



2023

## **DPA-avtal**

Personuppgiftsansvarig:

Personuppgiftsbiträde:

Amesto Solutions AB

## Standardavtalsklausuler

Standardavtalsklausuler enligt artikel 28.3 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen)

Företagsnamn:

Organisationsnummer:

Adress:

(Personuppgiftsansvarig)

Och

**Amesto Solutions AB**

Organisationsnummer: 556210-6681

Vasagatan 11

111 20 Stockholm

SVERIGE

(personuppgiftsbiträde)

var och en "part", tillsammans "parterna"

Har enats om följande avtalsklausuler ("klausulerna") för att uppfylla kraven i den allmänna dataskyddsförordningen och säkerställa skyddet av den registrerades rättigheter. Eventuellt intressebolag måste anges i bilaga E för att omfattas av gällande avtal

## Innehållsförteckning

1	Ingress.....	4
2	Den personuppgiftsansvariges rättigheter och skyldigheter .....	4
3	Personuppgiftsbiträden ska följa anvisningarna .....	5
4	Sekretess .....	5
5	Säkerhet vid behandling .....	5
6	Användning av underleverantörer .....	6
7	Överföring av uppgifter till tredjeland eller internationella organisationer.....	7
8	Stöd till den personuppgiftsansvarige .....	8
9	Underrättelse om personuppgiftsincident.....	10
10	Radera och återlämna uppgifter .....	10
11	Granskning och inspektion .....	10
12	Parternas överenskommelse om andra villkor.....	11
13	Inledande och avslutande.....	12
14	Kontakter/kontaktpunkter för den personuppgiftsansvarige och personuppgiftsbiträdet .....	13
	Tillägg A Information om behandlingen .....	14
	Tillägg B Godkända underleverantörer .....	16
	Tillägg C Instruktioner för användning av personuppgifter .....	17
	Tillägg D Parternas reglering av andra frågor .....	20

## 1 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 tjänster i enlighet med huvudavtalet ingått mellan parterna 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 personuppgiftsbitrådets 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.

## 2 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 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.

### **3 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 personuppgiftsbitrådets uppfattning inte följer den allmänna dataskyddsförordningen eller tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten.

### **4 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.

### **5 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 avseende fysiska personers rättigheter och friheter vid behandlingen och vidta nödvändiga åtgärder för att minska dessa risker. Det innebär att den personuppgiftsansvarige 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.
  4. Om därefter – enligt den personuppgiftsansvariges bedömning – en reducering av identifierade risker kräver att ytterligare åtgärder vidtas av personuppgiftsbiträdet för att minska risken, 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.

## 6 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.

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 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.

3. 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.

4. 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.
5. 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 anlitas av personuppgiftsbiträdet följer avtalet, t.ex. genom att låta den personuppgiftsansvarige ge underleverantören i uppgift att ta bort eller återlämna personuppgifter.
6. 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.

## **7 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.

## 8 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 personuppgiftsbitrådets skyldighet att bistå den personuppgiftsansvarige enligt klausul 6.4, ska personuppgiftsbitrådet dessutom, med beaktande av behandlingens art och den information som finns tillgänglig för personuppgiftsbitrådet, 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, 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, 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 personuppgiftsbitrådet ska bistå den personuppgiftsansvarige med, samt omfattningen för det stöd som krävs. Detta avser de skyldigheter som anges i klausul 8.1 och 8.2.

## 9 Underrättelse om personuppgiftsincident

1. Vid en personuppgiftsincident ska personuppgiftsbiträdet, utan onödigt dröjsmål efter upptäckten, anmäla incidenten till personuppgiftsansvarige.
2. Personuppgiftsbitrådets underrättelse till den personuppgiftsansvarige ska om möjligt äga rum inom 72 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 8.2 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.

## 10 Radera och återlämna uppgifter

1. När personuppgiftsbehandlingen avslutas ska personuppgiftsbiträdet återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior, såvida inte det enligt unionens eller medlemsstatens lagstiftning krävs att personuppgifterna lagras.
2. Personuppgiftsbiträdet ska också löpande radera personuppgifter i enlighet med avtalet och de villkor som är fastställda enligt Bilaga C, punkt 4.

## 11 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 personuppgiftsbitrådets lokaler, eller ombud som agerar på uppdrag av sådana tillsynsmyndigheter, tillgång till personuppgiftsbitrådets fysiska lokaler vid uppvisande av lämplig id-handling.

## **12 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.

## 13 Inledande och avslutande

1. Klausulerna börjar gälla det datum då båda parter har undertecknat dem.
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 10.1 och tillägg C.4, kan klausulerna upphävas skriftligen av någon av parterna.

