itm8®

Itm8 Sverige AB

Personuppgifts-biträdesavtal

Innehållsförteckning

Personuppgiftsbiträdesavtal klausuler

1 Standardklausuler

Enligt artikel 28(3) i förordning 2016/679 (allmän dataskyddsförordning) vad gäller behandling av personuppgifter av personuppgiftsbiträdet

mellan

Kund (specificerad i Tjänsteavtalet)

(nedan kallad "Personuppgiftsansvarige")

och

itm8 bolaget (specificerad i Tjänsteavtalet)

(nedan kallad "Personuppgiftsbiträdet"),

Som varje är en "part" och tillsammans utgöra de "parterna"

Följande standardavtalsklausuler ("Klausulerna") har överenskommits för att följa GDPR och säkerställa skydd av privatliv och grundläggande rättigheter och friheter avseende fysiska personer.

2 Inledning

1. Kunden har ingått ett Avtal ("**Tjänsteavtal**") med Leverantören och utförandet av de avtalade Tjänsterna ("**Tjänsterna**") är föremål för dessa Villkor.
2. Dessa klausuler avser den/de behandlingsaktivitet(er) ("**Behandlingsaktivitet**") som överenskommits i Tjänsteavtalet.
3. I samband med tillhandahållande av Tjänster behandlar personuppgiftsbiträdet personuppgifter för den personuppgiftsansvariges räkning, vilket är anledningen till att parterna har ingått detta personuppgiftsbiträdesavtal och dess bilagor (gemensamt kallat "Personuppgiftsbiträdesavtalet"), vilket utgör en integrerad del av parternas Tjänsteavtal.
4. Dessa klausuler anger rättigheter och skyldigheter för personuppgiftsbiträdet vid behandling av personuppgifter för den personuppgiftsansvariges räkning.
5. Dessa Klausuler är utformade för att Parterna ska följa Artikel 28(3) av Europaparlamentets och rådets förordning (EU) 2016/679 från den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om den fria rörligheten för sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
6. Klausulerna har företräde över motsvarande klausuler i andra avtal mellan parterna.
7. Dessa klausuler åtföljs av bilagor och bilagorna utgör en integrerad del av klausulerna.
8. Bilaga A innehåller detaljer för bearbetning av personuppgifter, inklusive de ändamål och naturen av Behandlingen, typ av personuppgifter, kategorier av personuppgifter och bearbetningens varaktighet. **Bilaga A1** innehåller krav för de överenskomna behandlingsaktiviteterna som är kopplade till det/de överenskomna serviceområdet/-områdena.
9. Bilaga B innehåller den personuppgiftsansvariges villkor för personuppgiftsbiträdets användning av underbiträden. **Bilaga B1** innehåller en lista över underbiträden för de behandlingsaktiviteter som rör det/de avtalade serviceområden som den personuppgiftsansvarige har godkänt användning av.
10. Bilaga C innehåller den personuppgiftsansvariges instruktioner gällande personuppgiftsbiträdets behandling av personuppgifter, en beskrivning av säkerhetsåtgärder som personuppgiftsbiträdet måste implementera som ett minimum, och hur personuppgiftsbiträdet och eventuella underbiträden övervakas. **Bilaga C1** innehåller de överenskomna säkerhetsåtgärderna.
11. Bilaga D innehåller klausuler relaterande till andra aktiviteter som inte är täckta av Klausulerna, inklusive separata nationella dataskyddskrav som beskrivs i **bilaga D8** .
12. Klausulerna och deras bilagor är lagrade elektroniskt på **legal & Compliance på itm8**. Personuppgiftsansvarige åtar sig till hålla egna kopior av Klausulerna inklusive dess bilagor.

13. Dessa klausuler befriar inte personuppgiftsbiträdet från skyldigheter som åligger personuppgiftsbiträdet enligt den allmänna dataskyddsförordningen eller någon annan tvingande lagstiftning.

3 Rättigheter och skyldigheter för Personuppgiftsansvarige

1. Personuppgiftsansvarige ansvarar för att behandlingen av personuppgifter sker i överensstämmelse med den allmänna dataskyddsförordningen (”GDPR”) (se Artikel 24 i förordningen), den tillämpliga EU- eller medlemsstaten[1] databestämmelserna och klausulerna.

2. Den personuppgiftsansvarige har rätt och skyldighet att bestämma över vilket/vilka ändamål och med vilka medel personuppgifter får behandlas.

3. Den Personuppgiftsansvarige ska bland annat ansvara för att säkerställa att behandlingen av personuppgifter som personuppgiftsbiträdet har anlitas för har en laglig grund.

4 Personuppgiftsbiträdets handlingar enligt till instruktioner

1. Personuppgiftsbiträdet skall behandla personuppgifter endast på dokumenterad instruktioner från den Personuppgiftsansvarige, såvida det inte krävs enligt EU-rätt eller nationell rätt. Denna instruktion skall vara specificerad i Bilaga A och **bilaga A1** och bilaga C och **bilaga C1**. Efterföljande instruktioner kan också ges av den personuppgiftsansvarige under hela den varaktighet som Behandlingen av personuppgifter sker, men sådana instruktionerna ska alltid vara skriftligen dokumenterade, inklusive elektroniskt, i förbindelse med dessa klausuler.

2. Personuppgiftsbiträdet skall omedelbart informera Personuppgiftsansvarige om instruktioner som är givna av Personuppgiftsansvarige, som i personuppgiftsbiträdets omdöme, strider mot GDPR eller de tillämpliga EU- eller medlemsstaternas dataskyddsbestämmelser.

