Dokumentägare	CSE
Klassificering	Public
Status	Final
Dokumentid	TDA1766
Dokumentversion	1.0
Senast ändrat	2024-09-05

Personuppgiftsbiträdesavtal

TUTUS DATA AB, organisationsnummer 556527-7687 (”**personuppgiftsbiträde**””) och [FÖRETAGSNAMN], organisationsnummer [XXXXXX-XXXX] (”**den personuppgiftsansvarige**”) har enats om de avtalsklausuler (”**klausulerna**”) som anges i detta avtal för att uppfylla kraven enligt artikel 28.3 i förordning (EU) 2016/679 (”**den allmänna dataskyddsförordningen**”) och för och säkerställa skyddet av den registrerades rättigheter.

Den personuppgiftsansvarige och personuppgiftsbiträdet kallas tillsammans för ”**parterna**” och var och en ”**part**”.

1. Innehållsförteckning

2 Ingress

1. I följande avtalsklausuler (”klausulerna”) anges rättigheter och skyldigheter för den personuppgiftsansvarige och personuppgiftsbiträdet vid behandling av personuppgifter på uppdrag av den personuppgiftsansvarige.

2. Klausulerna har utformats för att säkerställa parternas uppfyllande av artikel 28.3 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 (allmän dataskyddsförordning).

3. I samband med tillhandahållandet av [TJÄNSTENS NAMN] kommer personuppgiftsbiträdet att behandla personuppgifter åt den personuppgiftsansvarige i enlighet med klausulerna.

4. Klausulerna ska ha företräde framför liknande bestämmelser i andra avtal mellan parterna.

5. Det finns fyra tillägg till klausulerna, vilka utgör en integrerad del av klausulerna.

6. Tillägg A innehåller information om behandlingen av personuppgifter, inklusive behandlingens syfte och art, typ av personuppgifter, kategorier av registrerade och behandlingens varaktighet.

7. Tillägg B innehåller den personuppgiftsansvariges villkor för personuppgiftsbiträdets användning av underleverantörer, samt en lista med underleverantörer som är godkända av den personuppgiftsansvarige.

8. Tillägg C innehåller den personuppgiftsansvariges anvisningar avseende behandlingen av personuppgifter, minimiuppsättningen säkerhetsåtgärder som krävs av personuppgiftsbiträdet, samt hur granskningar av personuppgiftsbiträdet och eventuella underleverantörer ska utföras.

9. Tillägg D innehåller bestämmelser för andra aktiviteter som inte omfattas av klausulerna.

10. Klausulerna och tilläggen ska lagras både skriftligt och elektroniskt av båda parterna.

11. Klausulerna undantar inte personuppgiftsbiträdet från skyldigheter som personuppgiftsbiträdet omfattas av enligt den allmänna dataskyddsförordningen eller annan lagstiftning.

3 Den personuppgiftsansvariges rättigheter och skyldigheter

1. Den personuppgiftsansvarige är ansvarig för att säkerställa att behandlingen av personuppgifter utförs i enlighet med den allmänna dataskyddsförordningen (se artikel 24 i den allmänna dataskyddsförordningen), tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten[1] och klausulerna.

2. Den personuppgiftsansvarige har rätt och skyldighet att besluta om syften och medel för behandlingen av personuppgifter.

3. Den personuppgiftsansvarige är bland annat ansvarig för att den behandling av personuppgifter som personuppgiftsbiträden ombeds utföra har rättslig grund.

4 Personuppgiftsbiträden ska följa anvisningarna

1. Personuppgiftsbiträden får enbart behandla personuppgifter enligt dokumenterade anvisningar från den personuppgiftsansvarige, såvida de inte är skyldiga att göra detta enligt unionens eller medlemsstatens lagstiftning som de omfattas av. Sådana anvisningar anges i tilläggen A och C. Efterföljande anvisningar kan också ges av den personuppgiftsansvarige under behandlingen av personuppgifterna, men sådana anvisningar ska alltid dokumenteras och lagras skriftligt samt elektroniskt i anslutning till klausulerna.

2. Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om dessa anvisningar enligt personuppgiftsbiträdets uppfattning inte följer den allmänna dataskyddsförordningen eller tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten.

[1] Hänvisningar till ”medlemsstater” i klausulerna ska tolkas som hänvisningar till ”EES-medlemsstater”.

