldigheter enligt GDPR. EDPB rekommenderar att de relevanta faktorerna och den interna analysen som utförs dokumenteras för att fördela de olika skyldigheterna. Denna analys är en del av dokumentationen enligt ansvarsprincipen.

169. Skyldigheterna behöver inte vara jämnt fördelade mellan de gemensamt personuppgiftsansvariga. I detta avseende har EU-domstolen nyligen konstaterat att ”*förekomsten av gemensamt ansvar innebär inte nödvändigtvis lika ansvar för de olika operatörer som är involverade i behandlingen av personuppgifter*”.[77] Det kan dock finnas fall där inte alla skyldigheter kan fördelas och alla gemensamt personuppgiftsansvariga kan behöva följa samma krav som följer av GDPR, med beaktande av den gemensamma behandlingens natur och sammanhang. Till exempel måste gemensamt personuppgiftsansvariga som använder delade databehandlingsverktyg eller system både se till att principen för syftesbegränsning följs och införa lämpliga åtgärder för att upprätthålla säkerheten för personuppgifter som behandlas via de delade verktygen.

170. Ett annat exempel är kravet på att varje gemensamt personuppgiftsansvarig ska föra ett register över behandlingsaktiviteter eller utse ett dataskyddsombud om villkoren i artikel 37.1 är uppfyllda. Sådana krav är inte relaterade till den gemensamma behandlingen utan är tillämpliga på dem personuppgiftsansvariga.

2.2 Ansvarsfördelning måste ske genom ett arrangemang

2.2.1 Arrangemangets form

171. Artikel 26.1 i GDPR föreskriver som en ny skyldighet för gemensamt personuppgiftsansvariga att de ska bestämma sina respektive ansvarsområden ”*med hjälp av en överenskommelse mellan dem*”. Den

kompromissa med hemligheter (t.ex. skydd av företagshemligheter, immateriella rättigheter, konfidentiell affärsinformation) eller avslöja sårbarheter” (s. 7).

[76] Varje överföring från en personuppgiftsansvarig kräver en laglig grund och bedömning av kompatibilitet, oavsett om mottagaren är en separat personuppgiftsansvarig eller en gemensamt personuppgiftsansvarig. Med andra ord betyder förekomsten av ett gemensamt personuppgiftsansvar inte automatiskt att den gemensamt personuppgiftsansvarige som tar emot uppgifterna också lagligen kan behandla uppgifterna för ytterligare ändamål som ligger utanför ramen för gemensamt personuppgiftsansvar.

[77] Domslut i *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punkt 43.

juridiska formen för ett sådant arrangemang specificeras inte av GDPR. Därför står det gemensamt personuppgiftsansvariga fritt att komma överens om arrangemangets form.

172. Dessutom är arrangemanget om ansvarsfördelning bindande för var och en av de gemensamt personuppgiftsansvariga. De kommer överens och förbinder sig gentemot varandra om att ansvara för att respektera de respektive skyldigheter som anges i deras arrangemang som deras ansvar.

173. För rättssäkerhetens skull, även om det inte finns något lagstadgat krav i GDPR för ett avtal eller annan rättsakt, rekommenderar EDPB därför att en sådan överenskommelse görs i form av ett bindande dokument, som ett avtal eller annan juridiskt bindande handling under EU-lagstiftning eller medlemsstatslagstiftning som de personuppgiftsansvariga är underställda. Detta skulle skapa säkerhet och kan användas för att bevisa insyn och ansvar. I själva verket, i händelse av att den överenskomna tilldelningen i arrangemanget inte följs, gör dess bindande karaktär det möjligt för en personuppgiftsansvarig att kräva den andras ansvar för vad som anges i avtalet som faller under dennes ansvar. I enlighet med ansvarsskyldighetsprincipen kommer användningen av ett avtal eller en annan rättsakt även att göra det möjligt för gemensamt personuppgiftsansvariga att visa att de uppfyller de skyldigheter som åläggs dem av GDPR.

174. Hur ansvarsområden, det vill säga uppgifterna, fördelas mellan varje gemensamt personuppgiftsansvarig måste anges med ett klart och tydligt språk i arrangemanget.[78] Detta krav är viktigt eftersom det garanterar rättssäkerheten och undviker eventuella konflikter, inte bara i förhållandet mellan de gemensamt personuppgiftsansvariga, utan även gentemot de registrerade personerna och dataskyddsmyndigheterna.