5 Sekretess

1. Personuppgiftsbiträdet ska endast ge tillgång till personuppgifter som behandlas för den personuppgiftsansvariges räkning till personer som omfattas av personuppgiftsbiträdets instruktioner och som har åtagit sig sekretess eller som omfattas av lämplig lagstadgad sekretess, och endast i den utsträckning det är nödvändigt. Förteckning över personer som har beviljats åtkomst ska ses över regelbundet. Baserat på denna granskning kan sådan åtkomst till personuppgifter återkallas om åtkomst inte längre är nödvändig, och personuppgifter ska följaktligen inte längre vara tillgängliga för dessa personer.

2. Personuppgiftsbiträdet ska på den personuppgiftsansvariges begäran visa att de berörda personerna under personuppgiftsbiträdets behörighet omfattas av ovannämnda tystnadsplikt.

[1] Referenser till "Medlem staterna" gjord över hela Klausulernaskall vara förstått som referenser till EES Medlem "Stater".

6 Säkerhet i bearbetningen

1. Artikel 32 GDPR anger att den Personuppgiftsansvarige och Personuppgiftsbiträdet ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en skyddsnivå som är lämplig i förhållande till riskerna, med beaktande av den aktuella tekniken, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och syften samt risker av varierande sannolikhet och allvarlighetsgrad för fysiska personers rättigheter och friheter.

   Den Personuppgiftsansvarige ska utvärdera riskerna för fysiska personers rättigheter och friheter som är inneboende i i Behandlingen och genomföra åtgärder att mildra dessa risker. Beroende på deras relevans kan åtgärderna omfatta följande:

   a. pseudonymisering och kryptering av personuppgifter.

   b. förmågan att säkerställa pågående sekretess, integritet, tillgänglighet och motståndskraft i bearbetningssystem och tjänster.

   c. förmåga till att återställa tillgänglighet och åtkomst till personuppgifter utan onödigt dröjsmål vid en fysisk eller teknisk incident.

   d. ett förfarande för regelbundet testning, bedöma och utvärdera effektiviteten av tekniska och organisatorisk åtgärder för säkerställandet av Behandlingen.

2. Enligt artikel 32 i GDPR ska personuppgiftsbiträdet även – oberoende av den Personuppgiftsansvarige – utvärdera de risker för fysiska personers rättigheter som behandlingen medför och vidta åtgärder för att minska dessa risker. I detta syfte ska den Personuppgiftsansvarige förse personuppgiftsbiträdet med all information som behövs för att identifiera och utvärdera sådana risker.

3. Dessutom, ska Personuppgiftsbiträdet hjälpa Personuppgiftsansvariges efterlevnad enligt artikel 32 GDPR, bland annat att förse den Personuppgiftsansvarige med nödvändig information om de tekniska och organisatoriska säkerhetsåtgärder som redan är implementerad av Personuppgiftsbiträdet i enlighet med till Artikel 32 GDPR och all annan information som är nödvändig för att den Personuppgiftsansvarige ska kunna fullgöra sin skyldighet enligt artikel 32 i GDPR.

   Om hanteringen av de identifierade riskerna – enligt den personuppgiftsansvariges bedömning – kräver införande av ytterligare åtgärder utöver de åtgärder som redan har vidtagits av personuppgiftsbiträdet, ska den personuppgiftsansvarige specificera de ytterligare åtgärder som ska vidtas i Bilaga C, inklusive **bilaga C1**.

7 Användning av underbiträden

1. Personuppgiftsbiträdet måste uppfylla villkoren i artikel 28(2) och (4) i GDPR för att få anlita ett annat personuppgiftsbiträde (ett underbiträde).

2. Personuppgiftsbiträdet får därför inte anlita ett underbiträde för att uppfylla dessa klausuler utan föregående generellt skriftligt godkännande från den personuppgiftsansvarige.

3. Personuppgiftsbiträdet har personuppgiftsansvariges allmänna behörighet att anlita underbiträde enligt **bilaga B1**.

4. **Bilaga B1** innehåller en förteckning över underbiträden för de överenskomna behandlingsaktiviteterna som är kopplade till det/de överenskomna serviceområden som den personuppgiftsansvarige har godkänt användning av.

5. Personuppgiftsbiträdet ska skriftligen underrätta den personuppgiftsansvarige om alla planerade ändringar avseende tillägg eller utbyte av underbiträden med minst 30 dagars varsel, varigenom den personuppgiftsansvarige har möjlighet att invända mot sådana ändringar innan den/de berörda underbiträdena används. Förteckningen över underbiträden som redan är auktoriserade av den personuppgiftsansvarige finns i **bilaga B1**.

6. När personuppgiftsbiträdet anlitar ett underbiträde för att utföra specifika behandlingsaktiviteter för den personuppgiftsansvariges räkning, ska personuppgiftsbiträdet genom avtal eller annan rättsakt enligt unionsrätten eller medlemsstatens nationella rätt ålägga underbiträdet samma dataskyddsskyldigheter som följer av dessa klausuler, särskilt genom att tillhandahålla tillräckliga garantier för att underbiträdet kommer att vidta de tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven enligt dessa klausuler och dataskyddsförordningen (GDPR).
   Personuppgiftsbiträdet ska därmed ansvara för att säkerställa att underbiträdet åtminstone uppfyller de skyldigheter som personuppgiftsbiträdet omfattas av enligt dessa klausuler och dataskyddsförordningen (GDPR).

7. Underbiträdesavtalet/avtalen och eventuella efterföljande ändringar därav ska – på begäran av Personuppgiftsansvarige – skickas som en kopia till den Personuppgiftsansvarige, som därigenom har möjligheten att säkerställa att liknande dataskyddsskyldigheter som följer av dessa klausuler åläggs underbiträdet. Klausuler om kommersiella villkor som inte påverkar den rättsliga data skydd innehåll av de underleverantör avtal, skall inte behöva skickas till den personuppgiftsansvarige.

