

Personuppgiftsbiträdesavtal

Innehållsförteckning

1	PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER.....	2
2	DEFINITIONER	2
3	BAKGRUND OCH SYFTE.....	4
4	BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION	4
5	DEN PERSONUPPGIFTSANSVARIGES ANSVAR	4
6	PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN	4
7	SÄKERHETSÅTGÄRDER	5
8	SEKRETESS/TYSTNADSPLIKT	6
9	GRANSKNING, TILLSYN OCH REVISION	6
10	HANTERING AV RÄTTELSE OCH RADERING M.M.	7
11	PERSONUPPGIFTSINCIDENTER	7
12	UNDERBITRÄDE	8
13	LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND	9
14	ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING.....	9
15	PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING.....	9
16	ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.....	9
17	ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE.....	10
18	MEDDELANDE INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER.....	10
19	KONTAKTPERSONER	10
20	ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER.....	11
21	LAGVAL OCH TVISTER.....	11

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679¹

1 PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	Personuppgiftsbiträde
	Utilitas
Organisationsnummer	Organisationsnummer
	802555-0925
Postadress	Postadress
	Utilitas Box 2861 116 74 Stockholm
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	Kontaktperson för administration av detta personuppgiftsbiträdesavtal
Namn: E-post: Tfn:	Namn: Martin Forster E-post: kontakt@utilitas.nu Tfn: 0709-424225
Person ansvarig för dataskydd (som undertecknar detta avtal)	Person ansvarig för dataskydd (som undertecknar detta avtal)
Namn: E-post: Tfn:	Namn: Martin Forster E-post: kontakt@utilitas.nu Tfn: 0709424225

2 DEFINITIONER

- 2.1 Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner, oavsett om de används i plural eller singular, i bestämd eller

¹ Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbitrådets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

Behandling

En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring

Dataskyddslagstiftning

Avser all integritets- och personuppgiftslagstiftning, samt annan lagstiftning, förordningar och föreskrifter som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning

Personuppgiftsansvarig

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.

Instruktion

De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.

Logg

Logg är resultatet av Loggning.

Loggning

Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.

Personuppgiftsbiträde

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning

Personuppgift

Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsincident

En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.

Registrerad

Fysisk person vars Personuppgifter Behandlas.

Tredje land

En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).

Underbiträde

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3 BAKGRUND OCH SYFTE

- 3.1 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt "PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad som stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen").
- 3.2 När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet "Huvudavtalet" i PUB-avtalet.
- 3.3 För det fall något av det som stadgas i avsnitt 1, punkt 3.2, avsnitt 15 eller 16, punkt 17.6, avsnitt 18–20 eller **Fel! Hittar inte referenskälla.** i PUB-avtalet regleras på annat sätt i Huvudavtalet, ska Huvudavtalets reglering ha företräde.
- 3.4 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

4 BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

- 4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.
- 4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.
- 4.3 Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

5 DEN PERSONUPPGIFTSANSVARIGES ANSVAR

- 5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner med hänsyn till Behandlingens art så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.
- 5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.
- 5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6 PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

- 6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och för de specifika ändamål som anges i Instruktioner samt att följa

Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

- 6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet och Instruktioner.
- 6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.
- 6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.
- 6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner, om inte parterna kommer överens om annat.
- 6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7 SÄKERHETSÅTGÄRDER

- 7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas. De säkerhetsåtgärder som Personuppgiftsbiträdet ska vidta framgår av Bilaga 2 – Dataskydd och informationssäkerhet.
- 7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.
- 7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.
- 7.4 Personuppgiftsbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbitrådets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.
- 7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.
- 7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8 SEKRETESS/TYSTNADSPLIKT

- 8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, varken direkt eller indirekt, såvida inte annat avtalats.
- 8.2 Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.
- 8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.
- 8.4 Om den Registrerade, tillsynsmyndighet eller tredje man riktar en begäran till Personuppgiftsbiträdet som rör Behandlingen, ska Personuppgiftsbiträdet utan onödigt dröjsmål vidarebefordra begäran till den Personuppgiftsansvarige och i övrigt avstå från att själv besvara eller handlägga begäran, såvida inte Personuppgiftsbiträdet är rättsligt förpliktat enligt tvingande lag att lämna information eller har fått uttrycklig och skriftlig instruktion från den Personuppgiftsansvarige; i sådant fall ska utlämnande begränsas till vad som är nödvändigt och ske i enlighet med den Personuppgiftsansvariges instruktioner.