### 5. Underskrift

På uppdrag av den personuppgiftsansvarige

Namn

Befattning

Datum

Underskrift

På uppdrag av personuppgiftsbiträdet

Namn

Befattning

Datum

Underskrift

## 14 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.

- a. För den personuppgiftsansvarige

KONTAKT 1:

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

KONTAKT 2:

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

- b. För Personuppgiftsbiträdet

KONTAKT 1:

Namn
Telefonnummer
E-postadress

KONTAKT 2:

Namn
Befattning
Telefonnummer
E-postadress

## Tillägg A Information om behandlingen

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

Syftet med behandlingen är att på uppdrag av personuppgiftsansvarig bistå med support, underhåll och utveckling av standardprogramvara. I och med detta kommer personuppgiftsbiträde behandla personuppgifter genom:

- Tidsbegränsad åtkomst från egen dator
- Åtkomst från egen dator
- Temporär och tidsbegränsad lagring/behandling av personuppgifter, t.ex på dator eller Azure Cloud
- Lagring/behandling av personuppgifter utanför personuppgiftsansvarigs miljö, i t.ex Azure, Amesto Flow

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

Behandlingen avser åtkomst till personuppgiftsansvarigs personuppgifter. Syftet med uppdraget är inte att förädla eller bearbeta personuppgifter, annat än i undantagsfall, vid till exempel rensning av personuppgifter eller import av personuppgifter.

Vid arbete med personuppgiftsansvarigs systemstöd inom ERP, CRM och HRM med tillhörande applikationer, rapporteringslösningar och integrationer kommer personuppgiftsbiträdet att ha tillgång till personuppgifter, uppkopplat eller i bitrådets egen miljö.

### A.3. Behandlingen inkluderar följande typer av personuppgifter om registrerade, dock varierande beroende på vilken typ av personuppgifter den personuppgiftsansvarige har lagrat i sina system:

**Kontaktinformation, såsom:**

För- och Efternamn, Telefon, Adress, e-postadress, födelsedatum, anställningsförhållande.

**Personuppgiftsansvarigs kunder och övriga intressenters personal såsom:** Titel, arbetsgivare, yrkesmässiga intressen, löpande kommunikation i form av händelser och dokument/e-post.

**Vid förekommande fall med HRM-system såsom:** Anställdas Namn, e-post, mobiltelefon, anställningsnummer, roll, titel, chef, förrättningsområde, arbetsställe, personnummer.

### A.4. Behandlingen inkluderar följande kategorier av registrerade, dock varierande beroende på vilken typ av personuppgifter den personuppgiftsansvarige har lagrat i sina system:

- Personuppgiftsansvarigs slutanvändare
- Personuppgiftsansvarigs kunders, prospects och övriga intressenters personal
- Anställda hos personuppgiftsansvarig

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

Behandling/Access	Lagring av personuppgifter eller åtkomst	JA	NEJ
Från egen dator, av personuppgiftsansvarig reglerad tidsbegränsad åtkomst, för t.ex support, design, teknik- eller utveckling	Ingen persondata lagras. Åtkomst avslutas direkt efter avslutad session.	X	
Från egen dator, via bitrådets egna anslutningsuppgifter, åtkomst för t.ex support, design, teknik- eller utveckling	Ingen persondata lagras. Anslutningsuppgifter raderas i samband med terminering av avtal, när anställd slutar eller på personuppgiftsansvarigs instruktion.	X	
Temporär och tidsbegränsad lagring/behandling av personuppgifter utanför personuppgiftsansvarigs miljö, t.ex på dator, mail, server hos Amesto.	Raderas 30 dagar efter uppdragets godkännande eller på personuppgiftsansvarigs instruktion.		X
Ej tidsbegränsad lagring/behandling av personuppgifter utanför personuppgiftsansvarigs miljö, i t.ex Azure, Amesto Flow - SaaS	Raderas 30 dagar efter uppdragets avslutande eller på personuppgiftsansvarigs instruktion.		X

## Tillägg B Godkända underleverantörer

### B.1. Godkända underleverantörer

Nedanför listas de, vid var tid, underleverantörer som är godkända av den personuppgiftsansvarige:

NAMN	ORGANISATIONSNR	LAND	BESKRIVNING AV BEHANDLINGEN
Bolag inom koncernen "Amesto TechHouse A/S"	938473617	Norge, Sverige och Danmark	Amesto Solutions AB kan använda sig av systerföretag inom koncernen när det löser uppkomna behov.

