

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2021/915**av den 4 juni 2021****om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i Europaparlamentets och rådets förordning (EU) 2016/679 och artikel 29.7 i Europaparlamentets och rådets förordning (EU) 2018/1725****(Text av betydelse för EES)**

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av 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 (allmän dataskyddsförordning) ⁽¹⁾, särskilt artikel 28.7,med beaktande av Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG ⁽²⁾, särskilt artikel 29.7, och

av följande skäl:

- (1) Begreppen personuppgiftsansvarig och personuppgiftsbiträde har en central roll vid tillämpningen av förordning (EU) 2016/679 och förordning (EU) 2018/1725. Den personuppgiftsansvarige är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Vid tillämpning av förordning (EU) 2018/1725 avses med personuppgiftsansvarig den unionsinstitution eller det unionsorgan eller det generaldirektorat eller varje annan organisatorisk enhet som ensam(t) eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för denna behandling bestäms av en särskild unionsakt kan den personuppgiftsansvarige eller de särskilda kriterierna för utnämning av personuppgiftsansvarig föreskrivas i unionsrätten. Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
- (2) Samma uppsättning standardavtalsklausuler bör vara tillämpliga med avseende på förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden som omfattas av förordning (EU) 2016/679 och även när de omfattas av förordning (EU) 2018/1725. Detta beror på att bestämmelserna om skydd av personuppgifter i förordning (EU) 2016/679, som gäller för den offentliga sektorn i medlemsstaterna, och bestämmelserna om skydd av personuppgifter i förordning (EU) 2018/1725, som gäller för unionens institutioner, organ och byråer, så långt som möjligt har anpassats till varandra för att främja en konsekvent strategi för skyddet av personuppgifter i hela unionen och det fria flödet av personuppgifter inom unionen.
- (3) För att säkerställa att kraven i förordning (EU) 2016/679 och förordning (EU) 2018/1725 uppfylls, bör den personuppgiftsansvarige, när denne anförtrot behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden som ger tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i förordning (EU) 2016/679 och förordning (EU) 2018/1725, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter.
- (4) När uppgifter behandlas av ett personuppgiftsbiträde ska behandlingen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och som innehåller de delar som förtecknas i artikel 28.3 och 28.4 i förordning (EU) 2016/679 eller artikel 29.3 och 29.4 i förordning (EU) 2018/1725. Avtalet eller rättsakten bör upprättas skriftligen, inbegripet i ett elektroniskt format.
- (5) I enlighet med artikel 28.6 i förordning (EU) 2016/679 och artikel 29.6 i förordning (EU) 2018/1725 får den personuppgiftsansvarige och personuppgiftsbiträdet välja att förhandla fram ett enskilt avtal som innehåller de obligatoriska delar som anges i artikel 28.3 och 28.4 i förordning (EU) 2016/679 respektive artikel 29.3 och 29.4 i förordning (EU) 2018/1725, eller att helt eller delvis använda standardavtalsklausuler som antagits av kommissionen i enlighet med artikel 28.7 i förordning (EU) 2016/679 och artikel 29.7 i förordning (EU) 2018/1725.

⁽¹⁾ EUT L 119, 4.5.2016, s. 1.⁽²⁾ EUT L 295, 21.11.2018, s. 39.