5 Sekretess

1. Personuppgiftsbiträdet ska endast bevilja tillgång till de personuppgifter som behandlas på uppdrag av den personuppgiftsansvarige för personer som är underställda personuppgiftsbiträdet och har åtagit sig att bevara sekretessen, eller som omfattas av en lämplig lagstadgad och behovsenlig tystnadsplikt. Förteckningen över de personer som har beviljats tillgång ska granskas regelbundet. Med granskningen som grund kan sådan tillgång till personuppgifter återkallas om tillgången inte längre är nödvändig. Personuppgifterna är därefter inte längre tillgängliga för dessa personer.

2. Personuppgiftsbiträdet ska på begäran av den personuppgiftsansvarige kunna visa att berörda personer som är underställda personuppgiftsbiträdet iakttar ovannämnda sekretess.

6 Säkerhet vid behandling

1. I artikel 32 i den allmänna dataskyddsförordningen anges att med beaktande av tidigare känd teknik, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt risken, av varierande sannolikhets- och allvarlighetsgrad, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

   Den personuppgiftsansvarige ska utvärdera riskerna avseende fysiska personers rättigheter och friheter vid behandlingen och vidta åtgärder för att minska dessa risker. Beroende på relevans kan dessa åtgärder inkludera följande:

   a. Pseudonymisering och kryptering av personuppgifter.

   b. Möjligheten att säkerställa fortlöpande sekretess, integritet, tillgänglighet och motståndskraft i systemen och tjänsterna för behandlingen.

   c. Möjligheten att återställa tillgängligheten och tillgången till personuppgifter inom rimlig tid vid en fysisk eller teknisk incident.

d. Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten i de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Enligt artikel 32 i den allmänna dataskyddsförordningen ska personuppgiftsbiträdet även – fristående från den personuppgiftsansvarige – utvärdera riskerna för fysiska personers rättigheter och friheter vid behandlingen och vidta åtgärder för att minska dessa risker.

   Det innebär att den personupgiftsansvarige ska förse personuppgiftsbiträdet med all information som krävs för identifiering och utvärdering av sådana risker.

3. Dessutom ska personuppgiftsbiträdet bistå den personuppgiftsansvarige i att säkerställa efterlevnad av den personuppgiftsansvariges skyldigheter enligt artikel 32 i den allmänna dataskyddsförordningen, genom att bland annat förse den personuppgiftsansvarige med information avseende tekniska och organisatoriska åtgärder som redan har genomförts av personuppgiftsbiträdet enligt artikel 32 i den allmänna dataskyddsförordningen, samt all övrig information som krävs för att den personuppgiftsansvarige ska kunna fullgöra sin skyldighet enligt artikel 32.

   Om därefter – enligt den personuppgiftsansvariges bedömning – en minskning av identifierade risker kräver att ytterligare åtgärder vidtas av personuppgiftsbiträdet än de som redan har vidtagits enligt artikel 32 i den allmänna dataskyddsförordningen, ska den personuppgiftsansvarige ange att dessa ytterligare åtgärder ska vidtas i tillägg C.

7 Användning av underleverantörer

1. Personuppgiftsbiträdet ska uppfylla de krav som anges i artikel 28.2 och 28.4 i den allmänna dataskyddsförordningen om ett annat personuppgiftsbiträde anlitas (en underleverantör).

2. Personuppgiftsbiträdet får därför inte anlita ett annat personuppgiftsbiträde (underleverantör) enligt klausulerna utan ett föregående allmänt skriftligt tillstånd från den personuppgiftsansvarige.

3. Personuppgiftsbiträdet har den personuppgiftsansvariges allmänna tillstånd att anlita underleverantörer. Personuppgiftsbiträdet ska skriftligen informera den personuppgiftsansvarige om alla avsiktliga förändringar avseende tillägg eller utbyte av underleverantörer minst en månad i förväg och därmed ge den personuppgiftsansvarige möjlighet att invända mot sådana förändringar innan

berörd underleverantör anlitas. Längre tidsperioder för förhandsinformation om specifika underleverantörstjänster kan anges i tillägg B. Den förteckning över underleverantörer som redan har godkänts av den personuppgiftsansvarige återfinns i tillägg B.

4. Om personuppgiftsbiträdet använder en underleverantör för att utföra specifik behandling på uppdrag av den personuppgiftsansvarige, gäller samma dataskyddskyldigheter som anges i klausulerna för underleverantören via avtal eller annan rättsakt enligt EU:s eller medlemsstatens rätt, i synnerhet avseende tillräckliga garantier att vidta lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i klausulerna och den allmänna dataskyddsförordningen.

   Personuppgiftsbiträdet ska därför kräva att underleverantören som ett minimum fullgör de skyldigheter som gäller för personuppgiftsbiträdet enligt klausulerna och den allmänna dataskyddsförordningen.