Den personuppgiftsansvarige godkänner när klausulerna börjar gälla 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

Godkännande av underleverantör ska skriftligt godkännas innan underleverantör får användas för angiven behandling.



## Tillägg C Instruktioner för användning av personuppgifter

### C.1. Omfattningen av/instruktioner för behandlingen

#### Skyldigheter som personuppgiftsbiträde

Personuppgiftsbiträdet ska endast behandla personuppgifter i den utsträckning som krävs för att utföra uppdragen och fullgöra sina skyldigheter enligt huvudavtalet eller det beskrivna uppdraget.

#### Konfidentialitet och tystnadsplikt

Personuppgiftsbiträdet ska se till att behöriga personer är skyldiga att behandla personuppgifterna konfidentiellt, eller att de omfattas av lagstadgad tystnadsplikt. Detta görs genom ett undertecknat sekretessavtal som ingås i samband med anställningen hos Amesto.

Tystnadsplikten gäller även efter det att databehandlingsuppdraget har slutförts.

Personuppgiftsbiträdet ska endast auktorisera personer som måste ha tillgång till personuppgifterna av nödvändiga skäl.

Om instruktionerna bryter mot gällande regler, och den personuppgiftsansvarige informeras om detta men anser att hantering är nödvändig för att slutföra uppdraget, kommer ansvaret för behandlingen att ligga hos den personuppgiftsansvarige.

### C.2. Säkerhet vid behandlingen

Personuppgiftsbiträdet vidtar alla nödvändiga åtgärder enligt artikel 32 i personuppgiftslagen. *Säkerhet vid behandling.*

*Amesto-dator som har godkänts enligt Amestos säkerhetspolicy innebär bland annat att datorn stänger ute andra, endast giltigt konto kan logga in sig på enheten. Använder Remote Wipe vid förlust av dator för att skydda innehållet.*

*Refererar till Amestos integritetspolicy punkt 3. <https://www.amestosolutions.se/om-amesto-solutions/integritetspolicy/>*

Överföring av data som innehåller uppgifter från personuppgiftsansvarig till personuppgiftsbiträdet ska ske genom användning av säkra överföringssystem enligt överenskommelse med personuppgiftsansvarig.

### C.3. Assistans till personuppgiftsansvarig

Personuppgiftsbiträdet ska, i möjligaste mån – inom den omfattning och i den utsträckning som anges nedan – bistå personuppgiftsansvarig i enlighet med punkt 8.1 och 8.2 genom att införa följande tekniska och organisatoriska åtgärder:

Se Amestos integritetspolicy, punkt 3:

<https://www.amesto.com/amesto-trust-center/privacy/integritetspolicy/>

Se också Amesto Trust Center:

Amesto Trust Center: <https://www.amesto.com/amesto-trust-center/>

#### C.4. Procedur för lagringstid/radering

Behandling/Access	Lagring av personuppgifter eller åtkomst
Från egen dator, av personuppgiftsansvarig reglerad tidsbegränsad åtkomst, för t.ex. support, design, teknik- eller utveckling	Inga personuppgifter lagras. Åtkomsten avslutas omedelbart efter att uppdraget har slutförts
Från egen dator, via bitrådets egna anslutningsuppgifter, åtkomst för t.ex support, design, teknik- eller utveckling	Inga personuppgifter lagras. Åtkomstinformation raderas i samband med uppsägning av avtalet, när den anställda på Amesto Solutions avslutar sin tjänst eller på personuppgiftsansvarigs begäran
Tillfällig och tidsbegränsad lagring/behandling av personuppgifter utanför den personuppgiftsansvariges egen miljö, på t.ex. dator, i mejl, server hos Amesto	Raderas 30 dagar efter uppdragets godkännande eller på personuppgiftsansvarigs instruktion
Ej tidsbegränsad lagring/behandling av personuppgifter utanför den personuppgiftsansvariges egen miljö. I t.ex. Azure, Amesto Flow - Saas	Raderas 30 dagar efter uppdragets godkännande eller på personuppgiftsansvarigs instruktion

#### C.5. Behandlingsplats

Behandlingen sker i personuppgiftsbitrådets utvecklings-/administrations-/systemutvecklings- och driftsmiljö i Norge, Sverige och Danmark.

Om platsen ligger utanför EU/EES (tredje land) eller om plats som anges här ändras, ska den hanteras enligt punkt 7 i personuppgiftsbiträdesavtalet.

#### C.6 Instruktioner för överföring av personuppgifter till tredje land

Personuppgiftsbitrådet får endast behandla personuppgifter enligt den personuppgiftsansvariges instruktioner när det gäller överföring av personuppgifter till tredje land eller internationella organisationer, såvida inte sådan behandling krävs enligt EU-lagstiftningen eller medlemsstaternas nationella lagstiftning som personuppgiftsbitrådet omfattas av; i så fall ska personuppgiftsbitrådet underrätta personuppgiftsansvarig om detta rättsliga krav före behandlingen, förutsatt gällande lagstiftning inte förbjuder sådan underrättelse av hänsyn till viktiga samhällsintressen, jf art 28 punkt 3a.

Om personuppgiftsansvarig inte föreskriver det i dessa bestämmelser eller i ett senare skede ger en dokumenterad instruktion om överföring av personuppgifter till tredje land, ska personuppgiftsbitrådet inte ha rätt att göra sådana överföringar.

### C.7 Procedurer för personuppgiftsansvariges revisioner, inklusive inspektioner, för behandlingen av personuppgifter som har överlåtits till personuppgiftsbiträdet

Personuppgiftsbiträdet ska på skriftlig begäran förse den personuppgiftsansvarige med dokumentation av de tekniska och organisatoriska åtgärderna som har vidtagits för att säkerställa en lämplig säkerhetsnivå, samt annan information som är nödvändig för att dokumentera, personuppgiftsbitrådets efterlevnad av dataskyddsförordningen, dataskyddsbestämmelser i annan EU-lagstiftning eller medlemsstaternas nationella lagstiftning och dessa bestämmelser.

Personuppgiftsansvarig ska ha rätt att en gång om året för egen räkning erhålla en revisionsförklaring från en oberoende tredje part på egen bekostnad. Den personuppgiftsansvarige ska stå för alla kostnader i samband med revisionen, och personuppgiftsbiträdet har rätt till ersättning för alla kostnader som uppkommer till följd av revisionen, inklusive ersättning till personuppgiftsbiträdet för rimlig tid som personuppgiftsbiträdet och dennes personal har avsatt för att bistå under revisionen.

Personuppgiftsbiträdet ska dock stå för sådana kostnader om en revision visar på väsentliga brister i fullgörandet av de skyldigheter som framgår av dessa bestämmelser eller personuppgiftslagstiftningen.

Baserat på resultatet av förklaringen har personuppgiftsbiträdet rätt att begära att ytterligare åtgärder vidtas för att säkerställa att dataskyddsförordningen, dataskyddsbestämmelser i annan EU-lagstiftning eller medlemsstaternas nationella lagstiftning och dessa bestämmelser.

## Tillägg D Parternas reglering av andra frågor

### D.1. Meddelande om brott mot säkerheten för personuppgifter

Personuppgiftsbiträdet ska tillhandahålla rimlig hjälp så att personuppgiftsansvarig kan fullgöra sina skyldigheter att lämna ut tilläggsinformation till tillsynsmyndigheten och de registrerade.

### D.2. Meddelande om brott mot säkerheten för personuppgifter

Personuppgiftsbiträdet ska vidta nödvändiga och lämpliga korrigerande åtgärder. Personuppgiftsbiträdet ska också samarbeta med personuppgiftsansvarig för att förebygga, minimera konsekvenserna av eller korrigera säkerhetsincidenter.

### D.3. Ansvar

Ingen part ska vara ansvarig gentemot den andra för indirekta förluster eller följdskador av något slag (inklusive men inte begränsat till förlust till följd av driftavbrott, förlust av data, utebliven vinst eller liknande) oavsett ansvarsgrund, oavsett om det är i avtal, culpa-ansvar, produktansvar eller annat, även om parten har informerats om möjligheten för sådana skador (gemensamt kallat "indirekt förlust").

Ingen part ska vara ansvarig gentemot den andra för;

- a) fel eller förseningar som ligger utanför partens rimliga kontroll, inklusive allmänna internet- eller linjefördröjningar, strömavbrott eller fel på maskiner eller
- b) fel som orsakats av den andra partens system eller handlingar, vårdslöshet eller försummelser, som endast ska vara den partens ansvar.

Det totala och maximala ansvaret för varje period om tolv (12) månader för en part gentemot den andra under eller i enlighet med detta personuppgiftsbiträdesavtal, får under inga omständigheter överstiga ett belopp motsvarande det totala belopp som har betalats för tjänsten enligt avtalet under de tolv (12) föregående månaderna före handlingen som orsakade skadan.

Ovannämnda begränsningar gäller inte för skador till följd av bedrägeri, grov vårdslöshet eller uppsåt.

## Tillägg E Berörda bolag.

Nedanför listas de företag som är berörda av detta avtal.

FÖRETAGSNAMN	ORGANISATIONSNUMMER

**Simplifying business.**