- (6) Det bör stå den personuppgiftsansvarige och personuppgiftsbiträdet fritt att inkludera standardavtalsklausulerna i detta beslut i ett mer omfattande avtal och att lägga till andra klausuler eller ytterligare skyddsåtgärder, förutsatt att de inte direkt eller indirekt strider mot standardavtalsklausulerna eller påverkar de registrerades grundläggande rättigheter och friheter. Användning av standardavtalsklausulerna påverkar inte eventuella avtalsförpliktelser som den personuppgiftsansvarige och/eller personuppgiftsbiträdet har för att säkerställa att tillämpliga privilegier och immuniteter iakttas.
- (7) Standardavtalsklausulerna bör omfatta både materiella och processuella bestämmelser. I enlighet med artikel 28.3 i förordning (EU) 2016/679 och artikel 29.3 i förordning (EU) 2018/1725 bör det i standardavtalsklausulerna även krävas att den personuppgiftsansvarige och personuppgiftsbiträdet anger föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter, kategorier av registrerade och den personuppgiftsansvariges skyldigheter och rättigheter.
- (8) I enlighet med artikel 28.3 i förordning (EU) 2016/679 och artikel 29.3 i förordning (EU) 2018/1725 måste personuppgiftsbiträdet omedelbart informera den personuppgiftsansvarige om denne anser att en instruktion från den personuppgiftsansvarige strider mot förordning (EU) 2016/679 eller förordning (EU) 2018/1725 eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.
- (9) Om ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för att utföra specifika uppgifter bör de särskilda krav som avses i artikel 28.2 och 28.4 i förordning (EU) 2016/679 eller artikel 29.2 och 29.4 i förordning (EU) 2018/1725 tillämpas. I synnerhet krävs ett särskilt eller allmänt skriftligt förhandstillstånd. Oberoende huruvida det är frågan om ett särskilt eller allmänt förhandstillstånd, bör det första personuppgiftsbiträdet hålla en förteckning över andra personuppgiftsbiträden uppdaterad.
- (10) För att uppfylla kraven i artikel 46.1 i förordning (EU) 2016/679 har kommissionen antagit standardavtalsklausuler i enlighet med artikel 46.2 c i förordning (EU) 2016/679. Dessa klausuler uppfyller även kraven i artikel 28.3 och 28.4 i förordning (EU) 2016/679 för överföringar av uppgifter från personuppgiftsansvariga som omfattas av förordning (EU) 2016/679 till personuppgiftsbiträden utanför den förordningens territoriella tillämpningsområde eller från personuppgiftsbiträden som omfattas av förordning (EU) 2016/679 till underleverantörer utanför den förordningens territoriella tillämpningsområde. Dessa standardavtalsklausuler kan inte användas som standardavtalsklausuler i den mening som avses i kapitel V i förordning (EU) 2016/679.
- (11) Tredje parter bör kunna bli parter i standardavtalsklausulerna under avtalets hela löptid.
- (12) Standardavtalsklausulernas tillämpning bör utvärderas som en del av den regelbundna utvärderingen av förordning (EU) 2016/679 enligt artikel 97 i den förordningen.
- (13) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.1 och 42.2 i förordning (EU) 2018/1725 och har avgett ett [gemensamt yttrande] den 14 januari 2021 ⁽³⁾, vilket har beaktats vid utarbetandet av detta beslut.
- (14) De åtgärder som föreskrivs i detta beslut följer yttrandet från den kommitté som inrättats enligt artikel 93 i förordning (EU) 2016/679 respektive artikel 96.2 i förordning (EU) 2018/1725.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Standardavtalsklausulerna i bilagan uppfyller kraven för avtal mellan personuppgiftsansvariga och personuppgiftsbiträden i artikel 28.3 och 28.4 i förordning (EU) 2016/679 och i artikel 29.3 och 29.4 i förordning (EU) 2018/1725.

Artikel 2

Standardavtalsklausulerna i bilagan får användas i avtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde som behandlar personuppgifter för den personuppgiftsansvariges räkning.

⁽³⁾ Gemensamt yttrande 1/2021 från Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) om Europeiska kommissionens genomförandebeslut om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden för de frågor som avses i artikel 28.7 i förordning (EU) 2016/679 och artikel 29.7 i förordning (EU) 2018/1725.

Artikel 3

Kommissionen ska utvärdera den praktiska tillämpningen av standardavtalsklausulerna i bilagan på grundval av all tillgänglig information som en del av den regelbundna utvärdering som föreskrivs i artikel 97 i förordning (EU) 2016/679.

Artikel 4

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 4 juni 2021.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

STANDARDAVTALSKLAUSULER

AVSNITT I

Klausul 1

Syfte och tillämpningsområde

- a) Syftet med dessa standardavtalsklausuler (*klausulerna*) är att säkerställa överensstämmelse med [välj relevant alternativ: ALTERNATIV 1: artikel 28.3 och 28.4 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]/[ALTERNATIV 2: artikel 29.3 och 29.4 i Europaparlamentets och rådets förordning (EG) nr 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)].
- b) De personuppgiftsansvariga och de personuppgiftsbiträden som anges i bilaga I har kommit överens om att tillämpa dessa klausuler för att säkerställa efterlevnaden av artikel 28.3 och 28.4 i förordning (EU) 2016/679 och/eller artikel 29.3 och 29.4 i förordning (EU) 2018/1725.
- c) Dessa klausuler är tillämpliga på behandling av personuppgifter i enlighet med bilaga II.
- d) Bilagorna I–IV utgör en integrerad del av klausulerna.
- e) Dessa klausuler påverkar inte de skyldigheter som den personuppgiftsansvarige har enligt förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725.
- f) Genom dessa klausuler säkerställs inte i sig att skyldigheterna i samband med internationella överföringar i enlighet med kapitel V i förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725 fullgörs.