8. Om underbiträdet inte fullgör sina dataskyddsskyldigheter, kvarstår personuppgiftsbiträdet som fullt ansvarigt gentemot den personuppgiftsansvarige för uppfyllandet av underbiträdets skyldigheter. Detta påverkar inte de registrerades rättigheter enligt dataskyddsförordningen (GDPR) – i synnerhet de rättigheter som följer av artiklarna 79 och 82 GDPR – gentemot den personuppgiftsansvarige och personuppgiftsbiträdet, inklusive underbiträdet.

8 Överföra personuppgifter till tredje land eller internationella organisationer

1. All överföring av personuppgifter till tredjeländer eller internationella organisationer av personuppgiftsbiträdet får endast ske på grundval av dokumenterade instruktioner från den personuppgiftsansvarige och ska alltid ske i enlighet med kapitel V i dataskyddsförordningen (GDPR).

2. Om överföringar till tredjeländer eller internationella organisationer, som personuppgiftsbiträdet inte uttryckligen har instruerats att utföra av den personuppgiftsansvarige, krävs enligt unionsrätten eller medlemsstatens nationella rätt som personuppgiftsbiträdet omfattas av, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om detta rättsliga krav innan behandlingen påbörjas, såvida inte sådan information är förbjuden enligt lag av hänsyn till viktiga allmänintressen.

3. Utan dokumenterade instruktioner från den personuppgiftsansvarige får personuppgiftsbiträdet inte, inom ramen för dessa klausuler:

    a. överföra personuppgifter till en personuppgiftsansvarig eller en personuppgiftsbiträde i en tredje land eller en internationell organisation .

    b. överföra Behandlingen av personuppgifter till ett underbiträde i tredje land.

    c. behandla personuppgifter i ett tredje land.

4. Den personuppgiftsansvariges instruktioner avseende överföring av personuppgifter till tredje land, inklusive i förekommande fall den överföringsmekanism enligt kapitel V GDPR som överföringen grundar sig på, ska anges i Bilaga C.6.

5. Dessa klausuler ska inte förväxlas med standardavtalsklausuler för dataskydd enligt artikel 46.2 c och d GDPR, och dessa klausuler utgör inte i sig en rättslig grund för överföring av personuppgifter enligt kapitel V GDPR.

9 Assistans till den Personuppgiftsansvarige

1. Med beaktande av behandlingens art ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med lämplig teknisk och organisatorisk åtgärd, i den mån som detta är möjligt, för att fullgöra den Personuppgiftsansvariges skyldigheter gentemot den registrerades rättigheter som anges i kapitel III i GDPR.

    Detta innebär att de personuppgiftsbiträdet måste, i den mån som detta är möjlig, hjälpa den Personuppgiftsansvarige i Personuppgiftsansvariges efterlevnad av:

    a. Rätt att få information när personuppgifter samlas in från den registrerade.

    b. Rätt att få information när personuppgifter inte har erhållits från den registrerade.

    c. Den registrerades rätt till tillgång (registerutdrag).

    d. Rätt till rättelse.

    e. Rätt till radering (”rätten att bli bortglömd”).

    f. Rätt till begränsning av behandling.

    g. Underrättelseskyldighet avseende rättelse eller radering av personuppgifter eller begränsning av behandling.

    h. Rätt till dataportabilitet.

    i. Rätt att göra invändningar.

    j. Rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inklusive profilering.

2. Utöver personuppgiftsbiträdets skyldighet att bistå den personuppgiftsansvarige enligt punkt 6.3 ska personuppgiftsbiträdet, med beaktande av behandlingens art och den information som står till personuppgiftsbiträdets förfogande, även bistå den personuppgiftsansvarige med följande:

    a. Den personuppgiftsansvariges skyldighet att utan onödigt dröjsmål och, när så är möjligt, senast 72 timmar efter att ha fått kännedom om den, anmäla en personuppgiftsincident till behörig tillsynsmyndighet, Integritetsmyndigheten (IMY), såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

    b. Den personuppgiftsansvariges skyldighet att utan onödigt dröjsmål underrätta den registrerade om personuppgiftsincidenten, när incidenten sannolikt medför en hög risk för fysiska personers rättigheter och friheter.

    c. Den personuppgiftsansvariges skyldighet att före behandlingen genomföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (konsekvensbedömning avseende dataskydd, DPIA).

    d. Den personuppgiftsansvariges skyldighet att, innan behandlingen påbörjas, samråda med behörig tillsynsmyndighet, Integritetsmyndigheten (IMY), när en konsekvensbedömning avseende dataskydd visar att behandlingen skulle medföra en hög risk i avsaknad av åtgärder som den personuppgiftsansvarige vidtar för att begränsa risken.

3. Parterna ska i Bilaga C fastställa de lämpliga tekniska och organisatoriska åtgärder genom vilka personuppgiftsbiträdet är skyldigt att bistå den personuppgiftsansvarige, samt omfattningen och graden av det bistånd som krävs. Detta gäller de skyldigheter som anges i punkterna 9.1 och 9.2.

10 Underrättelse av personuppgiftsincident

1. Vid personuppgiftsincident ska personuppgiftsbiträdet, utan onödigt dröjsmål efter att ha blivit medveten om det, underrätta den personuppgiftsansvarige om personuppgiftsincidenten.