5. En kopia av ett sådant underleverantörsavtal och efterföljande ändringar ska – på begäran av den personuppgiftsansvarige – skickas till den personuppgiftsansvarige och därmed ge den personuppgiftsansvarige möjlighet att säkerställa att samma dataskyddsskyldigheter som anges i klausulerna gäller för underleverantören. Klausuler för verksamhetsrelaterade frågor som inte påverkar det rättsliga dataskyddsinnehållet i underleverantörsavtalet, behöver inte lämnas till den personuppgiftsansvarige.

6. Personuppgiftsbiträdet ska godkänna en klausul om berättigad tredje part med underleverantören där – i händelse av att personuppgiftsbiträdet går i konkurs – den personuppgiftsansvarige ska vara berättigad tredje part i underleverantörsavtalet och ha rätt att se till att den underleverantör som anlitats av personuppgiftsbiträdet följer avtalet, t.ex. genom att låta den personuppgiftsansvarige ge underleverantören i uppgift att ta bort eller återlämna personuppgifter.

7. Om underleverantören inte fullgör sina dataskyddsskyldigheter är personuppgiftsbiträdet helt ansvarigt inför den personuppgiftsansvarige när det gäller fullgörandet av underleverantörens skyldigheter. Detta påverkar inte de registrerades rättigheter enligt den allmänna dataskyddsförordningen – särskilt de som föreskrivs i artiklarna 79 och 82 i den allmänna dataskyddsförordningen – gentemot den personuppgiftsansvarige och personuppgiftsbiträdet, inklusive underleverantören.

8 Överföring av uppgifter till tredjeland eller internationella organisationer

1. All överföring av personuppgifter till tredjeland eller internationella organisationer av personuppgiftsbiträdet får endast utföras enligt dokumenterade anvisningar från den personuppgiftsansvarige och ska alltid utföras i enlighet med kapitel V i den allmänna dataskyddsförordningen.

2. Om överföringar till tredjeland eller internationella organisationer, vilka personuppgiftsbiträdet inte har anvisats att utföra av den personuppgiftsansvarige, krävs enligt EU:s eller medlemsstatens lagstiftning som omfattar personuppgiftsbiträdet, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan behandlingen utförs, såvida inte sådan information är förbjuden i lagstiftningen av hänsyn till allmänintresset.

3. Utan dokumenterade anvisningar från den personuppgiftsansvarige har personuppgiftsbiträdet därför inte rätt att inom ramen för klausulerna

   a. överföra personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland eller i en internationell organisation,

   b. överföra behandlingen av personuppgifter till en underleverantör i ett tredjeland,

   c. låta personuppgifterna behandlas av ett personuppgiftsbiträde i ett tredjeland.

4. Anvisningarna från den personuppgiftsansvarige avseende överföring av personuppgifter till ett tredjeland, däribland, om tillämpligt, det överföringsverktyg enligt kapitel V i den allmänna dataskyddsförordningen som de bygger på, ska anges i tillägg C.6.

5. Klausulerna får inte förväxlas med standarddataskyddsklausulerna enligt artikel 46.2 c och d i den allmänna dataskyddsförordningen, och klausulerna kan inte åberopas av parterna som ett överföringsverktyg enligt kapitel V i den allmänna dataskyddsförordningen.

9 Stöd till den personuppgiftsansvarige

1. Med beaktande av behandlingens art ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med lämpliga tekniska och organisatoriska åtgärder när det är möjligt, i syfte att fullgöra den personuppgiftsansvariges skyldigheter att besvara förfrågningar om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskyddsförordningen.

   Detta innebär att datauppgiftsbiträdet så långt det är möjligt ska bistå den personuppgiftsansvarige vid den personuppgiftsansvariges efterlevnad av

   a. rätten till information när personuppgifter samlas in från den registrerade,
   b. rätten till information när personuppgifter inte har erhållits från den registrerade,
   c. den registrerades rätt till tillgång,
   d. rätten till rättelse,
   e. rätten till radering (”rätten att bli bortglömd”).
   f. rätten till begränsning av behandling,
   g. anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling,
   h. rätten till dataportabilitet,
   i. rätten att göra invändningar,
   j. rätten att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering.