Klausul 2

Klausulernas oföränderlighet

- a) Parterna förbinder sig att inte ändra klausulerna, förutom för att lägga till information i bilagorna eller uppdatera informationen i dem.
- b) Detta hindrar inte parterna från att inkludera de standardavtalsklausuler som fastställs i dessa klausuler i ett mer omfattande avtal eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt strider mot klausulerna eller begränsar de registrerades grundläggande rättigheter eller friheter.

Klausul 3

Tolkning

- a) Om de begrepp som definieras i förordning (EU) 2016/679 respektive förordning (EU) 2018/1725 används i dessa klausuler ska dessa begrepp ha samma betydelse som i den förordningen.
- b) Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679 respektive förordning (EU) 2018/1725.
- c) Dessa klausuler ska inte tolkas så att de strider mot de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679 respektive förordning (EU) 2018/1725 eller påverkar de registrerades grundläggande rättigheter eller friheter.

Klausul 4

Hierarki

Om dessa klausuler strider mot bestämmelser i tillhörande avtal mellan parterna som gäller vid den tidpunkt då dessa klausuler avtalas eller ingås därefter, ska dessa klausuler ha företräde.

*Klausul 5 – Frivillig***Dockningsklausul**

- a) Varje enhet som inte är part i dessa klausuler får, med godkännande från samtliga parter, när som helst ansluta sig till dessa klausuler som personuppgiftsansvarig eller personuppgiftsbiträde genom att fylla i bilagorna och underteckna bilaga I.
- b) När de bilagor som avses i led a har fyllts i och undertecknats ska den anslutande enheten behandlas som part i dessa klausuler och ha de rättigheter och skyldigheter som gäller personuppgiftsansvariga eller personuppgiftsbiträden i överensstämmelse med dess intagande i bilaga I.
- c) Den anslutande enheten ska inte ha några rättigheter eller skyldigheter som följer av dessa klausuler innan den blir part.

AVSNITT II

PARTERNAS SKYLDIGHETER*Klausul 6***Beskrivning av behandlingen**

Närmare uppgifter om behandlingen, särskilt kategorierna av personuppgifter och de ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning, anges i bilaga II.

*Klausul 7***Parternas skyldigheter****7.1 Instruktioner**

- a) Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida detta inte är förbjudet med hänvisning till ett viktigt allmänintresse enligt denna rätt. Den personuppgiftsansvarige får även ge efterföljande instruktioner under hela den tid som personuppgifterna behandlas. Dessa instruktioner ska alltid dokumenteras.
- b) Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om personuppgiftsbiträdet anser att en instruktion från den personuppgiftsansvarige strider mot förordning (EU) 2016/679 eller förordning (EU) 2018/1725 eller mot unionens eller medlemsstaternas tillämpliga dataskyddsbestämmelser.

7.2 Ändamålsbegränsning

Personuppgiftsbiträdet får behandla personuppgifterna endast för det eller de specifika ändamål med behandlingen som anges i bilaga II, såvida det inte erhåller ytterligare instruktioner från den personuppgiftsansvarige.

7.3 Varaktigheten för behandlingen av personuppgifter

Behandling som utförs av personuppgiftsbiträdet får endast äga rum under den tid som anges i bilaga II.

7.4 Säkerhet i samband med behandlingen

- a) Personuppgiftsbiträdet ska åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga III för att säkerställa säkerheten för personuppgifterna. Detta omfattar att skydda uppgifterna mot säkerhetsincidenter som leder till oavsiktlig eller olaglig förstörelse, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till uppgifterna (personuppgiftsincident). Vid bedömningen av lämplig säkerhetsnivå ska parterna ta vederbörlig hänsyn till den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerade.
- b) Personuppgiftsbiträdet ska bevilja sin personal tillgång till de personuppgifter som behandlas endast i den mån det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Personuppgiftsbiträdet ska säkerställa att personer med behörighet att behandla de erhållna personuppgifterna har åtagit sig att iakttäta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

7.5 Känsliga uppgifter

Om behandlingen omfattar personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter eller biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning eller uppgifter om fällande domar i brottmål och överträdelser (*känsliga uppgifter*), ska personuppgiftsbiträdet tillämpa särskilda begränsningar och/eller ytterligare skyddsåtgärder.