2. Personuppgiftsbiträdets underrättelse till Personuppgiftsansvarige ska, om möjligt, genomföras inom 24 timmar efter att ha blivit medveten om intrånget så att den personuppgiftsansvarige kan fullgöra sin skyldighet att anmäla personuppgiftsincidenten till den behöriga tillsynsmyndigheten, jfr artikel 33 GDPR.

3. I enlighet med klausul 9.2.a ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att meddela de personuppgiftsincidenten till behörig tillsynsmyndighet. Detta menas att personuppgiftsbiträdet ska bistå med att tillhandahålla följande information, vilken enligt artikel 33(3) i GDPR ska ingå i den personuppgiftsansvariges anmälan om intrånget till den behöriga tillsynsmyndigheten:

    a. personuppgiftsincidentens art, inklusive, om möjligt, kategorierna och det ungefärliga antalet berörda registrerade, samt kategorierna och det ungefärliga antalet berörda personuppgiftsregister.

b. troliga konsekvenser av personuppgiftsincidenten.

c. vidtagna åtgärder eller föreslagna att tas av Personuppgiftsansvarige för att ta itu med personuppgiftsincidenten, inklusive, i tillämpliga fall, åtgärder för att mildra dess eventuella negativa effekter.

4. Parterna ska i Bilaga C fastställa vilken information som personuppgiftsbiträdet ska tillhandahålla inom ramen för sitt bistånd till den personuppgiftsansvarige i dennes skyldighet att anmäla personuppgiftsincidenter till behörig tillsynsmyndighet.

11 Radering och återlämning av personuppgifter

1. Vid upphörande av tjänsterna för behandling av personuppgifter ska personuppgiftsbiträdet vara skyldigt att radera samtliga personuppgifter som behandlas för den personuppgiftsansvariges räkning och bekräfta till den personuppgiftsansvarige att personuppgifterna har raderats, eller att återlämna samtliga personuppgifter och radera befintliga kopior, om inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstatens nationella rätt.

12 Granskning och inspektion

1. Personuppgiftsbiträdet ska göra all information tillgänglig för den personuppgiftsansvarige som är nödvändig för att visa att de skyldigheter som fastställs i artikel 28 i dataskyddsförordningen (GDPR) samt i dessa klausuler uppfylls, samt möjliggöra och bidra till revisioner, inklusive inspektioner, som utförs av den personuppgiftsansvarige eller av annan revisor som utsetts av den personuppgiftsansvarige.

2. Förfaranden som gäller för den personuppgiftsansvariges revisioner, inklusive inspektioner, av personuppgiftsbiträdet och eventuella underbiträden anges i Bilagorna C.7 och C.8.

3. Personuppgiftsbiträdet ska vara skyldigt att ge tillsynsmyndigheter som, i enlighet med tillämplig lagstiftning, har tillträde till den personuppgiftsansvariges eller personuppgiftsbiträdets lokaler, eller företrädare som agerar på sådana tillsynsmyndigheters vägnar, tillträde till personuppgiftsbiträdets fysiska lokaler mot uppvisande av giltig legitimation.

13 Övriga villkor

1. Parterna får i avtalet om tillhandahållande av Tjänsterna eller i Bilaga D avtala om andra klausuler avseende behandlingen av personuppgifter, exempelvis beträffande ansvar, under förutsättning att sådana klausuler inte direkt eller indirekt strider mot dessa klausuler eller inskränker de registrerades grundläggande rättigheter och friheter enligt dataskyddsförordningen (GDPR).

14 Början och uppsägning

1. Dessa klausuler träder i kraft den dag då Parterna ansluter sig till Tjänsteavtalet.
2. Vardera parten har rätt att begära att dessa klausuler omförhandlas om ändringar i lagstiftningen eller brister/olämpligheter i klausulerna ger upphov till ett sådant behov.
3. Dessa klausuler ska gälla under hela den tid som tjänster för behandling av personuppgifter tillhandahålls. Under denna period får klausulerna inte sägas upp, såvida inte andra klausuler som reglerar tillhandahållandet av tjänster för behandling av personuppgifter har avtalats mellan parterna.
4. Om tillhandahållandet av Tjänster relaterade till behandling av personuppgifter upphör och personuppgifterna har raderats eller återlämnats till den personuppgiftsansvarige i enlighet med punkt 11.1 och Bilaga C.4, får dessa klausuler sägas upp av endera parten genom skriftligt meddelande.
5. Undertecknande

    a. Dessa klausuler ska anses accepterade i samband med undertecknandet av Parternas Tjänsteavtal avseende leverans av Tjänsterna.

    b. Parterna bekräftar och är överens om att en digital signatur som tillhandahålls av en part i samband med ingåendet av Tjänsteavtalet har samma rättsliga giltighet och bindande verkan som ett egenhändigt (fysiskt) undertecknande av dessa klausuler.

15 Personuppgiftsansvariges och personuppgiftsbiträdets kontakter

1. Parterna får kontakta varandra via de kontaktpersoner som anges i det avtalade Tjänsteavtalet.
2. Parterna är skyldiga att hålla varandra underrättade om förändringar avseende kontaktpersoner.

Bilaga A - Information om Behandlingen

A.1 Ändamålet med personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning

Parterna har avtalat att personuppgiftsbiträdet ska tillhandahålla varje avtalad Tjänst som regleras i parternas Tjänsteavtal. Utförandet av de avtalade Tjänsterna innebär behandlingsaktiviteter i den mening som avses i dataskyddslagstiftningen. De avtalade behandlingsaktiviteterna anges i Tjänsteavtalet.

De avtalade behandlingsaktiviteterna hänförliga till de avtalade Tjänsteområdena fastställer kraven för Kundens instruktioner, föremålet för behandlingen, behandlingens art, typer av personuppgifter avseende de registrerade samt typer av registrerade som beskrivs i **bilaga A1.**

Personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning påbörjas när parternas avtal om tillhandahållande av Tjänster träder i kraft och pågår till dess att behandlingen upphör.

Bilaga B - Underbiträden

B.1. Anlitade Underbiträden

Vid ikraftträdandet av dessa klausuler har den personuppgiftsansvarige godkänt att underbiträden anlitas för de avtalade behandlingsaktiviteterna som är hänförliga till det/de avtalade Tjänsteområdet/-områdena.

Bilaga B1 innehåller en förteckning över de underbiträden som anlitas för de avtalade behandlingsaktiviteterna kopplade till det/de avtalade Tjänsteområdet/-områdena.

Vid köp av nya eller förändring av befintliga Tjänsteområden ska regleringen av godkända underbiträden anges i bilaga B1 .

Personuppgiftsbiträdets underrättelse om planerade ändringar avseende tillägg av eller utbyte av underbiträden sker i enlighet med punkt B.2.

B.2 Förhandsmeddelande om godkännande av underbiträden

Personuppgiftsbiträdets underrättelse om planerade ändringar avseende tillägg av eller utbyte av underbiträden ska, i den mån det är omedelbart möjligt, ha kommit den personuppgiftsansvarige tillhanda minst 30 dagar innan ändringen eller tillämpningen ska träda i kraft.

Oaktat ovanstående godtar den personuppgiftsansvarige att det kan förekomma särskilda fall där det finns ett specifikt behov av att genomföra ändringar avseende tillägg av eller utbyte av underbiträden med kortare varsel eller omedelbart. I sådana fall ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige om ändringen så snart som möjligt.

Om den personuppgiftsansvarige invänder mot ändringen ska den personuppgiftsansvarige underrätta personuppgiftsbiträdet före det aviserade ikraftträdandedatumet för ändringen. Den personuppgiftsansvarige får endast invända om det finns sakliga och konkreta skäl för invändningen.

Genom invändningen accepterar den personuppgiftsansvarige samtidigt att personuppgiftsbiträdet kan hindras från att tillhandahålla hela eller delar av de avtalade Tjänsterna. Sådan utebliven fullgörelse ska inte anses utgöra ett avtalsbrott hänförligt till personuppgiftsbiträdet. Personuppgiftsbiträdet behåller sin rätt till ersättning för sådana Tjänster, trots att de inte kan tillhandahållas den personuppgiftsansvarige.

Om det uttryckligen har avtalats att personuppgiftsbiträdet inte får anlita underbiträden utan den personuppgiftsansvariges förhandsgodkännande, accepterar den personuppgiftsansvarige att detta kan medföra att personuppgiftsbiträdet hindras från att utföra Tjänsterna. Om den personuppgiftsansvarige har motsatt sig ändringar avseende tillägg av eller utbyte av underbiträden, ska utebliven tillhandahållande av Tjänster inte anses utgöra ett avtalsbrott avseende Tjänsteavtalet som är hänförligt till personuppgiftsbiträdet, i de fall utebliven fullgörelse kan hänföras till ett underbiträde.

Bilaga C - Instruktioner rörande behandling av personuppgifter

C.1. Föremålet för / instruktion avseende behandlingen

Den personuppgiftsansvarige instruerar personuppgiftsbiträdet att behandla personuppgifter i enlighet med vad som har avtalats mellan parterna, varvid personuppgiftsbiträdets säkerhetsåtgärder beskrivs i **Bilaga C1** .

C.2. Säkerhet vid behandling

De avtalade säkerhetsåtgärderna anges i **Bilaga C1** .

C.3 Bistånd till den personuppgiftsansvarige

Personuppgiftsbiträdet ska – i den mån det är möjligt – inom den ram och omfattning som anges nedan – bistå den personuppgiftsansvarige i enlighet med punkterna 9.1 och 9.2 genom att vidta följande tekniska och organisatoriska åtgärder:

På särskild begäran av den personuppgiftsansvarige och med beaktande av behandlingens art ska personuppgiftsbiträdet, så långt det är möjligt, bistå den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder för att fullgöra den personuppgiftsansvariges skyldighet att besvara begäranden om utövande av de registrerades rättigheter enligt GDPR.

Om en registrerad lämnar in en begäran om att utöva sina rättigheter till personuppgiftsbiträdet, ska personuppgiftsbiträdet utan onödigt dröjsmål informera den personuppgiftsansvarige.

Med beaktande av behandlingens art och den information som står personuppgiftsbiträdet till förfogande ska personuppgiftsbiträdet, på särskild begäran, även bistå den personuppgiftsansvarige med att säkerställa efterlevnad av den personuppgiftsansvariges skyldigheter avseende:

- införande av lämpliga tekniska och organisatoriska åtgärder,
- säkerhetsincidenter,
- underrättelse om personuppgiftsincidenter till den registrerade,
- genomförande av konsekvensbedömningar, samt
- förhandssamråd med tillsynsmyndigheter.

C.4 Lagringsperiod / raderingsrutiner

Vid upphörande av tjänsten för behandling av personuppgifter ska personuppgiftsbiträdet antingen radera eller återlämna personuppgifterna i enlighet med punkt 11.1.

C.5 Behandlingsplats

Behandling av de personuppgifter som omfattas av klausulerna får inte, utan föregående skriftligt godkännande från den personuppgiftsansvarige, ske på andra platser än en eller flera av följande adresser:

- personuppgiftsbiträdets adresser,
- datacenter som personuppgiftsbiträdet använder,
- adresser till underbiträden och deras respektive underbiträden.

Utöver detta får distansarbete utföras i enlighet med personuppgiftsbiträdets riktlinjer för distansarbete.

C.6. Instruktion avseende överföring av personuppgifter till tredjeländer

Personuppgiftsbiträdet får endast överföra personuppgifter till länder utanför EU eller EES (ett ”Tredjeland”) eller till en internationell organisation i enlighet med vad som anges nedan.

C.6.1 Allmän behörighet för överföring av personuppgifter till säkra Tredjeländer

Den personuppgiftsansvarige lämnar genom dessa klausuler sitt generella och förhandsgodkännande (instruktion) till att personuppgiftsbiträdet får överföra personuppgifter till tredjeländer i de fall Europeiska kommissionen har fastställt att det berörda tredjelandet, territoriet eller sektorn säkerställer en adekvat skyddsnivå.

Den personuppgiftsansvarige lämnar även genom dessa klausuler sitt generella och förhandsgodkännande (instruktion) till att personuppgiftsbiträdet får överföra personuppgifter till organisationer i Förenta staterna som är certifierade enligt EU–U.S. Data Privacy Framework (”DPF”).

C.6.2 Godkännande av överföring till specifika mottagare av personuppgifter i tredjeländer

Den personuppgiftsansvarige ska instruera personuppgiftsbiträdet att överföra personuppgifter till Tredjeländer genom angivna underbiträden i de fall överföring av personuppgifter till Tredjeländer sker enligt vad som anges i **Bilaga B1** . Därutöver ska personuppgiftsbiträdet vara behörigt att överföra personuppgifter till Tredjeländer när detta krävs till följd av den personuppgiftsansvariges åtgärder.

Personuppgiftsbiträdet har rätt att säkerställa nödvändig överföringsmekanism, exempelvis genom användning av standardavtalsklausuler (Standard Contractual Clauses, ”SCC”), och därigenom ingå standardavtalsklausuler med relevant underbiträde. Den personuppgiftsansvarige ska, i den mån det är nödvändigt, bistå personuppgiftsbiträdet med att säkerställa överföringsmekanismen, inklusive exempelvis standardavtalsklausuler.

Om Europeiska kommissionen antar nya standardavtalsklausuler efter avtalets ingående, är personuppgiftsbiträdet behörigt att förnya, uppdatera och/eller använda de standardavtalsklausuler som vid var tid är gällande.

Innehållet i dessa klausuler ska inte anses ändra innehållet i standardavtalsklausulerna.

Om den personuppgiftsansvarige inte lämnar dokumenterade instruktioner i dessa klausuler eller senare avseende överföring av personuppgifter till ett tredjeland, är personuppgiftsbiträdet inte behörigt att genomföra sådana överföringar inom ramen för dessa klausuler.

C.7 Förfaranden för den personuppgiftsansvariges revisioner, inklusive inspektioner, av den behandling av personuppgifter som utförs av personuppgiftsbiträdet

I enlighet med artiklarna 24 och 28 i dataskyddsförordningen (GDPR) har den personuppgiftsansvarige rätt och skyldighet att utöva tillsyn över personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. Den personuppgiftsansvariges genomförande av sådan tillsyn kan ske genom att den personuppgiftsansvarige vidtar någon av följande åtgärder:

- egenkontroll baserad på dokumentation som personuppgiftsbiträdet gör tillgänglig för den personuppgiftsansvarige,
- skriftlig tillsyn, eller
- fysiska inspektioner.

C.7.1 Egenkontroll

Den personuppgiftsansvarige genomför egenkontroll av personuppgiftsbiträdet baserat på dokumentation som görs tillgänglig via *Legal & Compliance in itm8*.

C.7.2 Skriftlig tillsyn och fysisk inspektion

Den personuppgiftsansvarige får välja att genomföra en revision antingen som en skriftlig revision eller genom fysisk inspektion. Revisionen kan genomföras av den personuppgiftsansvarige själv och/eller i samarbete med tredje part. En revision ska baseras på de säkerhetsåtgärder som avtalats mellan parterna.

Vid begäran om skriftlig tillsyn eller fysisk inspektion ska följande förfarande tillämpas. Förfarande och rapportering vid skriftlig tillsyn eller fysisk inspektion:

- Den personuppgiftsansvarige skickar sitt tillsynsformulär till personuppgiftsbiträdet via e-post till **gdpr@itm8.com** med en begäran om tillsyn och/eller inspektion.
- Personuppgiftsbiträdet bekräftar mottagandet och anger slutdatum för revisionen och/eller inspektionen.
- Genomförandet av revisionen och/eller inspektionen sker.
- Den personuppgiftsansvarige vidarebefordrar eventuella iakttagelser från revisionen till **gdpr@itm8.com**.

- Personuppgiftsbiträdet granskar och kommenterar de iakttagelser som den personuppgiftsansvarige har gjort (kan upprepas flera gånger).
- Den personuppgiftsansvarige fastställer sin slutliga bedömning av revisionen och skickar rapporten till personuppgiftsbiträdet.
- Inspektionen avslutas.

C.8 Förfaranden för revisioner, inklusive inspektioner, av bearbetning av personuppgifter utförs av underleverantörer

Baserat på personuppgiftsbiträdets riskbedömning och med hänsyn till de specifika behandlingsaktiviteterna, de personuppgiftsbiträdet utför revisioner, inklusive inspektioner, av underleverantörer behandling av personuppgifter antingen i form av egenkontroll av revisionsutlåtanden och liknande (där så är möjligt), skriftlig tillsyn eller fysisk inspektion, eller en kombination av dessa.

Personuppgiftsansvarige maj, på de data kontrollantens begäran, få ytterligare information på de kontrollåtgärder som implementerats och tillämpats på varje underleverantör.

Bilaga D – Parternas överenskommelse om andra frågor

D.1 Allmänt

I förhållande till personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning har parterna enats om följande ytterligare villkor.

Klausulerna i detta avtal har företräde framför eventuella motsvarande bestämmelser i tjänsteavtal mellan parterna i den del som avser personuppgiftsbiträdets aktiviteter och ansvar kopplade till personuppgiftsbehandling, medan utförandet av samtliga andra aktiviteter relaterade till leverans av de avtalade Tjänsterna regleras av övriga delar av Tjänsteavtalet.

Övriga villkor i Tjänsteavtalet, inklusive ansvarsbegränsningar och liknande, ska även tillämpas på personuppgiftsbiträdets fullgörande av dessa klausuler.

Vid eventuell motstridighet mellan klausulerna och de villkor som anges i denna Bilaga D ska Bilaga D ha företräde, och om Tjänsteavtalet i övrigt innehåller villkor avseende personuppgiftsbiträdets behandlingsaktiviteter ska även Bilaga D ges företräde.

D.2 Konsekvenser av den personuppgiftsansvariges otillåtna instruktion

Den personuppgiftsansvarige är medveten om att personuppgiftsbiträdet är beroende av den personuppgiftsansvariges instruktioner för att avgöra i vilken omfattning personuppgiftsbiträdet är behörigt att använda och behandla personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet ska därför inte ansvara för krav som uppstår till följd av personuppgiftsbiträdets handlingar eller underlåtenheter i den mån sådana handlingar eller underlåtenheter utgör en personuppgiftsbehandlingsaktivitet som utförts i enlighet med den personuppgiftsansvariges instruktioner.

D.3 Införande av andra säkerhetsåtgärder

Personuppgiftsbiträdet har rätt att införa och upprätthålla alternativa säkerhetsåtgärder till dem som anges i avtalet om tillhandahållande av Tjänster och **Bilaga C1**, under förutsättning att sådana alternativa säkerhetsåtgärder sammantaget säkerställer en säkerhetsnivå som är likvärdig med de föreskrivna säkerhetsåtgärderna.

D.4 Användning av tredjepartstjänster

Oavsett vad som anges i punkt 7 i klausulerna är parterna överens om att, om personuppgiftsbiträdet använder underbiträden som identifierats i ett Tjänsteavtal som leverantörer av standardiserade tredjepartstjänster (Standard Third-Party Services), ska eventuella behandlingsaktiviteter som utförs av tredjepartsleverantörer (i egenskap av underbiträde) i samband med tillhandahållandet av dessa standardiserade tredjepartstjänster omfattas av tredjepartsleverantörens egna villkor för behandlingsaktiviteter som underbiträde.

Personuppgiftsbiträdet har gjort dessa villkor tillgängliga via Legal & Compliance på itm8, och det är den personuppgiftsansvariges eget ansvar att ta del av dem samt i övrigt säkerställa att villkoren på ett tillfredsställande sätt uppfyller kraven för tredjepartsleverantörens behandlingsaktiviteter.

Den personuppgiftsansvarige är medveten om att dessa villkor kan ändras av respektive tredjepartsleverantör löpande, och den personuppgiftsansvarige ska därför fortlöpande säkerställa att villkoren uppfyller kraven för behandlingsaktiviteterna.

Den personuppgiftsansvarige får när som helst kontakta personuppgiftsbiträdet för att erhålla tillämpliga villkor.

Genom att acceptera dessa klausuler accepterar och instruerar den personuppgiftsansvarige även att behandlingsaktiviteter utförs i enlighet med tredjepartsleverantörens villkor.

D.5 Radering och återlämnande av uppgifter

Parterna är överens om att den personuppgiftsansvarige ska instruera personuppgiftsbiträdet att radera och återlämna personuppgifterna i samband med att dessa klausuler upphör att gälla.

Den personuppgiftsansvarige ska, senast 30 dagar efter det att behandlingen av personuppgifter har upphört, underrätta personuppgiftsbiträdet om huruvida samtliga personuppgifter ska raderas eller återlämnas till den personuppgiftsansvarige. Om personuppgifterna ska återlämnas till den personuppgiftsansvarige ska personuppgiftsbiträdet även radera eventuella kopior. Personuppgiftsbiträdet ska säkerställa att även eventuella underbiträden följer den personuppgiftsansvariges instruktion.

Skyldigheten att radera gäller inte (i) kopior av elektroniskt utbytta personuppgifter som lagras som en del av automatiserade säkerhetskopieringsfunktioner, under förutsättning att åtkomsten är begränsad till IT-personal eller personal med ansvar för regelefterlevnad och att sådana uppgifter fortsatt behandlas i enlighet med dessa klausuler, samt (ii) personuppgifter som personuppgiftsbiträdet är skyldigt att bevara enligt tvingande lag.

Om personuppgiftsbiträdet inte har mottagit någon underrättelse från den personuppgiftsansvarige inom 30 dagar efter det att behandlingen av personuppgifter har upphört, ska personuppgiftsbiträdet skicka en påminnelse till den personuppgiftsansvarige. Om den personuppgiftsansvarige därefter inte underrättar personuppgiftsbiträdet om huruvida samtliga personuppgifter ska raderas eller återlämnas till den personuppgiftsansvarige, har personuppgiftsbiträdet rätt att radera personuppgifterna utan ytterligare underrättelse.

Personuppgiftsbiträdet har rätt till ersättning för sina behandlingsaktiviteter fram till dess att den personuppgiftsansvarige underrättar personuppgiftsbiträdet om huruvida samtliga personuppgifter ska raderas eller återlämnas till den personuppgiftsansvarige.

D.6 Ersättning

D.6.1 Bistånd – allmänt

Om inte personuppgiftsbiträdet, som en del av de avtalade Tjänsterna och inom ramen för det fasta priset för sådana Tjänster, har åtagit sig att fullgöra dessa klausuler, har personuppgiftsbiträdet rätt till ersättning för bistånd i enlighet med de biståndstjänster som avtalats i klausulerna, inklusive punkt 9.

Ersättningen beräknas utifrån nedlagd arbetstid och de i Tjänsteavtalet överenskomna timpriserna för tillhandahållande av Tjänster. Om inga timpriser har avtalats där, ska ersättningen beräknas enligt personuppgiftsbiträdets vid var tid gällande timpriser.

Eventuella externa kostnader som uppstår, inklusive kostnader som personuppgiftsbiträdet ådrar sig för bistånd från underbiträden, ska faktureras den personuppgiftsansvarige.

D.6.2 Införande av andra säkerhetsåtgärder

Om den personuppgiftsansvariges instruktioner med mera, samt personuppgiftsbiträdets löpande bedömningar, generellt medför strängare krav än de krav som anges i ett Tjänsteavtal avseende säkerhetsåtgärder för tillhandahållandet av Tjänster eller i Bilaga C och **Bilaga C1**, ska personuppgiftsbiträdet lojalt eftersträva att uppfylla sådana krav, i den mån detta är tekniskt möjligt och förenligt med uppfyllandet av andra krav för de berörda Tjänsterna.

Personuppgiftsbiträdet har rätt till ersättning och kostnadsersättning enligt samma principer som anges ovan.

D.6.3 Tillsyn och revision

Personuppgiftsbiträdet har rätt till ersättning för den personuppgiftsansvariges genomförande av tillsyn och revision. Ersättningen beräknas utifrån den nedlagda arbetstiden och de i Tjänsteavtalet avtalade timpriserna för tillhandahållande av Tjänster, eller – om inga timpriser har avtalats – enligt personuppgiftsbiträdets vid var tid gällande timpriser.

Eventuella externa kostnader som uppstår, inklusive kostnader som personuppgiftsbiträdet ådrar sig för bistånd från underbiträden, ska faktureras den personuppgiftsansvarige.

D.7 Ansvar och avtalsbrott

Varje överträdelse av klausulerna ska regleras och hanteras i enlighet med parternas Tjänsteavtal avseende tillhandahållande av Tjänster, med följande tillägg:

a) I de fall personuppgiftsbiträdet har erlagt ersättning till registrerade i enlighet med artikel 82 i dataskyddsförordningen (GDPR) eller Skadeståndslagen (1972:207) (”SkL”), ska personuppgiftsbiträdet ha full regressrätt gentemot den personuppgiftsansvarige för den del av ersättningen som överstiger den avtalade ansvarsbegränsningen i parternas Tjänsteavtal avseende tillhandahållande av Tjänster. Parterna har härmed avtalsvis avvikit från artikel 82.5 GDPR och Skadeståndslagen (1972:207).

b) Oaktat artikel 82.5 GDPR gäller att om personuppgiftsbiträdet har betalat ersättning till en

skadelidande part som inte motsvarar full ersättning, får personuppgiftsbiträdet utöva regress enligt den princip som följer av artikel 82.5 GDPR.

c) När det gäller annan ersättning för icke-ekonomiska skador till registrerade ska principen i artikel 82 GDPR även tillämpas vid den interna slutliga fördelningen av ansvar mellan personuppgiftsbiträdet och den personuppgiftsansvarige.

d) Parterna får inte kräva regress eller skadestånd av den andra parten för administrativa sanktionsavgifter eller andra offentligrättsliga påföljder som har påförts enligt dataskyddsförordningen (GDPR), inklusive sanktionsavgifter enligt artikel 83 i GDPR, eller enligt tillämplig svensk dataskyddslagstiftning.

e) Personuppgiftsbiträdets totala ansvar för överträdelser av klausulerna omfattas av den beloppsmässiga ansvarsbegränsning (och ingår i det maximala skadeståndsansvaret) som följer av parternas Tjänsteavtal. Ansvaret (inklusive eventuellt skadestånd eller annan ekonomisk ersättning som kan ha tillerkänts den personuppgiftsansvarige enligt Tjänsteavtalet) ska vara begränsat till ett belopp som understiger 150 % av det belopp som personuppgiftsbiträdet har erhållit under de tolv (12) månader som föregått den skadevållande händelsen. Om en period om tolv månader ännu inte har förflutit ska ansvarsbegränsningen beräknas som genomsnittet av de belopp som erhållits under de månader som förflutit, multiplicerat med tolv (12).

f) Personuppgiftsbiträdets ansvar för överträdelser av klausulerna omfattar inte indirekt skada, inklusive driftförlust, följdskada eller annan indirekt förlust.

g) Personuppgiftsbiträdet ansvarar inte för överträdelser av klausulerna som orsakas av datorvirus, cyberbrottslighet eller andra former av obehörigt intrång från tredje man i den personuppgiftsansvariges eller personuppgiftsbiträdets IT-system, såvida förlusten inte är direkt hänförlig till underlåtenhet att uppfylla överenskomna säkerhetskrav enligt parternas Tjänsteavtal.

D.8 Nationella särregler

Om den personuppgiftsansvarige är etablerad utanför Sverige gäller särskilda krav i enlighet med nationella dataskyddsbestämmelser i den personuppgiftsansvariges hemland. Dessa nationella särregler framgår av **Bilaga D8 .**