175. För att bättre utforma ansvarsfördelningen mellan parterna rekommenderar EDPB att arrangemanget också ger allmän information om den gemensamma behandlingen genom att särskilt ange ämnet och ändamålet med behandlingen, typen av personuppgifter och kategorierna av registrerade personer.

2.2.2 Skyldigheter gentemot registrerade personer

176. GDPR stipulerar flera skyldigheter för gemensamt personuppgiftsansvariga gentemot registrerade personer:

Arrangemanget ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot de registrerade personerna.

177. Som ett komplement till vad som förklaras ovan i avsnitt 2.1 i de här riktlinjerna är det viktigt att de gemensamt personuppgiftsansvariga i arrangemanget förtydligar sina respektive roller, ”*särskilt*” när det gäller utövandet av den registrerade personens rättigheter och deras skyldigheter att lämna ut den information som avses i artiklarna 13 och 14. I artikel 26 i GDPR betonas vikten av dessa specifika skyldigheter. De gemensamt personuppgiftsansvariga måste därför organisera och komma överens om hur och av vem informationen kommer att tillhandahållas och hur och av vem svaren på de registrerade personernas förfrågningar kommer att tillhandahållas. Oavsett innehållet i arrangemanget angående denna specifika punkt, kan den registrerade personen kontakta någon av de gemensamt personuppgiftsansvariga för att utöva sina rättigheter i enlighet med artikel 26.3, vilket förklaras ytterligare nedan.

[78] Som anges i skäl 79 i GDPR ”*(...) de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar, även i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga*”.

178. Hur dessa skyldigheter organiseras i arrangemanget bör vara ”*vederbörligen*”, dvs. korrekt återspegla verkligheten i den underliggande gemensamma behandlingen. Till exempel, om bara en av de gemensamt personuppgiftsansvariga kommunicerar med de registrerade personerna i anslutning till den gemensamma behandlingen, kan en sådan personuppgiftsansvarig vara i bättre stånd att informera de registrerade personerna och eventuellt besvara på deras förfrågningar.

Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade personen

179. Denna bestämmelse syftar till att säkerställa att den registrerade personen är medveten om ”*arrangemangets väsentliga innehåll*”. Till exempel måste det vara helt klart för en registrerad person vilken personuppgiftsansvarig som fungerar som kontaktpunkt för utövandet av de registrerade personernas rättigheter (trots att han eller hon kan utöva sina rättigheter med avseende på och gentemot varje gemensamt personuppgiftsansvarig). Skyldigheten att göra det väsentliga i arrangemanget tillgängligt för registrerade personer är viktig vid gemensamt personuppgiftsansvar för att den registrerade personen ska veta vem av de personuppgiftsansvariga som ansvarar för vad.

180. Vad som bör omfattas av begreppet ”*det väsentliga i arrangemanget*” specificeras inte av GDPR. EDPB rekommenderar att det väsentliga omfattar åtminstone alla delar av den information som avses i artiklarna 13 och 14 som redan bör vara tillgängliga för den registrerade personen, och för vart och ett av dessa element bör arrangemanget specificera vilken gemensam personuppgiftsansvarig som ansvarar för att säkerställa överensstämmelse med dessa element. Det väsentliga i arrangemanget måste också ange kontaktpunkten, om en sådan är utsedd.

181. Hur sådan information ska göras tillgänglig för den registrerade personen specificeras inte. I motsats till andra bestämmelser i GDPR (t.ex. artikel 30.4 för registrering av behandling eller artikel 40.11 för registret över godkända uppförandekoder) anger artikel 26 inte att tillgängligheten varken ska vara ”*på begäran*” eller ”*offentligt tillgänglig på lämpligt sätt*”. Därför är det upp till de gemensamt personuppgiftsansvariga att besluta om det mest effektiva sättet att göra det väsentliga i arrangemanget tillgängligt för de registrerade personer (t.ex. tillsammans med informationen i artikel 13 eller 14, i integritetspolicyn eller på begäran till dataskyddsombudet, i förekommande fall, eller till den kontaktpunkt som kan ha utsetts). Gemensamt personuppgiftsansvariga bör se till att informationen tillhandahålls på ett konsekvent sätt.

Arrangemanget kan utse en kontaktpunkt för de registrerade personerna

182. Enligt artikel 26.1 har gemensamt personuppgiftsansvariga möjlighet att i arrangemanget utse en kontaktpunkt för registrerade personer. Detta är inte obligatoriskt.

183. Genom att bli informerad om ett enda sätt att kontakta potentiellt flera gemensamt personuppgiftsansvariga kan registrerade personer få reda på vem de kan kontakta när det gäller alla frågor som rör behandlingen av deras personuppgifter. Dessutom blir det möjligt för flera gemensamt personuppgiftsansvariga att på ett mera effektivt sätt samordna sina relationer och sin kommunikation gentemot registrerade personer.