7.6 Dokumentation och efterlevnad

- a) Parterna ska kunna visa att dessa klausuler följs.
- b) Personuppgiftsbiträdet ska skyndsamt och på lämpligt sätt hantera förfrågningar från den personuppgiftsansvarige om behandlingen av uppgifter i enlighet med dessa klausuler.
- c) Personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som behövs för att påvisa efterlevnad av de skyldigheter som fastställs i dessa klausuler och härrör direkt från förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725. På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet även tillåta och bidra till granskningar av den behandling som omfattas av dessa klausuler, med rimliga intervall eller om det finns tecken på bristande efterlevnad. Vid beslut om översyn eller granskning får den personuppgiftsansvarige ta hänsyn till relevanta certifieringar som personuppgiftsbiträdet innehar.
- d) Den personuppgiftsansvarige kan välja att själv utföra granskningen eller bemyndiga en oberoende revisor. Granskningar får även omfatta inspektioner i personuppgiftsbitrådets lokaler eller fysiska anläggningar och ska vid behov utföras med rimligt varsel.
- e) Parterna ska på begäran göra den information som avses i denna klausul, inklusive resultaten av eventuella granskningar, tillgänglig för den (de) behöriga tillsynsmyndighet(en).

7.7 Användning av underleverantörer

- a) **ALTERNATIV 1: SÄRSKILT FÖRHANDSTILLSTÅND:** Personuppgiftsbiträdet får inte utan särskilt föregående skriftligt tillstånd från den personuppgiftsansvarige lägga ut någon av de behandlingar som utförs för den personuppgiftsansvariges räkning i enlighet med dessa klausuler på en underleverantör. Personuppgiftsbiträdet ska överlämna begäran om särskilt tillstånd minst [SPECIFICERA TIDSPERIOD] innan den berörda underleverantören anlitas, tillsammans med den information som krävs för att den personuppgiftsansvarige ska kunna besluta om tillståndet. Förteckningen över de underleverantörer som den personuppgiftsansvarige har godkänt återfinns i bilaga IV. Parterna ska hålla bilaga IV uppdaterad.

ALTERNATIV 2: ALLMÄNT SKRIFTLIGT TILLSTÅND: Personuppgiftsbiträdet har erhållit ett allmänt tillstånd från den personuppgiftsansvarige att anlita underleverantörer från en överenskommen förteckning. Personuppgiftsbiträdet ska skriftligen informera den personuppgiftsansvarige om eventuella planerade ändringar av förteckningen genom att underleverantörer läggs till eller ersätts minst [SPECIFICERA TIDSPERIOD] i förväg, så att den personuppgiftsansvarige får tillräckligt med tid för att kunna invända mot sådana ändringar innan den eller de berörda underleverantörerna anlitas. Personuppgiftsbiträdet ska tillhandahålla den personuppgiftsansvarige den information som krävs för att denne ska kunna utöva sin rätt att göra invändningar.

- b) Om personuppgiftsbiträdet anlitar en underleverantör för att utföra en specifik behandling (för den personuppgiftsansvariges räkning) ska personuppgiftsbiträdet göra detta genom ett avtal som i sak ålägger underleverantören samma skyldigheter i fråga om uppgiftsskydd som de som personuppgiftsbiträdet åläggs i enlighet med dessa klausuler. Personuppgiftsbiträdet ska se till att underleverantören uppfyller de skyldigheter som personuppgiftsbiträdet omfattas av enligt dessa klausuler och förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725.
- c) På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet tillhandahålla den personuppgiftsansvarige en kopia av ett sådant underleverantörsavtal och eventuella senare ändringar. I den mån det är nödvändigt för att skydda affärshemligheter eller annan konfidentiell information, inbegripet personuppgifter, får personuppgiftsbiträdet redigera avtalstexten innan kopian delas.
- d) Personuppgiftsbiträdet ska fortsatt vara fullt ut ansvarig gentemot den personuppgiftsansvarige för att underleverantören fullgör sina skyldigheter i enlighet med sitt avtal med personuppgiftsbiträdet. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige om underleverantören underlåter att uppfylla sina skyldigheter enligt avtalet.

- e) Personuppgiftsbiträdet och underleverantören ska avtala om en klausul om tredjepartsberättigande, enligt vilken den personuppgiftsansvarige – om personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp underleverantörsavtalet och instruera underleverantören att radera eller återlämna personuppgifterna.

7.8 Internationella överföringar

- a) Personuppgiftsbiträdet får endast överföra uppgifter till ett tredjeland eller en internationell organisation på grundval av dokumenterade instruktioner från den personuppgiftsansvarige eller för att uppfylla ett särskilt krav enligt unionsrätten eller en medlemsstats lagstiftning som personuppgiftsbiträdet omfattas av, och överföringen ska genomföras i enlighet med kapitel V i förordning (EU) 2016/679 eller förordning (EU) 2018/1725.
- b) Den personuppgiftsansvarige samtycker till att, om personuppgiftsbiträdet anlitar en underleverantör i enlighet med klausul 7.7 för att utföra specifik behandling (för den personuppgiftsansvariges räkning) och denna behandling omfattar en överföring av personuppgifter i den mening som avses i kapitel V i förordning (EU) 2016/679, personuppgiftsbiträdet och underleverantören kan säkerställa att kapitel V i förordning (EU) 2016/679 efterlevs genom att använda standardavtalsklausuler som antagits av kommissionen i enlighet med artikel 46.2 i förordning (EU) 2016/679, förutsatt att villkoren för att använda dessa standardavtalsklausuler är uppfyllda.

Klausul 8

Stöd till den personuppgiftsansvarige

- a) Personuppgiftsbiträdet ska utan dröjsmål underrätta den personuppgiftsansvarige om varje begäran som erhållits från den registrerade. Personuppgiftsbiträdet ska inte själv besvara begäran, såvida inte den personuppgiftsansvarige har godkänt detta.
- b) Personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige att fullgöra sin skyldighet att besvara framställningar från registrerade för att utöva sina rättigheter, med hänsyn till behandlingens art. Personuppgiftsbiträdet ska följa den personuppgiftsansvariges instruktioner när det fullgör sina skyldigheter i enlighet med leden a och b.
- c) Utöver personuppgiftsbitrådets skyldighet att bistå den personuppgiftsansvarige enligt klausul 8 b ska personuppgiftsbiträdet dessutom bistå den personuppgiftsansvarige med att säkerställa att följande skyldigheter fullgörs, med beaktande av uppgiftsbehandlingens art och den information som personuppgiftsbiträdet har att tillgå:
- 1) Skyldigheten att utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (en konsekvensbedömning avseende dataskydd) om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.
 - 2) Skyldigheten att samråda med den (de) behöriga tillsynsmyndigheten(-erna) före behandling om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.
 - 3) Skyldigheten att säkerställa att personuppgifterna är korrekta och uppdaterade genom att utan dröjsmål informera den personuppgiftsansvarige om personuppgiftsbiträdet får kännedom om att de personuppgifter som behandlas är felaktiga eller har blivit föråldrade.
 - 4) Skyldigheterna i [ALTERNATIV 1] artikel 32 i förordning (EU) 2016/679/[ALTERNATIV 2] artikel 33 och artiklarna 36–38 i förordning (EU) 2018/1725.
- d) Parterna ska i bilaga III ange de lämpliga tekniska och organisatoriska åtgärder genom vilka personuppgiftsbiträdet ska bistå den personuppgiftsansvarige vid tillämpningen av denna klausul samt räckvidden och omfattningen av det bistånd som krävs.

Klausul 9

Anmälan av personuppgiftsincidenter

Vid en personuppgiftsincident ska personuppgiftsbiträdet samarbeta med och bistå den personuppgiftsansvarige för att denne ska kunna fullgöra sina skyldigheter enligt artiklarna 33 och 34 i förordning (EU) 2016/679 eller artiklarna 34 och 35 i förordning (EU) 2018/1725, i tillämpliga fall, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

9.1 Personuppgiftsincidenter som rör uppgifter som behandlas av den personuppgiftsansvarige

I händelse av en personuppgiftsincident som rör uppgifter som behandlas av den personuppgiftsansvarige ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att

- a) anmäla personuppgiftsincidenten till den (de) behöriga tillsynsmyndigheten(-erna), utan onödigt dröjsmål efter det att den personuppgiftsansvarige har fått kännedom om den, i förekommande fall/(med undantag för om det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter),
- b) erhålla följande information som, i enlighet med [ALTERNATIV 1] artikel 33.3 i förordning (EU) 2016/679/[ALTERNATIV 2] artikel 34.3 i förordning (EU) 2018/1725, ska anges i den personuppgiftsansvariges anmälan, och åtminstone ska omfatta
 - 1) personuppgifternas art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
 - 2) de sannolika konsekvenserna av personuppgiftsincidenten,
 - 3) de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om och i den mån det inte är möjligt att tillhandahålla all denna information samtidigt ska den ursprungliga anmälan innehålla den information som finns tillgänglig, och ytterligare information ska därefter, i den mån den blir tillgänglig, tillhandahållas utan onödigt dröjsmål.

- c) uppfylla, i enlighet med [ALTERNATIV 1] artikel 34 i förordning (EU) 2016/679/[ALTERNATIV 2] artikel 35 i förordning (EU) 2018/1725, skyldigheten att utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten, om den sannolikt kommer att medföra en hög risk för fysiska personers rättigheter och friheter.

9.2 Personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet

I händelse av en personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter det att personuppgiftsbiträdet har fått kännedom om incidenten. En sådan anmäla ska åtminstone innehålla

- a) en beskrivning av incidentens art (inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade och uppgiftsposter som berörs),
- b) uppgifter från en kontaktpunkt där mer information om personuppgiftsincidenten kan erhållas,
- c) de sannolika konsekvenserna och de åtgärder som vidtagits eller föreslagits för att åtgärda incidenten, inbegripet åtgärder för att mildra dess potentiella negativa effekter.

Om och i den mån det inte är möjligt att tillhandahålla all denna information samtidigt ska den ursprungliga anmälan innehålla den information som finns tillgänglig, och ytterligare information ska därefter, i den mån den blir tillgänglig, tillhandahållas utan onödigt dröjsmål.

Parterna ska i bilaga III ange alla andra uppgifter som personuppgiftsbiträdet ska tillhandahålla när denne bistår den personuppgiftsansvarige vid fullgörandet av den personuppgiftsansvariges skyldigheter enligt [ALTERNATIV 1] artiklarna 33 och 34 i förordning (EU) 2016/679/[ALTERNATIV 2] artiklarna 34 och 35 i förordning (EU) 2018/1725.

AVSNITT III

SLUTBESTÄMMELSER

Klausul 10

Bristande efterlevnad av klausulerna och uppsägning

- a) Utan att det påverkar tillämpningen av bestämmelserna i förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725 får den personuppgiftsansvarige, om personuppgiftsbiträdet inte fullgör sina skyldigheter enligt dessa klausuler, instruera personuppgiftsbiträdet att avbryta behandlingen av personuppgifter till dess att denne uppfyller dessa klausuler eller avtalet sägs upp. Personuppgiftsbiträdet ska omedelbart underrätta den personuppgiftsansvarige om denne av något skäl inte kan följa dessa klausuler.

- b) Den personuppgiftsansvarige ska ha rätt att säga upp avtalet i den mån det avser behandling av personuppgifter i enlighet med dessa klausuler om
- 1) personuppgiftsbiträdet behandling av personuppgifter har avbrutits av den personuppgiftsansvarige i enlighet med led a och om efterlevnaden av dessa klausuler inte återställs inom rimlig tid och i alla händelser inom en månad efter det att behandlingen avbrutits,
 - 2) personuppgiftsbiträdet allvarligt eller ihållande åsidosätter dessa klausuler eller sina skyldigheter enligt förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725,
 - 3) personuppgiftsbiträdet underlåter att följa ett bindande beslut från en behörig domstol eller den (de) behöriga tillsynsmyndigheten(-erna) som rör dennes skyldigheter i enlighet med dessa klausuler eller förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725.
- c) Personuppgiftsbiträdet ska ha rätt att säga upp avtalet i den mån det avser behandling av personuppgifter enligt dessa klausuler, om den personuppgiftsansvarige, efter att ha informerats av personuppgiftsbiträdet om att dennes instruktioner strider mot tillämpliga rättsliga krav i enlighet med klausul 7.1 b, insisterar på att instruktionerna följs.
- d) Efter uppsägningen av avtalet ska personuppgiftsbiträdet, beroende på vad den personuppgiftsansvarige väljer, radera alla personuppgifter som behandlats för den personuppgiftsansvariges räkning och intyga för den personuppgiftsansvarige att detta är utfört, eller återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt. Till dess att uppgifterna raderas eller återlämnas ska personuppgiftsbiträdet säkerställa efterlevnaden av dessa klausuler.
-

BILAGA I

Förteckning över parter

Personuppgiftsansvariga: *[Identitet och kontaktuppgifter för den eller de berörda personuppgiftsansvariga, samt, i tillämpliga fall, för den personuppgiftsansvariges dataskyddsombud]*

1. Namn:

Adress:

Kontaktpersonens namn, befattning och kontaktuppgifter:

Underskrift och anslutningsdatum:

2.

.....

Personuppgiftsbiträden: *[Identitet och kontaktuppgifter för den eller de berörda personuppgiftsbiträdena samt, i tillämpliga fall, för personuppgiftsbiträdets dataskyddsombud]*

1. Namn:

Adress:

Kontaktpersonens namn, befattning och kontaktuppgifter:

Underskrift och anslutningsdatum:

2.

.....

BILAGA II

Beskrivning av behandlingen

Kategorier av registrerade vars personuppgifter behandlas

.....

Kategorier av personuppgifter

.....

Känsliga uppgifter som behandlas (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder som fullt ut tar hänsyn till uppgifternas art och de risker som är förknippade med dem, t.ex. strikt ändamålsbegränsning, åtkomstbegränsningar (inbegripet åtkomst endast för personal som har gått en specialiserad utbildning), registrering av åtkomst till uppgifterna, begränsningar för vidareöverföring eller ytterligare säkerhetsåtgärder.

.....

Behandlingens art

.....

Ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning

.....

Behandlingens varaktighet

.....

.....

För behandling som utförs av personuppgiftsbiträden (eller underleverantörer), ange även föremålet för behandlingen, behandlingens art och dess varaktighet

BILAGA III

Tekniska och organisatoriska åtgärder, inbegripet tekniska och organisatoriska åtgärder för att säkerställa datasäkerheten

FÖRKLARANDE ANMÄRKNING:

De tekniska och organisatoriska åtgärderna måste beskrivas konkret och inte på ett allmänt sätt.

En beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som den eller de berörda personuppgiftsbiträdena vidtagit (inbegripet eventuella relevanta certifieringar) för att säkerställa en lämplig säkerhetsnivå, med beaktande av behandlingens art, omfattning, sammanhang och syfte samt riskerna för fysiska personers rättigheter och friheter. Exempel på möjliga åtgärder omfattar följande:

Åtgärder för pseudonymisering och kryptering av personuppgifter.

Åtgärder för att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna.

Åtgärder för att säkerställa förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.

Förfaranden för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärderna för att säkerställa behandlingens säkerhet.

Åtgärder för identifiering och godkännande av användare.

Åtgärder för skydd av uppgifter under överföring.

Åtgärder för skydd av uppgifter under lagring.

Åtgärder för att säkerställa fysisk säkerhet på platser där personuppgifter behandlas.

Åtgärder för att säkerställa loggning av händelser.

Åtgärder för att säkerställa systemkonfiguration, inklusive standardkonfiguration.

Åtgärder för intern it och styrning och hantering av it-säkerhet.

Åtgärder för certifiering/säkring av processer och produkter.

Åtgärder för att säkerställa uppgiftsminimering.

Åtgärder för att säkerställa datakvalitet.

Åtgärder för att säkerställa begränsad lagring av uppgifter.

Åtgärder för att säkerställa ansvarsskyldighet.

Åtgärder för att möjliggöra dataportabilitet och säkerställa radering.

I fråga om överföringar till personuppgiftsbiträden (eller underleverantörer), beskriv även de specifika tekniska och organisatoriska åtgärder som personuppgiftsbiträdet (eller underleverantören) ska vidta för att kunna bistå den personuppgiftsansvarige.

Beskrivning av de specifika tekniska och organisatoriska åtgärder som personuppgiftsbiträdet ska vidta för att kunna bistå den personuppgiftsansvarige.

BILAGA IV

Förteckning över underleverantörer

FÖRKLARANDE ANMÄRKNING:

Denna bilaga måste fyllas i vid särskilt godkännande av underleverantörer (klausul 7.7 a, alternativ 1).

Den personuppgiftsansvarige har godkänt användningen av följande underleverantörer:

1. Namn:

Adress:

Kontaktpersonens namn, befattning och kontaktuppgifter:

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts):

2.