2. Förutom personuppgiftsbiträdets skyldighet att bistå den personuppgiftsansvarige enligt klausul 6.4, ska personuppgiftsbiträdet dessutom, med beaktande av behandlingens art och den information som finns tillgänglig för personuppgiftsbiträdet, bistå den personuppgiftsansvarige för att säkerställa efterlevnad av

   a. den personuppgiftsansvariges skyldighet att utan dröjsmål och vid behov, inte senare än 72 timmar efter upptäckten, meddela personuppgiftsincidenten till behörig tillsynsmyndighet, Integritetsskyddsmyndigheten (IMY), såvida inte personuppgiftsincidenten troligen inte innebär någon risk för fysiska personers rättigheter och friheter,

   b. den personuppgiftsansvariges skyldighet att utan dröjsmål underrätta den registrerade om personuppgiftsincidenten, när personuppgiftsincidenten troligen resulterar i en hög risk för fysiska personers rättigheter och friheter,

c. den personuppgiftsansvariges skyldighet att utföra en bedömning av den påverkan som de planerade behandlingsåtgärderna får på skyddet av personuppgifter (en konsekvensanalys av dataskyddet),

d. den personuppgiftsansvariges skyldighet att samråda med den behöriga tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY), före behandlingen där en konsekvensbedömning av dataskyddet visar att behandlingen skulle innebära en hög risk om inga åtgärder vidtas av den personuppgiftsansvarige för att minska risken.

3. Parterna ska i tillägg C ange de lämpliga tekniska och organisatoriska åtgärder som personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med, samt omfattningen för det stöd som krävs. Detta avser de skyldigheter som anges i klausul 9.1 och 9.2.

10 Underrättelse om personuppgiftsincident

1. Vid en personuppgiftsincident ska personuppgiftsbiträdet, utan onödigt dröjsmål efter upptäckten, anmäla incidenten till den personuppgiftsansvarige.

2. Personuppgiftsbiträdets underrättelse till den personuppgiftsansvarige ska om möjligt äga rum inom två timmar efter det att personuppgiftsbiträdet har fått vetskap om personuppgiftsincidenten, för att göra det möjligt för den personuppgiftsansvarige att fullgöra skyldigheten att underrätta behörig tillsynsmyndighet om personuppgiftsincidenten, jfr artikel 33 i den allmänna dataskyddsförordningen.

3. I enlighet med klausul 9.2 a ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att underrätta behörig tillsynsmyndighet om personuppgiftsincidenten och bistå vid insamlingen av den information som anges nedan, vilket enligt artikel 33.3 i den allmänna dataskyddsförordningen ska anges i den personuppgiftsansvariges underrättelse till behörig tillsynsmyndighet:

a. Personuppgiftens art, inbegripet om så är möjligt de kategorier och ungefärliga antal registrerade som berörs, samt de kategorier och ungefärliga antal personuppgiftsposter som berörs.

b. De troliga konsekvenserna av personuppgiftsincidenten.

c. De åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att hantera personuppgiftsincidenten, inbegripet när så är lämpligt åtgärder för att mildra dess potentiella skadliga effekter.

4. Parterna ska i tillägg D fastställa allt som ska anges av personuppgiftsbiträdet som stöd när den personuppgiftsansvarige underrättar den behöriga tillsynsmyndigheten om personuppgiftsincidenten.

11 Radera och återlämna uppgifter

1. När personuppgiftsbehandlingen avslutas ska personuppgiftsbiträdet radera alla personuppgifter som har behandlats på uppdrag av den personuppgiftsansvarige samt intyga för den personuppgiftsansvarige att detta har gjorts, såvida inte det enligt unionens eller medlemsstatens lagstiftning krävs att personuppgifterna lagras.

12 Granskning och inspektion

1. Personuppgiftsbiträdet ska för den personuppgiftsansvarige tillgängliggöra all information som krävs för att visa att de skyldigheter som anges i artikel 28 och i klausulerna efterlevs, samt underlätta och bidra till granskningar och inspektioner som utförs av den personuppgiftsansvarige eller annan granskare på uppdrag av den personuppgiftsansvarige.

2. Förfaranden som är tillämpliga vid den personuppgiftsansvariges granskningar och inspektioner som utförs av personuppgiftsbiträdet och underleverantörer, anges i tilläggen C.7 och C.8.

3. Personuppgiftsbiträdet ska ge de tillsynsmyndigheter som enligt tillämplig lagstiftning har tillgång till den personuppgiftsansvariges och personuppgiftsbiträdets lokaler, eller ombud som agerar på uppdrag av sådana tillsynsmyndigheter, tillgång till personuppgiftsbiträdets fysiska lokaler vid uppvisande av lämplig id-handling.

13 Parternas överenskommelse om andra villkor

1. Parterna får komma överens om andra klausuler avseende behandlingen av personuppgifter genom att exempelvis ange ansvarsskyldighet, så länge de inte strider direkt eller indirekt mot klausulerna eller den registrerades grundläggande rättigheter eller friheter och det skydd som anges i den allmänna dataskyddsförordningen.

14 Inledande och avslutande

1. Klausulerna börjar gälla det datum då båda parter har undertecknat detta avtal.

2. Båda parterna ska ha rätt att kräva att klausulerna omförhandlas om ändringar i lagen eller klausulerna ger anledning till en sådan omförhandling.

3. Klausulerna ska gälla under den tid då tjänsterna för personuppgiftsbehandling erbjuds. Under den tid då personuppgiftsbehandlingen utförs kan klausulerna inte upphävas, såvida inte parterna har enats om andra klausuler som styr personuppgiftsbehandlingen.

4. Om personuppgiftsbehandlingen avslutas och personuppgifterna raderas eller återlämnas till den personuppgiftsansvarige i enlighet med klausul 11.1 och tillägg C.4, kan klausulerna upphävas skriftligen av någon av parterna.

5. Underskrift

På uppdrag av den personuppgiftsansvarige

Namn	[NAMN]
Befattning	[BEFATTNING]
Datum	[DATUM]
Underskrift	[UNDERSKRIFT]

På uppdrag av personuppgiftsbiträdet

Namn	[NAMN]
Befattning	[BEFATTNING]
Datum	[DATUM]
Underskrift	[UNDERSKRIFT]

15 Kontakter/kontaktpunkter för den personuppgiftsansvarige och personuppgiftsbiträdet

1. Parterna kan kontakta varandra via följande kontakter/kontaktpunkter:

2. Parterna är skyldiga att omedelbart informera varandra om ändringar i kontakter/kontaktpunkter.

Namn	[NAMN]
Befattning	[BEFATTNING]
Telefonnummer	[TELEFONNUMMER]
E-postadress	[E-POSTADRESS]

Namn	[NAMN]
Befattning	[BEFATTNING]
Telefonnummer	[TELEFONNUMMER]
E-postadress	[E-POSTADRESS]

Tillägg A Information om behandlingen

[OBSERVERA: I HÄNDELSE AV FLERA BEHANDLINGSAKTIVITETER MÅSTE FÖLJANDE MOMENT SLUTFÖRAS FÖR VARJE BEHANDLINGSAKTIVITET.]

A.1. Syftet med personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige:

[BESKRIV SYFTET MED BEHANDLINGEN].

A.2. Personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige ska huvudsakligen avse (behandlingens art):

[BESKRIV BEHANDLINGENS ART].

A.3. Behandlingen inkluderar följande typer av personuppgifter om registrerade:

[BESKRIV TYPEN AV PERSONUPPGIFTER SOM BEHANDLAS].

[EXEMPEL]

”Namn, e-postadress, telefonnummer, adress, personnummer, betalningsinformation, medlemsnummer, typ av medlemskap, närvaro i träningslokalen och anmälan till olika träningspass.”

[OBSERVERA: BESKRIVNINGEN SKA VARA SÅ DETALJERAD SOM MÖJLIGT OCH TYPEN AV PERSONUPPGIFT MÅSTE ALLTID SPECIFICERAS MED MER ÄN BARA ”PERSONUPPGIFT I ENLIGHET MED DEFINITIONEN I ARTIKEL 4.1 I DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN”, ELLER GENOM ATT ANGE VILKEN KATEGORI (”ARTIKEL 6, 9 ELLER 10 I DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN”) AV PERSONUPPGIFTER SOM SKA BEHANDLAS.]

A.4. Behandlingen inkluderar följande kategorier av registrerade:

[BESKRIV KATEGORIN AV REGISTRERADE].

A.5. Personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige får utföras när klausulerna börjar gälla. Behandlingen har följande varaktighet:

[BESKRIV BEHANDLINGENS VARAKTIGHET].

Tillägg B Godkända underleverantörer

B.1. Godkända underleverantörer

När klausulerna börjar gälla godkänner den personuppgiftsansvarige att följande underleverantörer anlitas:

NAMN	ORGANISATIONSNR	ADRESS	BESKRIVNING AV BEHANDLINGEN

Den personuppgiftsansvarige ska när klausulerna börjar gälla godkänna användningen av ovannämnda underleverantörer för den behandling som beskrivs för parten. Personuppgiftsbiträdet ska inte ha rätt att – utan den personuppgiftsansvariges skriftliga tillstånd – anlita en underleverantör för annan behandling än den som har godkänts, eller låta en annan underleverantör utföra angiven behandling.