184. Av dessa skäl, för att underlätta utövandet av de registrerade personernas rättigheter enligt GDPR, rekommenderar EDPB gemensamt personuppgiftsansvariga att utse en sådan kontaktpunkt.

185. Kontaktpunkten kan vara dataskyddsombudet, i förekommande fall, representanten inom EU (för gemensamt personuppgiftsansvariga som inte är etablerade inom EU) eller någon annan kontaktpunkt där information kan erhållas.

Oavsett villkoren i arrangemanget kan registrerade personer utöva sina rättigheter i anslutning till och mot vardera av de gemensamt personuppgiftsansvariga.

186. Enligt artikel 26.3 är en registrerad person inte bunden av villkoren i arrangemanget och kan utöva sina rättigheter enligt GDPR angående och gentemot var och en av de gemensamt personuppgiftsansvariga.

187. Till exempel, när det gäller gemensamt personuppgiftsansvariga som är etablerade i olika medlemsstater, eller om endast en av de gemensamt personuppgiftsansvariga är etablerade inom unionen, kan den registrerade personen, efter eget val, kontakta antingen den personuppgiftsansvarige som är etablerad i sin medlemsstat eller dennes vanliga bostad eller arbetsplats, eller den personuppgiftsansvarige som är etablerad någon annanstans inom EU eller EES.

188. Även om arrangemanget och det tillgängliga väsentliga innehållet i detta anger en kontaktpunkt för att ta emot och hantera alla registrerade personers förfrågningar, kan de registrerade personernas själva fortfarande välja något annat.

189. Därför är det viktigt att gemensamt personuppgiftsansvariga i förväg organiserar hur de kommer att hantera svar på förfrågningar de tar emot från registrerade personer. I detta avseende rekommenderas att gemensamt personuppgiftsansvariga meddelar den andra personuppgiftsansvariga som har ansvaret eller den utsedda kontaktpunkten de förfrågningar som tas emot för att de ska kunna hanteras effektivt. Att kräva att registrerade personer kontaktar den utsedda kontaktpunkten eller den ansvariga personuppgiftsansvarige skulle påföra den registrerade personen en alltför stor börda som skulle strida mot målet att underlätta utövandet av deras rättigheter enligt GDPR.

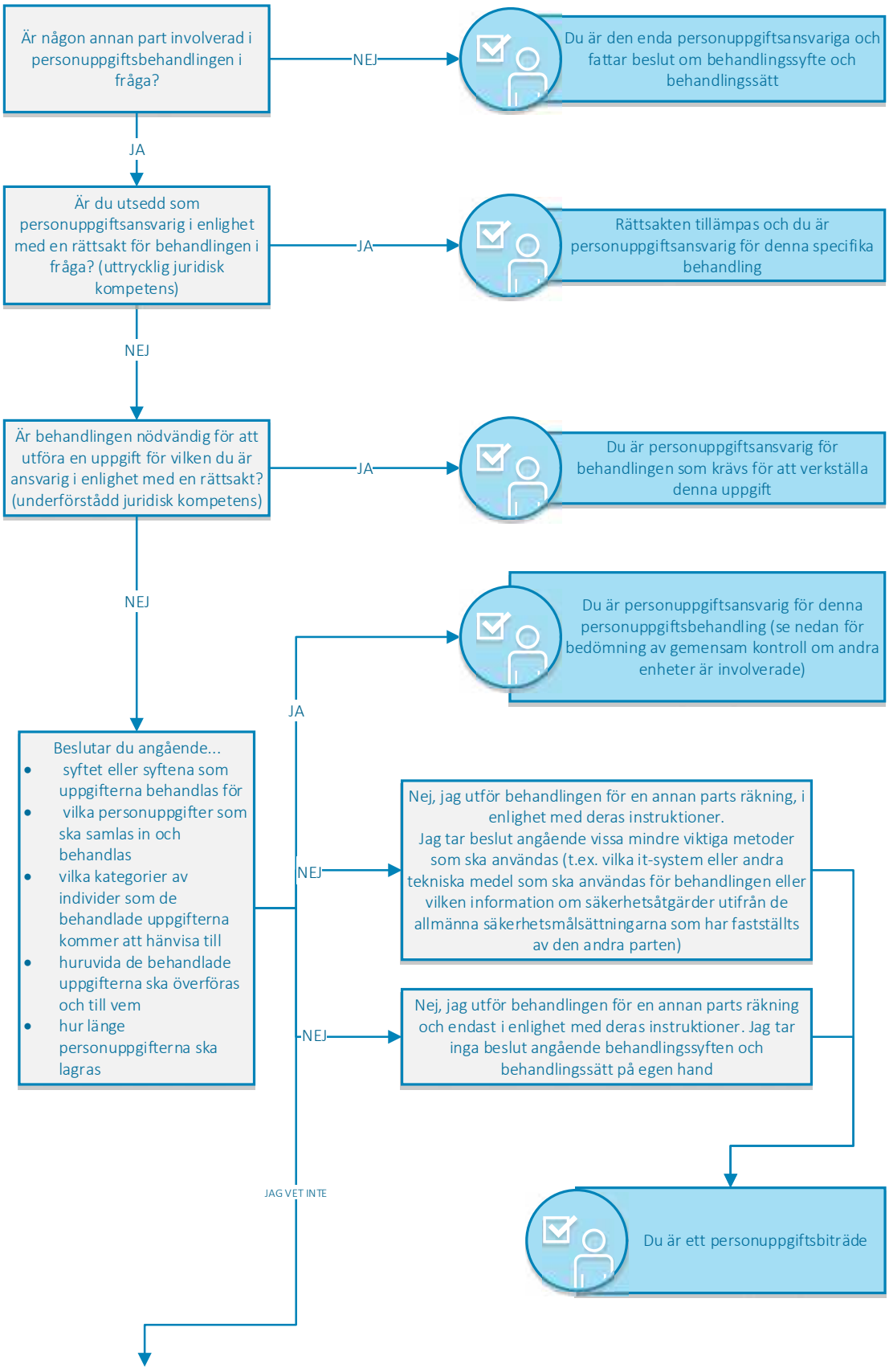
2.3 Skyldigheter gentemot dataskyddsmyndigheter