9 GRANSKNING, TILLSYN OCH REVISION

- 9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.
- 9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.
- 9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbitrådets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.
- 9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2–9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning

genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

- 9.5 Personuppgiftsbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.
- 9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt avsnitt 9 i PUB-avtalet.

10 HANTERING AV RÄTTELSE OCH RADERING M.M.

- 10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbitrådets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella Personuppgiften som ett led i processen för rättelse eller radering.
- 10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad som stadgas om meddelanden i avsnitt 18 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11 PERSONUPPGIFTSINCIDENTER

- 11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1.c i Dataskyddsförordningen.
- 11.2 Personuppgiftsbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.
- 11.3 Vid Personuppgiftsincident, vilken Personuppgiftsbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.
- 11.4 Beskrivningen ska redogöra för:
 - a. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
 - b. de sannolika konsekvenserna av Personuppgiftsincidenten, och

- c. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftsincidentens potentiella negativa effekter.
- 11.5 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkten 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12 UNDERBITRÄDE

- 12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckningen över Underbiträden. Aktuell lista över underbiträden finns på <https://www.ipsykologi.se/underbitraden>. Den personuppgiftsansvarige ska informeras om ändringar och har rätt att invända.
- 12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar den Behandling som Underbiträdet utför å den Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier. Underbiträdet ska genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddslagstiftningen. I fråga om dataskydd ska avtalet ålägga Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.
- 12.3 Personuppgiftsbiträdet ska i avtalet med Underbiträdet säkerställa att den Personuppgiftsansvarige har rätt att säga upp Underbiträdet och instruera Underbiträdet att exempelvis radera eller återlämna Personuppgifterna om Personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller hamnat på obestånd.
- 12.4 Personuppgiftsbiträdet ansvarar fullt ut för Underbitrådets Behandling gentemot den Personuppgiftsansvarige. Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om Underbiträdet underlåter att uppfylla sina skyldigheter i PUB-avtalet.
- 12.5 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden om inte annat anges i Instruktionen.
- 12.6 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbitrådets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om
- a. Underbitrådets namn, organisationsnummer och säte (adress och land),
 - b. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
 - c. var Personuppgifterna ska behandlas.
- 12.7 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.6 invända mot Personuppgiftsbitrådets anlitande av ett nytt Underbiträde och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkten 16.4.
- 12.8 Personuppgiftsbiträdet ska vid var tid föra en korrekt och uppdaterad förteckning över de Underbiträden som anlitas för Behandling av Personuppgifter för den Personuppgiftsansvariges räkning samt göra denna förteckning tillgänglig för den Personuppgiftsansvarige. Av förteckningen ska särskilt framgå i vilket land Underbiträdet behandlar Personuppgifterna och vilka typer av Behandlingar som Underbiträdet utför.
- 12.9 När Personuppgiftsbiträdet slutar använda ett Underbiträde ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om detta. Personuppgiftsbiträdet ska när ett avtal upphör säkerställa att Underbiträdet raderar eller återlämnar Personuppgifterna.

- 12.10 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Underbitrådets Behandling av Personuppgifter och förteckningen över Underbiträden enligt punkten 12.1.

13 LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

- 13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.
- 13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.
- 13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14 ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

- 14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.
- 14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.
- 14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten utan onödigt dröjsmål informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.
- 14.4 Oaktat vad som sägs i Huvudavtalet gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan parterna av krav sinsemellan såvitt avser Behandlingen.

15 PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

- 15.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tills vidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

16 ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

- 16.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.
- 16.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

- 16.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.
- 16.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitan­de av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.6, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

17 ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

- 17.1 Efter uppsägning av PUB-avtalet ska Personuppgiftsbiträdet utan onödigt dröjsmål, beroende på vad den Personuppgiftsansvarige väljer, antingen radera och intyga för den Personuppgiftsansvarige att det är utfört, eller återlämna
- a. alla Personuppgifter som Behandlats för den Personuppgiftsansvariges räkning
- 17.2 I samband med återlämning ska Personuppgiftsbiträdet även radera befintliga kopior av Personuppgifter och tillhörande information.
- 17.3 Skyldigheten att radera eller återlämna Personuppgifter eller tillhörande information gäller inte om lagring av Personuppgifterna eller informationen krävs enligt unionsrätten eller relevant nationell rätt där Behandling får utföras enligt PUB-avtalet.
- 17.4 Om Personuppgifter återlämnas ska det ske i ett allmänt använt och standardiserat format, om parterna inte har kommit överens om något annat format.
- 17.5 Till dess att uppgifterna raderas eller återlämnas ska Personuppgiftsbiträdet säkerställa efterlevnaden av PUB-avtalet.
- 17.6 Återlämning eller radering enligt PUB-avtalet ska vara utförd senast trettio (30) kalenderdagar räknat från tidpunkten för uppsägningen av PUB-avtalet, om inte annat anges i Instruktionen. Behandling av Personuppgifter som Personuppgiftsbiträdet utför därefter är att betrakta som otillåten Behandling.
- 17.7 Bestämmelser om sekretess/tystnadsplikt i avsnitt 8 ska fortsätta gälla även om PUB-avtalet i övrigt upphör att gälla.

18 MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

- 18.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för PUB-avtalet.
- 18.2 Meddelanden om parternas samarbete om dataskydd gällande Behandlingen ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för parternas samarbete om dataskydd.
- 18.3 Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

19 KONTAKTPERSONER

- 19.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.
- 19.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

20 ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

- 20.1 Varje part ansvarar för att de uppgifter som anges i avsnitt 1 i PUB-avtalet alltid är aktuella och korrekta.
- 20.2 Ändring av uppgifter i avsnitt 1 ska meddelas motparten enligt punkt 18.1 i PUB-avtalet.

21 LAGVAL OCH TVISTER

- 21.1 Vid tolkning och tillämpning av PUB-avtalet gäller svensk rätt med undantag för lagvals-reglerna. Tvister med anledning av PUB-avtalet ska avgöras av behörig svensk domstol.
-

Personuppgiftsansvarig

Ange organisationens fullständiga namn

Ort

Namnförtydligande

Signatur

Personuppgiftsbiträde

Utilitas

Stockholm

Namnförtydligande

Signatur

Bilaga 1 - Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

1. Ändamålet, föremålet och arten
1 a. Föremålet för Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att: Tillhandahålla, drifta och underhålla en webbaserad plattform för internetbaserade utbildnings- och stödinsatser, inklusive tillhörande funktioner för användaradministration, kursgenomförande och dokumentation av deltagande. 1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att: Möjliggöra för den Personuppgiftsansvarige att administrera, genomföra och följa upp utbildnings- och stödinsatser för registrerade användare inom ramen för den Personuppgiftsansvariges verksamhet. Personuppgiftsbiträdet behandlar Personuppgifterna uteslutande i syfte att tillhandahålla den tekniska plattformen och tillhörande funktionalitet och behandlar inte Personuppgifterna för egna ändamål. 1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur): Personuppgiftsbiträdets Behandling av Personuppgifter sker huvudsakligen genom automatiserade och systemstyrda behandlingsåtgärder och omfattar i huvudsak: • registrering och lagring av Personuppgifter i databaser, • strukturering och organisering av Personuppgifter för åtkomst via behörighetsstyrda gränssnitt, • tillhandahållande av läs- och skrivåtkomst för behöriga användare som den Personuppgiftsansvarige administrerar, • överföring av Personuppgifter inom plattformen i samband med användning av dess funktioner, • säkerhetskopiering, loggning och teknisk drift i syfte att upprätthålla informationssäkerhet och tillgänglighet. Personuppgiftsbiträdet och dess underbiträden tar inte del av Personuppgifternas innehåll annat än i den mån det är nödvändigt för felsökning, support eller säkerhetsåtgärder, och endast på dokumenterad instruktion från den Personuppgiftsansvarige.
2. Behandlingen omfattar följande typer av Personuppgifter
Personuppgiftsbiträdet har rätt att behandla följande typer av Personuppgifter för den Personuppgiftsansvariges räkning: Personuppgiftsbiträdet har rätt att behandla följande kategorier av Personuppgifter för den Personuppgiftsansvariges räkning: a) Identifierande och administrativa uppgifter Uppgifter som möjliggör identifiering och administration av användare i plattformen, såsom namn, kontaktuppgifter, organisatorisk tillhörighet och användaridentiteter.

b) Uppgifter om levnadsförhållanden och bakgrund

Uppgifter om demografiska och socioekonomiska förhållanden, såsom ålder, utbildningsnivå, sysselsättning, familjesituation och motsvarande bakgrundsvariabler.

c) Uppgifter om deltagande och användning

Uppgifter om registrering, deltagande, genomförande och aktivitet i utbildnings- eller stödinsatser inom plattformen.

d) Särskilda kategorier av personuppgifter enligt artikel 9 i Dataskyddsförordningen

Uppgifter om hälsa och närliggande förhållanden, såsom enkätsvar eller självskattningar avseende psykiskt eller fysiskt mående, beteenden eller relaterade omständigheter.

e) Fritextuppgifter

Uppgifter som Registrerade själva lämnar i fritextfält inom ramen för plattformens funktioner, vilka kan innehålla personuppgifter och i förekommande fall även särskilda kategorier av personuppgifter.

Personuppgiftsbiträdet behandlar Personuppgifterna uteslutande i enlighet med den Personuppgiftsansvariges instruktioner och utan att själv fastställa innehållet i eller ändamålet med uppgifterna.

3. Behandlingen omfattar vissa kategorier av Registrerade

Personuppgiftsbiträdet har rätt att Behandla Personuppgifter avseende följande kategorier av Registrerade:

Personuppgiftsbiträdet har rätt att behandla Personuppgifter avseende följande kategorier av Registrerade:

- personer som av den Personuppgiftsansvarige registrerats som deltagare eller användare av plattformen, såsom
 - brukare, klienter eller deltagare i utbildnings- eller stödinsatser,
 - vårdnadshavare eller närstående,
 - anställda eller uppdragstagare hos den Personuppgiftsansvarige i den mån dessa använder plattformen.

4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

Personuppgiftsbiträdet ska iaktta följande hanteringskrav vid Behandlingen av Personuppgifter åt den Personuppgiftsansvarige:

Personuppgiftsbiträdet ska iaktta följande hanteringskrav vid Behandlingen av Personuppgifter:

- Personuppgifter, inklusive särskilda kategorier av personuppgifter, behandlas endast i enlighet med dokumenterade instruktioner från den Personuppgiftsansvarige.
- Personuppgiftsbiträdet avgör inte vilka Personuppgifter som ska registreras i plattformen eller vilket innehåll som ska lämnas i fritextfält; detta ansvar åvilar den Personuppgiftsansvarige.
- Personuppgifter lagras i plattformen tills dess att den Personuppgiftsansvarige raderar, anonymiserar uppgifterna eller instruerar om gallring.

• Personuppgiftsbiträdet tillhandahåller funktioner för radering, anonymisering och avaktivering av användarkonton i enlighet med den Personuppgiftsansvariges instruktioner. • Åtkomst till Personuppgifter regleras genom behörighets- och rollbaserad åtkomstkontroll som administreras av den Personuppgiftsansvarige. • Säkerhetskopior används uteslutande för återställning vid incidenter och sparas under begränsad tid enligt fastställda rutiner.
5. Ange de särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbitrådets Behandling av Personuppgifter Personuppgiftsbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna: Personuppgiftsbiträdet ska vidta följande tekniska och organisatoriska säkerhetsåtgärder vid Behandlingen av Personuppgifter, inklusive särskilda kategorier av Personuppgifter: Organisatoriska säkerhetsåtgärder • fastställda styrdokument och rutiner för informationssäkerhet och dataskydd, • utsedd funktion med ansvar för dataskydd och informationssäkerhet, • rutiner för identifiering, rapportering och hantering av personuppgiftsincidenter. Säkerhetsåtgärder avseende personer • åtkomst till Personuppgifter begränsas till behörig personal med behov av åtkomst för drift eller support, • personal omfattas av sekretessförpliktelser, • utbildning i dataskydd och informationssäkerhet för relevant personal. Fysiska säkerhetsåtgärder • servermiljöer skyddas genom underbitrådets fysiska säkerhetsåtgärder, såsom inpasseringskontroll, övervakning och skydd av serverhallar. Tekniska säkerhetsåtgärder • kryptering av Personuppgifter vid överföring (t.ex. TLS), • behörighetsstyrd autentisering, • loggning av åtkomst och systemhändelser, • skydd mot obehörig åtkomst, intrång och skadlig kod, • regelbundna säkerhetskopior och rutiner för återställning av data.
6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem Personuppgiftsbiträdet ska iaktta följande krav avseende loggning av användaraktivitet och systemåtkomst: • loggar ska användas för säkerhetsändamål, felsökning och incidentutredning, • loggar ska endast vara tillgängliga för behörig personal, • loggar ska sparas under begränsad tid i enlighet med fastställda rutiner och därefter raderas eller anonymiseras.
7. Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgiftsbiträdet ska iaktta följande krav avseende lokalisering av Personuppgifter:
Personuppgiftsbiträdet har endast rätt att behandla Personuppgifterna på följande plats/er:

Sverige, genom drift av plattformen hos extern hostingleverantör. I förekommande fall inom Europeiska unionen (EU/EES), i den mån tekniska drift- eller supportåtgärder kräver detta och i enlighet med gällande personuppgiftsbiträdesavtal med underbiträden.

Om den Personuppgiftsansvarige inte har gett anvisningar om överföring av Personuppgifter till ett Tredje land i Instruktionen, har Personuppgiftsbiträdet inte rätt att göra en sådan överföring.

Personuppgiftsbiträdet ska iaktta följande krav avseende överföring av Personuppgifter till Tredje land:

Personuppgiftsbiträdet överför inte Personuppgifter till Tredje land. Eventuell framtida överföring till Tredje land får endast ske efter skriftlig instruktion från den Personuppgiftsansvarige och i enlighet med kapitel V i Dataskyddsförordningen.

8. Behandlingens varaktighet

Personuppgiftsbiträdet får behandla Personuppgifter under den tid som Personuppgiftsbiträdesavtalet gäller samt därefter i den mån det krävs för att fullgöra åtaganden enligt avtalet eller tillämplig lag.

Efter att Personuppgiftsbiträdesavtalet upphört ska Personuppgiftsbiträdet, på den Personuppgiftsansvariges begäran, radera eller återlämna Personuppgifterna i enlighet med avtalets bestämmelser och den Personuppgiftsansvariges instruktioner, om inte lagring krävs enligt tvingande lag.

9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

Utöver vad som anges ovan gäller följande instruktioner för Personuppgiftsbitrådets Behandling av Personuppgifter:

- Personuppgiftsbiträdet ska möjliggöra den Personuppgiftsansvariges granskning av efterlevnaden av Personuppgiftsbiträdesavtalet i enlighet med avtalets bestämmelser.
- Granskning ska i första hand ske genom tillhandahållande av relevant dokumentation, såsom beskrivningar av tekniska och organisatoriska säkerhetsåtgärder, styrdokument och rutiner.
- Fysiska inspektioner eller platsbesök ska endast genomföras om det är nödvändigt och efter överenskommelse mellan parterna, med beaktande av informationssäkerhet och sekretess.
- Ytterligare instruktioner ska lämnas skriftligen av den Personuppgiftsansvarige.
- Granskning ska ske på ett sätt som inte i onödan stör Personuppgiftsbitrådets verksamhet.

Bilaga 2 - Dataskydd och informationssäkerhet

Denna bilaga utgör en samlad beskrivning av Utilitas styrning, rutiner och säkerhetsåtgärder avseende dataskydd och informationssäkerhet. Utilitas agerar som personuppgiftsbiträde i förhållande till den Personuppgiftsansvarige. Bilagan gäller för styrelseledamöter, anställda, konsulter och underbiträden som behandlar personuppgifter inom ramen för uppdraget.

1. Styrning, roller och ansvar

Utilitas är en ideell förening och agerar som personuppgiftsbiträde. Styrelsen har det övergripande ansvaret för dataskydd och informationssäkerhet inom föreningen.

Styrelsen har genom särskilt beslut delegerat det operativa ansvaret för dataskydd och informationssäkerhet till föreningens anställda administratör. Delegationen gäller från beslutsdatum och tills vidare.

Den operativt ansvarige administratören ansvarar för att fastställda styrdokument och rutiner efterlevs i det dagliga arbetet och rapporterar vid behov till styrelsen.

2. Grundläggande principer för informationssäkerhet och dataskydd

Informationssäkerhetsarbetet inom Utilitas syftar till att säkerställa konfidentialitet, riktighet och tillgänglighet för personuppgifter.

Behandling av personuppgifter sker enligt dokumenterade instruktioner från den Personuppgiftsansvarige, inklusive sådana instruktioner som framgår av Personuppgiftsbiträdesavtalet och dess bilagor, samt genom den automatiserade behandling som är en integrerad del av Plattformens funktion.

3. Tekniska och organisatoriska säkerhetsåtgärder

Utilitas tillämpar tekniska och organisatoriska säkerhetsåtgärder som är proportionerliga i förhållande till behandlingens art, omfattning och risker för de registrerades rättigheter och friheter.

a. Teknisk infrastruktur och hosting

Plattformen driftas i en virtuell privat molnmiljö (Virtual Private Cloud) hos Bahnhof AB. Den tekniska infrastrukturen omfattar bland annat följande skyddsåtgärder:

- Drift i svenska datacenter som kontrolleras och förvaltas av Bahnhof AB.
- Ingen användning av underleverantörer utanför EU/EES i tjänsteleveransen.
- Datacenter som är ISO/IEC 27001-certifierade.
- Fysisk säkerhet med dygnet-runt-övervakning, kameraövervakning och larm.
- Datacenter som uppfyller Skyddsklass 3 och Larmklass 3 enligt svenska säkerhetsföreskrifter.
- Skydd mot överbelastningsattacker (DDoS).
- Brandväggar som är korrekt konfigurerade.
- Krypterad kommunikation vid överföring av data.
- Automatisk och kontinuerlig säkerhetskopiering samt möjlighet till återställning (backup & recovery).

Bahnhof AB är ett svenskt, svenskägt bolag som inte omfattas av amerikansk Cloud Act.

b. Åtkomstkontroll och behörighet

Åtkomst till personuppgifter styrs genom roll- och behörighetsbaserad åtkomstkontroll. Stark autentisering används för användare med administrativ åtkomst. Åtkomst ges endast i den utsträckning som krävs för att fullgöra arbetsuppgifter.

4. Loggning och spårbarhet

Administrativ och teknisk åtkomst till system och personuppgifter loggas i den mån det är relevant för säker drift, felsökning och incidentutredning.

Åtkomst till loggar är begränsad till behörig personal. Loggar sparas under begränsad tid enligt fastställda rutiner och raderas eller anonymiseras därefter.

5. Hantering av personuppgiftsincidenter

Utilitas har fastställda rutiner för identifiering, rapportering, hantering och uppföljning av personuppgiftsincidenter.

Alla personer med administrativ eller teknisk åtkomst ska omedelbart rapportera misstänkta incidenter till ansvarig administratör. Incidenter bedöms, begränsas och dokumenteras. Vid behov involveras tekniska underbiträden.

Den Personuppgiftsansvarige informeras utan onödigt dröjsmål om incidenter som berör dennes personuppgifter, tillsammans med relevant underlag för eventuell anmälan till tillsynsmyndighet.

6. Uppföljning och kontinuerlig förbättring

Informationssäkerhets- och dataskyddsarbetet följs upp löpande. Rutiner och åtgärder ses över och uppdateras vid behov, exempelvis vid förändringar i verksamhet, teknik eller regelverk.