B.2. Förhandsinformation om godkännande av underleverantörer

[VALFRITT] [OM TILLÄMPLIGT, BESKRIV TIDSPERIODERNA FÖR FÖRHANDSINFORMATION OM GODKÄNNANDE AV UNDERLEVERANTÖRER]

Tillägg C Instruktion avseende användningen av personuppgifter

C.1. Föremål/instruktion för behandlingen

Personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige ska utföras av personuppgiftsbiträdet som utför följande:

[BESKRIV DEN BEHANDLING SOM PERSONUPPGIFTSBITRÄDET HAR BLIVIT INSTRUERAD ATT UTFÖRA].

C.2. Säkerhet vid behandling

Säkerhetsnivån ska vara anpassad till följande:

[BESKRIV DE MOMENT SOM ÄR NÖDVÄNDIGA FÖR SÄKERHETSNIVÅN MED HÄNSYN TILL ARTEN, OMFATTNINGEN, INNEHÅLLET OCH SYFTET MED BEHANDLINGEN, SAMT RISKEN FÖR FYSISKA PERSONERS RÄTTIGHETER OCH FRIHETER.]

[EXEMPEL]

”Behandlingen innefattar en stor andel personuppgifter som omfattas av artikel 9 i den allmänna dataskyddsförordningens ’särskilda kategorier av personuppgifter’, vilket är skälet till att en ’hög’ säkerhetsnivå bör upprättas.”

Personuppgiftsbiträdet ska härefter ha rätt och skyldighet att fatta beslut om de tekniska och organisatoriska säkerhetsåtgärder som bör tillämpas för att skapa nödvändig (och godkänd) datasäkerhetsnivå.

Personuppgiftsbiträdet ska dock – i alla händelser och som ett minimum – vidta följande åtgärder som har godkänts av den personuppgiftsansvarige:

[BESKRIV KRAVEN FÖR PSEUDONYMISERING OCH KRYPTERING AV PERSONUPPGIFTER]

[BESKRIV KRAVEN FÖR ATT SÄKERSTÄLLA FORTLÖPANDE SEKRETESS, INTEGRITET, TILLGÄNGLIGHET OCH MOTSTÅNDSKRAFT I BEHANDLINGSSYSTEMEN OCH TJÄNSTERNA]

[BESKRIV KRAVEN FÖR MÖJLIGHETEN ATT ÅTERSTÄLLA TILLGÄNGLIGHETEN OCH TILLGÅNGEN TILL PERSONUPPGIFTER INOM RIMLIG TID VID EN FYSISK ELLER TEKNISK INCIDENT]

[BESKRIV KRAVEN FÖR DE PROCESSER SOM REGELBUNDET TESTAR, UNDERSÖKER OCH UTVÄRDERAR EFFEKTIVITETEN I DE TEKNISKA OCH

ORGANISATORISKA ÅTGÄRDER SOM SKA SÄKERSTÄLLA BEHANDLINGENS SÄKERHET]

[BESKRIV KRAVEN FÖR TILLGÅNG TILL DATA ONLINE]

[BESKRIV KRAVEN FÖR ATT SKYDDA DATA UNDER ÖVERFÖRING]

[BESKRIV KRAVEN FÖR ATT SKYDDA DATA VID LAGRING]

[BESKRIV KRAVEN FÖR DET FYSISKA SKYDDET AV PLATSER DÄR PERSONUPPGIFTER BEHANDLAS]

[BESKRIV KRAVEN FÖR HEM-/DISTANSARBETE]

[BESKRIV LOGGNINGSKRAVEN]

C.3. Stöd till den personuppgiftsansvarige

Personuppgiftsbiträdet ska så långt det är möjligt – inom ramen för det stöd som anges nedan – bistå den personuppgiftsansvarige i enlighet med klausul 9.1 och 9.2 genom att vidta följande tekniska och organisatoriska åtgärder:

[BESKRIV RÄCKVIDD OCH OMFATTNING FÖR DET STÖD SOM TILLHANDAHÅLLS AV PERSONUPPGIFTSBITRÄDET]

[BESKRIV DE SPECIFIKA TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER SOM SKA VIDTAS AV PERSONUPPGIFTSBITRÄDET SOM STÖD TILL DEN PERSONUPPGIFTSANSVARIGE]

C.4. Lagringsperiod/raderingsåtgärder

[ANGE LAGRINGSPERIOD/RADERINGSÅTGÄRDER FÖR PERSONUPPGIFTSBITRÄDET, OM TILLÄMPLIGT]

[EXEMPEL]

”Personuppgifter lagras under [ANGE TIDSPERIOD ELLER INCIDENT]. Därefter raderas personuppgifterna automatiskt av personuppgiftsbiträdet.

Vid avslutande av personuppgiftsbehandlingen ska personuppgiftsbiträdet antingen radera eller återlämna personuppgifterna i enlighet med klausul 11.1, såvida inte den personuppgiftsansvarige – efter avtalets undertecknande – har ändrat den personuppgiftsansvariges ursprungliga val. En sådan ändring ska dokumenteras och lagras både skriftligt och elektroniskt i anslutning till klausulerna.”

C.5. Behandlingsplats

Behandlingen av personuppgifter enligt klausulerna får inte utföras på andra platser än följande, om inte ett skriftligt förhandstillstånd har getts av den personuppgiftsansvarige:

[ANGE VAR BEHANDLINGEN ÄGER RUM] [ANGE PERSONUPPGIFTSBITRÄDET ELLER UNDERLEVERANTÖREN SOM ANVÄNDER ADRESSEN]

C.6. Instruktion om överföring av personuppgifter till tredjeland

[BESKRIV EN INSTRUKTION OM ÖVERFÖRINGEN AV PERSONUPPGIFTER TILL ETT TREDJELAND ELLER EN INTERNATIONELL ORGANISATION]

[ANGE DEN RÄTTSLIGA GRUNDEN FÖR ÖVERFÖRING ENLIGT KAPITEL V I DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN]
Om den personuppgiftsansvarige inte har angett anvisningar avseende överföringen av personuppgifter till ett tredjeland i klausulerna eller i efterföljande dokument, har personuppgiftsbiträdet inte rätt att inom ramen för klausulerna utföra en sådan överföring.

C.7. Förfarandet vid den personuppgiftsansvariges granskningar och inspektioner av personuppgiftsbiträdets behandling av personuppgifter

[BESKRIV FÖRFARANDET VID DEN PERSONUPPGIFTSANSVARIGES GRANSKNINGAR OCH INSPEKTIONER AV PERSONUPPGIFTSBITRÄDETS BEHANDLING AV PERSONUPPGIFTER]

Exempel:

”Personuppgiftsbiträdet ska under [ANGE TIDSPERIOD] erhålla en [GRANSKNINGSRAPPORT/INSPEKTIONSRAPPORT] från en fristående tredje part avseende personuppgiftsbiträdets efterlevnad av den allmänna dataskyddsförordningen, tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten samt klausulerna, vilket ska bekostas av [PERSONUPPGIFTSBITRÄDET/DEN PERSONUPPGIFTSANSVARIGE].

Parterna har godkänt att följande typer av [GRANSKNINGSRAPPORT/INSPEKTIONSRAPPORT] kan användas i enlighet med klausulerna:

[INFOGA GODKÄNDA GRANSKNINGSRAPPORTER/INSPEKTIONSRAPPORTER]

[GRANSKNINGSRAPPORTEN/INSPEKTIONSRAPPORTEN] ska utan onödigt dröjsmål lämnas in till den personuppgiftsansvarige för kännedom. Den personuppgiftsansvarige kan ifrågasätta omfattningen och/eller metoden för rapporten och kan i sådana fall begära en ny granskning/inspektion med ett reviderat omfång och/eller en annan metod.

Baserat på resultatet av en sådan granskning/inspektion kan den personuppgiftsansvarige begära att ytterligare åtgärder vidtas för att säkerställa efterlevnaden av den allmänna dataskyddsförordningen, tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten och klausulerna.

Den personuppgiftsansvarige eller den personuppgiftsansvariges ombud ska dessutom ha möjlighet att inspektera, även fysiskt, de platser där behandlingen av personuppgifterna utförs av personuppgiftsbiträdet, däribland de fysiska anläggningar och system som används för och i samband med behandlingen. En sådan inspektion ska utföras när den personuppgiftsansvarige anser att det krävs."

[ELLER]

"Den personuppgiftsansvarige eller den personuppgiftsansvariges ombud ska under [ANGE TIDSPERIOD] utföra en fysisk inspektion av de platser där behandlingen av personuppgifter utförs av personuppgiftsbiträdet, inklusive fysiska lokaler samt system som används för och i samband med behandlingen för att försäkra sig om personuppgiftsbiträdets efterlevnad av den allmänna dataskyddsförordningen, tillämpliga dataskyddsbestämmelser i EU och medlemsstaten samt klausulerna.

Förutom den planerade inspektionen kan den personuppgiftsansvarige utföra en inspektion hos personuppgiftsbiträdet när den personuppgiftsansvarige anser att det krävs"

[OCH, OM TILLÄMPLIGT]

"Den personuppgiftsansvariges kostnader avseende den fysiska inspektionen ska, om tillämpligt, bekostas av den personuppgiftsansvarige. Personuppgiftsbiträdet ska dock avsätta de resurser (i huvudsak tid) som krävs för att den personuppgiftsansvarige ska kunna utföra inspektionen."

Tillägg D - Parternas övriga avtalsvillkor

D.1 Ansvar för skada i samband med behandlingen

1. Om personuppgiftsbiträdet blir skadeståndsansvarig till registrerade på grund av överträdelse av klausulerna, tilläggen och/eller enligt den allmänna dataskyddsförordningen, annan lagstiftning eller andra förordningar och föreskrifter tillämpliga på den personuppgiftsbehandling som sker enligt klausulerna och den personuppgiftsansvarige medverkat vid samma behandling som är grund för den registrerades krav, ska den personuppgiftsansvarige ersätta personuppgiftsbiträdet den del av ersättningen personuppgiftsbiträdet enligt lag är skyldig att utge till registrerade som överstiger den ersättning personuppgiftsbiträdet lagligen varit skyldig att utge till registrerade om personuppgiftsbiträdet inte har fullgjort de skyldigheter i den allmänna dataskyddsförordningen som specifikt riktar sig till personuppgiftsbiträdet eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar. Den personuppgiftsansvarige ska därutöver ersätta personuppgiftsbiträdets skäliga och proportionerliga (i förhållande till den personuppgiftsansvariges ansvar) kostnader, inklusive ersättning för rättegångskostnader som personuppgiftsbiträdet blivit ålagd att utge till den registrerade, för att försvara sig mot sådana krav.

2. Om den personuppgiftsansvarige blir skadeståndsansvarig till registrerade på grund av överträdelse av klausulerna, tilläggen och/eller enligt den allmänna dataskyddsförordningen, annan lagstiftning eller andra förordningar och föreskrifter tillämpliga på den personuppgiftsbehandling som sker enligt klausulerna och personuppgiftsbiträdet medverkat vid samman behandling som grund för den registrerades krav, ska personuppgiftsbiträdet ersätta den personuppgiftsansvarige den del av ersättningen den personuppgiftsansvarige enligt lag är skyldig att utge till registrerade som motsvarar den ersättningen personuppgiftsbiträdet lagligen varit skyldig att utge om personuppgiftsbiträdet inte har fullgjort de skyldigheter i den allmänna data-skyddsförordningen som specifikt riktar sig till personuppgiftsbiträdet eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar och personuppgiftsbiträdet inte kan visa att personuppgiftsbiträdet inte på något sätt är ansvarig för den händelse som orsakade skadan. Personuppgiftsbiträdet ska därutöver ersätta den personuppgiftsansvarige skäliga och proportionerliga (i förhållande till personuppgiftsbiträdets ansvar) kostnader inklusive ersättnings för rättegångskostnader som den personuppgiftsansvarige blivit ålagd att utge till den registrerade, för att försvara sig mot sådana krav. Personuppgiftsbiträdets totala ansvar enligt denna bestämmelse är, såvida inte uppsåt eller grov vårdslöshet föreligger begränsat enligt vad som anges i det avtal som parterna träffat och till vilket personuppgiftsbehandlingen relaterar.

3. Parts ersättningsskyldighet enligt denna bestämmelse gäller även efter personuppgiftsbiträdesavtalet i övrigt har upphört.

4. Part som blir föremål för krav från registrerade ska inom skälig tid skriftligen underrätta den andra parten om framförda krav när det står sannolikt för parten att krav mot andra parten enligt punkterna 1 och 2 ovan kan komma att framställas, låta den andra parten få insyn i den registrerades och par-tens handlingar i sådant mål och låta den andra parten lämna synpunkter på detta. Part ska vidare framställa krav på skadestånd till motparten senast inom en månad från det att part blivit skadeståndsansvarig till registrerade.

5. Parts ansvar för andra typer av skador än de som uttryckligen regleras i denna bestämmelse regleras uteslutande av det avtal som parterna träffat och till vilket personuppgiftsbehandlingen relaterar.

D.2 Ersättning

1. Om den personuppgiftsansvarige ändrar sina instruktioner eller meddelar senare instruktioner har personuppgiftsbiträdet rätt till ersättning för nedlagda tid, enligt personuppgiftsbiträdes vid var tid gällande prislista, och övriga kostnader. Personuppgiftsbiträdet har också rätt till ersättning från den personuppgiftsansvarige för nedlagd tid och kostnader enligt samma princip om förfrågningar från enskilda om utövande av rättigheter enligt den allmänna dataskyddsförordningen och annan tillämplig dataskyddslagstiftning tar oproportionerlig tid och kostnader i anspråk hos personuppgiftsbiträdet.