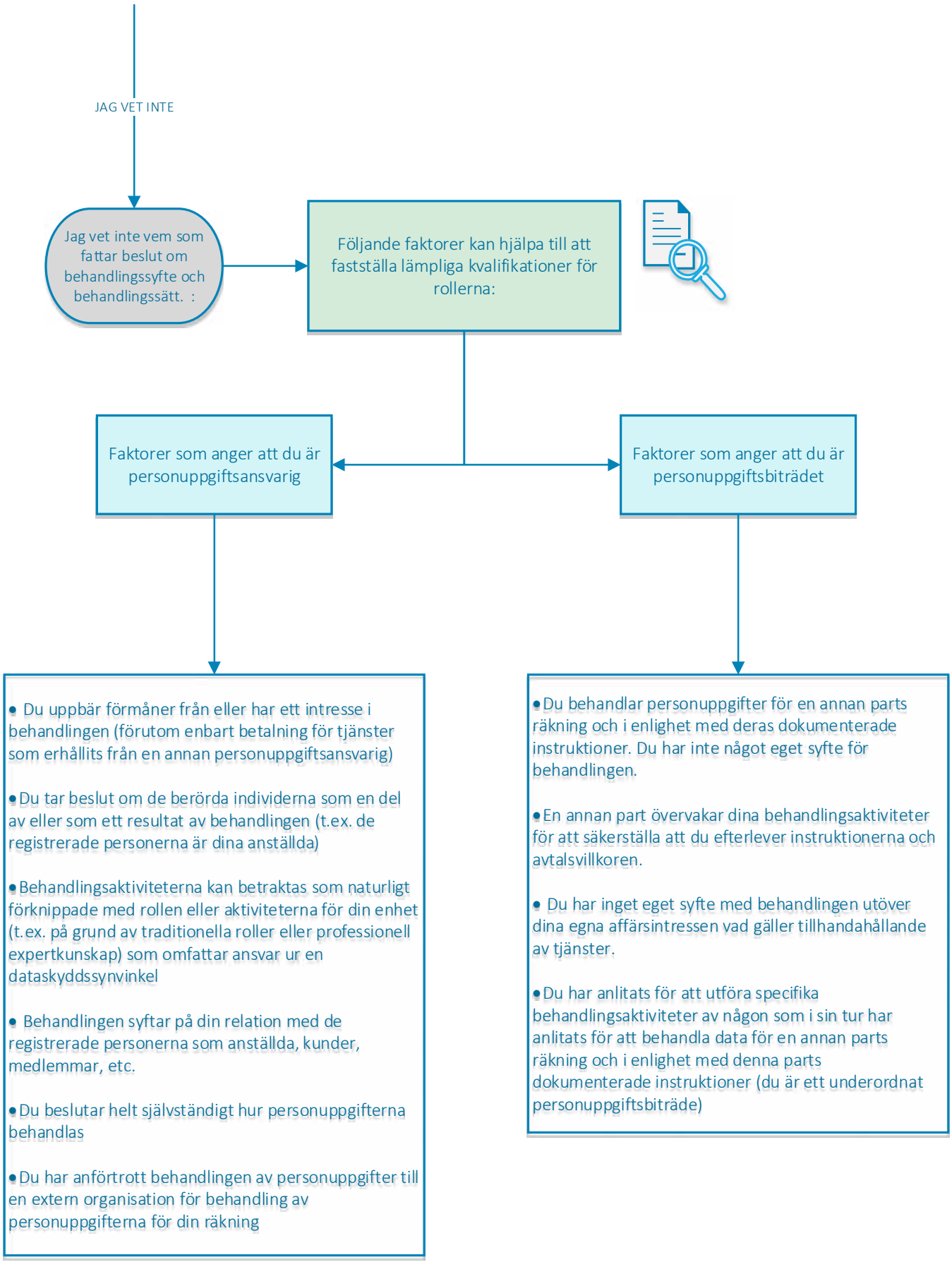
190. Gemensamt personuppgiftsansvariga bör i arrangemanget organisera hur de kommer att kommunicera med de behöriga tillsynsmyndigheterna för dataskydd. Sådan kommunikation kan omfatta eventuellt samråd enligt artikel 36 i GDPR, anmälan om ett dataintrång eller utnämnande av ett dataskyddsombud.

191. Man bör komma ihåg att tillsynsmyndigheterna inte är bundna av villkoren i avtalet, vare sig vad gäller frågan om kvalificering av parterna som gemensamt personuppgiftsansvariga eller den utsedda kontaktpunkten. Därför kan myndigheterna kontakta endera av de gemensamt personuppgiftsansvariga för att utöva sina befogenheter enligt artikel 58 när det gäller den gemensamma behandlingen.

Bilaga I – Flödesschema för tillämpning av koncepten för personuppgiftsansvarig, personuppgiftsbiträde och gemensamt personuppgiftsansvariga i praktiken

Observera: för att bedöma rollen för varje involverad enhet på rätt sätt måste man först identifiera den specifika behandlingen av personuppgifter som ska genomföras och dess exakta syfte. Om flera enheter är involverade är det nödvändigt att bedöma huruvida syften och behandlingssätt fastställs tillsammans, vilket leder till gemensamt personuppgiftsansvar.




JAG VET INTE
Jag vet inte vem som fattar beslut om behandlingssyfte och behandlingssätt. :
Följande faktorer kan hjälpa till att fastställa lämpliga kvalifikationer för rollerna:
Faktorer som anger att du är personuppgiftsansvarig
Faktorer som anger att du är personuppgiftsbiträdet
• Du uppbär förmåner från eller har ett intresse i behandlingen (förutom enbart betalning för tjänster som erhållits från en annan personuppgiftsansvarig)
• Du tar beslut om de berörda individerna som en del av eller som ett resultat av behandlingen (t.ex. de registrerade personerna är dina anställda)
• Behandlingsaktiviteterna kan betraktas som naturligt förknippade med rollen eller aktiviteterna för din enhet (t.ex. på grund av traditionella roller eller professionell expertkunskap) som omfattar ansvar ur en dataskyddssynvinkel
• Behandlingen syftar på din relation med de registrerade personerna som anställda, kunder, medlemmar, etc.
• Du beslutar helt självständigt hur personuppgifterna behandlas
• Du har anförtrott behandlingen av personuppgifter till en extern organisation för behandling av personuppgifterna för din räkning
• Du behandlar personuppgifter för en annan parts räkning och i enlighet med deras dokumenterade instruktioner. Du har inte något eget syfte för behandlingen.
• En annan part övervakar dina behandlingsaktiviteter för att säkerställa att du efterlever instruktionerna och avtalsvillkoren.
• Du har inget eget syfte med behandlingen utöver dina egna affärsintressen vad gäller tillhandahållande av tjänster.
• Du har anlitats för att utföra specifika behandlingsaktiviteter av någon som i sin tur har anlitats för att behandla data för en annan parts räkning och i enlighet med denna parts dokumenterade instruktioner (du är ett underordnat personuppgiftsbiträde)

Gemensam kontroll – Om du är personuppgiftsansvarig och andra parter är involverade i behandlingen av personuppgifter: