

Standardavtalsbestämmelser (Personuppgiftsbiträdesavtal)

I enlighet med artikel 28.3 i Europaparlamentets och rådets förordning (EU) 2016/679 (dataskyddsförordningen) avseende personuppgiftsbiträdets behandling av personuppgifter
Standardavtalsbestämmelser (Personuppgiftsbiträdesavtal)

mellan

KUNDENS [NAMN]

Organisationsnummer [ORG.NR]

[ADRESS]

[POSTNUMMER OCH ORT]

[LAND]

nedan kallad "den personuppgiftsansvarige"

och

Vitec MV AB

Organisationsnummer 556438-3080

Davidshallsgatan 114

211 45 Malmö

nedan kallad "personuppgiftsbiträdet"

vilka var för sig benämns "part" och gemensamt "parterna"

HARINGÅTT följande standardavtalsbestämmelser ("Bestämmelserna") i syfte att uppfylla kraven i dataskyddsförordningen samt säkerställa skyddet för privatlivet och fysiska personers grundläggande rättigheter och friheter.

Innehåll

2. Inledning.....	3
3. Den personuppgiftsansvariges rättigheter och skyldigheter.....	4
4. Personuppgiftsbiträdet agerar enligt instruktioner.....	4
5. Sekretess.....	4
6. Behandlingssäkerhet.....	5
7. Användning av underbiträden	6
8. Överföring till tredjeland eller internationell organisation.....	7
9. Biträde till den personuppgiftsansvarige.....	8
10. Underrättelse om personuppgiftsincidenter	9
11. Radering av uppgifter.....	10
12. Revision, inklusive inspektion	10
13. Parternas avtal om andra förhållanden.....	11
14. Ikraftträdande och upphörande	11
15. Kontaktpersoner hos den personuppgiftsansvarige och personuppgiftsbiträdet	12
Bilag A Uppgifter om behandlingen.....	13
Bilag B Underbiträden.....	16
Bilag C Instruktioner avseende behandling av personuppgifter	17
Bilag D Parternas reglering av andra förhållanden	27

2. Indledning

1. Dessa Bestämmelser fastställer personuppgiftsbitrådets rättigheter och skyldigheter när det behandlar personuppgifter för den personuppgiftsansvariges räkning.
2. Dessa Bestämmelser har utformats i syfte att parterna ska uppfylla kraven i 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 samt om upphävande av direktiv 95/46/EG (dataskyddsförordningen).
3. I samband med leveransen av tjänster enligt Huvudavtalet av den [datum] samt eventuella senare tillägg behandlar personuppgiftsbitrådet personuppgifter för den personuppgiftsansvariges räkning i enlighet med dessa Bestämmelser.
4. Bestämmelserna har företräde framför eventuella motsvarande bestämmelser i andra avtal mellan parterna.
5. Till dessa Bestämmelser hör fyra bilagor, vilka utgör en integrerad del av Bestämmelserna.
6. Bilaga A innehåller närmare uppgifter om behandlingen av personuppgifter, inklusive behandlingens ändamål och art, typer av personuppgifter, kategorier av registrerade samt behandlingens varaktighet.
7. Bilaga B innehåller den personuppgiftsansvariges villkor för personuppgiftsbitrådets användning av underbiträden samt en förteckning över de underbiträden vars användning har godkänts av den personuppgiftsansvarige.
8. Bilaga C innehåller den personuppgiftsansvariges instruktioner avseende personuppgiftsbitrådets behandling av personuppgifter, en beskrivning av de säkerhetsåtgärder som personuppgiftsbitrådet som minst ska genomföra samt hur tillsyn över personuppgiftsbitrådet och eventuella underbiträden ska utövas.
9. Bilaga D innehåller bestämmelser avseende andra aktiviteter som inte omfattas av dessa Bestämmelser.
10. Bestämmelserna med tillhörande bilagor ska bevaras skriftligen, inklusive i elektronisk form, av båda parter.

11. Dessa Bestämmelser befriar inte personuppgiftsbiträdet från de skyldigheter som åligger personuppgiftsbiträdet enligt dataskyddsförordningen eller någon annan tillämplig lagstiftning.

3. Den personuppgiftsansvariges rättigheter och skyldigheter

1. Den personuppgiftsansvarige ansvarar för att säkerställa att behandlingen av personuppgifter sker i enlighet med dataskyddsförordningen (se artikel 24 i förordningen), dataskyddsbestämmelser i annan EU-rätt eller medlemsstaternas nationella rätt samt dessa Bestämmelser.
2. Den personuppgiftsansvarige har rätt och skyldighet att fatta beslut om för vilka ändamål och med vilka medel personuppgifter får behandlas.
3. Den personuppgiftsansvarige ansvarar bland annat för att säkerställa att det finns en rättslig grund för den behandling av personuppgifter som personuppgiftsbiträdet instrueras att utföra.

4. Personuppgiftsbiträdet agerar enligt instruktioner

1. Personuppgiftsbiträdet får endast behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige, om inte behandling krävs enligt EU-rätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av. Dessa instruktioner ska anges i Bilaga A och C. Ytterligare instruktioner kan även lämnas av den personuppgiftsansvarige under pågående behandling av personuppgifter, men instruktionerna ska alltid dokumenteras och bevaras skriftligen, inklusive i elektronisk form, tillsammans med dessa Bestämmelser.
2. Personuppgiftsbiträdet ska utan dröjsmål underrätta den personuppgiftsansvarige om det enligt personuppgiftsbitrådets bedömning anser att en instruktion strider mot denna förordning eller dataskyddsbestämmelser i annan EU-rätt eller medlemsstaternas nationella rätt.
(Hänvisningar till "medlemsstat" i dessa bestämmelser ska anses avse "EES-medlemsstater.")

5. Sekretess

1. Personuppgiftsbiträdet får endast ge tillgång till personuppgifter som behandlas för den personuppgiftsansvariges räkning till personer som omfattas av

personuppgiftsbiträdets instruktionsbefogenhet, som har åtagit sig att iaktta sekretess eller omfattas av en lämplig lagstadgad tystnadsplikt, och endast i den utsträckning det är nödvändigt. Förteckningen över personer som har beviljats åtkomst ska löpande ses över. På grundval av denna översyn ska åtkomsten till personuppgifter återkallas om åtkomsten inte längre är nödvändig, och personuppgifterna ska därefter inte längre vara tillgängliga för dessa personer.

2. Personuppgiftsbiträdet ska på begäran av den personuppgiftsansvarige kunna visa att de berörda personer som omfattas av personuppgiftsbiträdets instruktionsbefogenhet är bundna av ovan nämnda tystnadsplikt eller sekretessförpliktelse.

6. Behandlingssäkerhet

1. Artikel 32 i dataskyddsförordningen anger att den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste tekniska utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhet och allvarlighetsgrad för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är anpassad till dessa risker.

Den personuppgiftsansvarige ska bedöma de risker för fysiska personers rättigheter och friheter som behandlingen medför och vidta åtgärder för att hantera dessa risker. Beroende på deras relevans kan sådana åtgärder omfatta:

- a. pseudonymisering och kryptering av personuppgifter
 - b. förmåga att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och behandlingstjänster
 - c. förmåga att i rätt tid återställa tillgängligheten till och åtkomsten till personuppgifter vid en fysisk eller teknisk incident
 - d. ett förfarande för regelbunden testning, bedömning och utvärdering av effektiviteten hos de tekniska och organisatoriska åtgärderna för att säkerställa behandlingssäkerheten.
2. Enligt artikel 32 i förordningen ska personuppgiftsbiträdet, oberoende av den personuppgiftsansvarige, även bedöma de risker för fysiska personers rättigheter och friheter som behandlingen medför och vidta åtgärder för att hantera dessa risker. För denna bedömning ska den personuppgiftsansvarige tillhandahålla den information som

är nödvändig för att personuppgiftsbiträdet ska kunna identifiera och bedöma sådana risker.

3. Därutöver ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att uppfylla dennes skyldigheter enligt artikel 32 i förordningen, bland annat genom att tillhandahålla den information som är nödvändig om de tekniska och organisatoriska säkerhetsåtgärder som personuppgiftsbiträdet redan har genomfört enligt artikel 32 i förordningen, samt all annan information som är nödvändig för att den personuppgiftsansvarige ska kunna uppfylla sina skyldigheter enligt artikel 32.

Om hanteringen av de identifierade riskerna, enligt den personuppgiftsansvariges bedömning, kräver att ytterligare åtgärder genomförs utöver de åtgärder som personuppgiftsbiträdet redan har genomfört, ska den personuppgiftsansvarige ange dessa ytterligare åtgärder i Bilaga C.

7. Användning af underbiträden

1. Personuppgiftsbiträdet ska uppfylla de villkor som anges i artikel 28.2 och 28.4 i dataskyddsförordningen för att få anlita ett annat personuppgiftsbiträde (ett underbiträde).
2. Personuppgiftsbiträdet får således inte anlita ett underbiträde för att fullgöra dessa Bestämmelser utan föregående allmänt skriftligt godkännande från den personuppgiftsansvarige.
3. Personuppgiftsbiträdet har den personuppgiftsansvariges allmänna godkännande att anlita underbiträden. Personuppgiftsbiträdet ska skriftligen underrätta den personuppgiftsansvarige om eventuella planerade förändringar avseende tillägg eller utbyte av underbiträden med minst 30 dagars varsel och därigenom ge den personuppgiftsansvarige möjlighet att invända mot sådana förändringar innan det eller de berörda underbiträdena anlitas. Längre underrättelsefrist för specifika behandlingsaktiviteter kan anges i Bilaga B. Förteckningen över de underbiträden som den personuppgiftsansvarige redan har godkänt framgår av Bilaga B.
4. När personuppgiftsbiträdet anlitar ett underbiträde för att utföra specifika behandlingsaktiviteter för den personuppgiftsansvariges räkning, ska personuppgiftsbiträdet genom avtal eller annat rättsligt dokument enligt EU-rätten eller medlemsstaternas nationella rätt ålägga underbiträdet samma dataskyddsskyldigheter som följer av dessa Bestämmelser. Därigenom ska särskilt tillräckliga garantier säkerställas för att underbiträdet genomför de tekniska och organisatoriska åtgärderna

på ett sådant sätt att behandlingen uppfyller kraven i dessa Bestämmelser och i dataskyddsförordningen.

Personuppgiftsbiträdet ansvarar därför för att säkerställa att underbiträdet som minst uppfyller personuppgiftsbitrådets skyldigheter enligt dessa Bestämmelser och dataskyddsförordningen.

5. Avtal om underbiträde(n) och eventuella senare ändringar av sådana avtal ska, på den personuppgiftsansvariges begäran, tillhandahållas den personuppgiftsansvarige i kopia. Därigenom ges den personuppgiftsansvarige möjlighet att säkerställa att underbiträdet har ålagts motsvarande dataskyddsskyldigheter som följer av dessa Bestämmelser. Bestämmelser om kommersiella villkor som inte påverkar innehållet i underbiträdesavtalet ur dataskyddssynpunkt behöver inte lämnas ut till den personuppgiftsansvarige.
6. Personuppgiftsbiträdet ska, där så är möjligt, i sitt avtal med underbiträdet införa den personuppgiftsansvarige som förmånstagande tredje part vid personuppgiftsbitrådets konkurs, så att den personuppgiftsansvarige kan inträda i personuppgiftsbitrådets rättigheter och göra dem gällande gentemot underbiträden, exempelvis för att kunna instruera underbiträdet att radera personuppgifterna.
7. Om underbiträdet inte uppfyller sina dataskyddsskyldigheter, förblir personuppgiftsbiträdet fullt ansvarigt gentemot den personuppgiftsansvarige för fullgörandet av underbitrådets skyldigheter. Detta påverkar inte de registrerades rättigheter enligt dataskyddsförordningen, inklusive särskilt artiklarna 79 och 82, gentemot den personuppgiftsansvarige och personuppgiftsbiträdet, inklusive underbiträdet.

8. Överföring till tredjeland eller internationella organisationer

1. Varje överföring av personuppgifter till tredjeland eller internationella organisationer får endast ske av personuppgiftsbiträdet på grundval av dokumenterade instruktioner från den personuppgiftsansvarige och ska alltid genomföras i enlighet med kapitel V i dataskyddsförordningen.
2. Om en överföring av personuppgifter till tredjeland eller internationella organisationer, som personuppgiftsbiträdet inte har instruerats att genomföra av den personuppgiftsansvarige, krävs enligt EU-rätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av, ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige om detta rättsliga krav innan behandlingen påbörjas, såvida inte sådan underrättelse är förbjuden enligt den aktuella lagstiftningen av hänsyn till viktiga allmänna intressen.

3. Utan dokumenterade instruktioner från den personuppgiftsansvarige får personuppgiftsbiträdet således inte inom ramen för dessa Bestämmelser:
 - a. överföra personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland eller till en internationell organisation
 - b. anförtro behandling av personuppgifter åt ett underbiträde i ett tredjeland
 - c. behandla personuppgifterna i ett tredjeland
4. Den personuppgiftsansvariges instruktioner avseende överföring av personuppgifter till ett tredjeland, inklusive den eventuella överföringsmekanism enligt kapitel V i dataskyddsförordningen som överföringen grundar sig på, ska anges i Bilaga C.6 och Bilaga B, B.1.
5. Dessa Bestämmelser ska inte förväxlas med de standardavtalsklausuler som avses i artikel 46.2 c och d i dataskyddsförordningen, och dessa Bestämmelser kan inte utgöra en grund för överföring av personuppgifter enligt kapitel V i dataskyddsförordningen.

9. Biträde till den personuppgiftsansvarige

1. Personuppgiftsbiträdet ska, med beaktande av behandlingens art, i möjligaste mån bistå den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder för att den personuppgiftsansvarige ska kunna uppfylla sin skyldighet att besvara begäranden om utövande av de registrerades rättigheter enligt kapitel III i dataskyddsförordningen.

Detta innebär att personuppgiftsbiträdet i möjligaste mån ska bistå den personuppgiftsansvarige med att säkerställa efterlevnaden av:

 - a. informationsskyldigheten vid insamling av personuppgifter från den registrerade
 - b. informationsskyldigheten när personuppgifter inte har samlats in från den registrerade
 - c. rätten till tillgång (registerutdrag)
 - d. rätten till rättelse
 - e. rätten till radering ("rätten att bli bortglömd")
 - f. rätten till begränsning av behandling
 - g. underrättelseskyldigheten i samband med rättelse eller radering av personuppgifter eller 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, inklusive profilering

2. Utöver personuppgiftsbitrådets skyldighet att bistå den personuppgiftsansvarige enligt punkt 6.3 ska personuppgiftsbitrådet, med beaktande av behandlingens art och den information som är tillgänglig för personuppgiftsbitrådet, även bistå den personuppgiftsansvarige med:
 - a. den personuppgiftsansvariges skyldighet att utan onödigt dröjsmål och, om möjligt, senast 72 timmar efter att ha fått kännedom om en personuppgiftsincident anmäla denna till den behöriga tillsynsmyndigheten, Integritetsskyddsmyndigheten (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 informera den registrerade om en personuppgiftsincident när incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter
 - c. den personuppgiftsansvariges skyldighet att före behandlingen genomföra en bedömning av de planerade behandlingsåtgärdernas konsekvenser för skyddet av personuppgifter (en konsekvensbedömning avseende dataskydd)
 - d. den personuppgiftsansvariges skyldighet att samråda med den behöriga tillsynsmyndigheten, Integritetsskyddsmyndigheten (IMY), före behandlingen, om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle medföra en hög risk i avsaknad av åtgärder som den personuppgiftsansvarige vidtar för att minska risken.
3. Parterna ska i Bilaga C ange de nödvändiga tekniska och organisatoriska åtgärder genom vilka personuppgiftsbitrådet ska bistå den personuppgiftsansvarige samt i vilken omfattning och utsträckning sådant bistånd ska lämnas. Detta gäller för de skyldigheter som följer av punkt 9.1 och 9.2 i Bestämmelserna.

10. Underrättelse om personuppgiftsincidenter

1. Personuppgiftsbitrådet ska utan onödigt dröjsmål underrätta den personuppgiftsansvarige efter att ha blivit medvetet om att en personuppgiftsincident har inträffat.
2. Personuppgiftsbitrådets underrättelse till den personuppgiftsansvarige ska om möjligt ske senast 24 timmar efter att personuppgiftsbitrådet fått kännedom om incidenten, så att den personuppgiftsansvarige kan uppfylla sin skyldighet att anmäla

personuppgiftsincidenten till den behöriga tillsynsmyndigheten enligt artikel 33 i dataskyddsförordningen.

3. I enlighet med punkt 9.2 a ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att anmäla incidenten till den behöriga tillsynsmyndigheten. Detta innebär att personuppgiftsbiträdet ska bistå med att tillhandahålla följande information, som enligt artikel 33.3 ska ingå i den personuppgiftsansvariges anmälan av incidenten till den behöriga tillsynsmyndigheten:
 - a. personuppgiftsincidentens art, inklusive, om möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs
 - b. de sannolika konsekvenserna av personuppgiftsincidenten
 - c. de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslår att vidta för att hantera personuppgiftsincidenten, inklusive, om relevant, åtgärder för att begränsa dess eventuella negativa effekter.
4. Parterna ska i Bilaga C ange vilken information personuppgiftsbiträdet ska tillhandahålla inom ramen för sitt bistånd till den personuppgiftsansvarige avseende dennes skyldighet att anmäla personuppgiftsincidenter till den behöriga tillsynsmyndigheten.

11. Radering av uppgifter

1. Vid upphörande av de tjänster som avser behandling av personuppgifter är personuppgiftsbiträdet skyldigt att radera samtliga personuppgifter som har behandlats för den personuppgiftsansvariges räkning och bekräfta för den personuppgiftsansvarige att uppgifterna har raderats, såvida inte EU-rätten eller medlemsstaternas nationella rätt föreskriver att personuppgifterna ska bevaras.

12. Revision, inklusive inspektion

1. Personuppgiftsbiträdet ska tillhandahålla all information som är nödvändig för att visa att kraven i artikel 28 i dataskyddsförordningen och dessa Bestämmelser efterlevs samt möjliggöra och bidra till revisioner, inklusive inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.
2. Rutinerna för den personuppgiftsansvariges revisioner, inklusive inspektioner, hos personuppgiftsbiträdet och dess underbiträden anges närmare i Bilaga C.7 och C.8.

3. Personuppgiftsbiträdet är skyldigt att ge tillsynsmyndigheter som enligt gällande lagstiftning har rätt till tillträde till den personuppgiftsansvariges eller personuppgiftsbitrådets lokaler, eller representanter som agerar på tillsynsmyndighetens vägnar, tillgång till personuppgiftsbitrådets fysiska lokaler mot uppvisande av giltig legitimation.

13. Parternas avtal om andra förhållanden

1. Parterna kan komma överens om andra bestämmelser avseende tjänsten och behandlingen av personuppgifter, exempelvis beträffande skadeståndsansvar, så länge dessa bestämmelser inte direkt eller indirekt strider mot Bestämmelserna eller försämrar den registrerades grundläggande rättigheter och friheter enligt dataskyddsförordningen.

14. Ikraftträdande och upphörande

1. Bestämmelserna träder i kraft den dag då båda parter har undertecknat dem.
2. Båda parter kan begära att Bestämmelserna omförhandlas om lagändringar eller brister i Bestämmelserna ger anledning till detta.
3. Bestämmelserna gäller så länge tjänsten avseende behandling av personuppgifter pågår. Under denna period kan Bestämmelserna inte sägas upp, såvida inte parterna träffar avtal om andra bestämmelser som reglerar tillhandahållandet av tjänsten avseende behandling av personuppgifter.
4. Om tillhandahållandet av tjänsterna avseende behandling av personuppgifter upphör och personuppgifterna har raderats i enlighet med punkt 11.1 och Bilaga C.4, kan Bestämmelserna sägas upp av endera parten genom skriftligt meddelande.
5. Underskrifter

För den personuppgiftsansvariges räkning

Namn	[NAMN]
Befattning	[BEFATTNING]
Telefonnummer	[TELEFONNUMMER]
E-post	[E-POST]
Underskrift	

För personuppgiftsbitrådets räkning

Namn	Hans-Erik Schou
Befattning	Verkställande direktör
Telefonnummer	+45 65 91 80 22
E-post	Hans-Erik.Schou@vitecsoftware.com
Underskrift	

15. Kontaktpersoner hos den personuppgiftsansvarige och personuppgiftsbitrådet

1. Parterna kan kontakta varandra genom nedanstående kontaktpersoner.
2. Parterna är skyldiga att fortlöpande informera varandra om ändringar avseende kontaktpersonerna.

Namn	[NAMN]
Befattning	[BEFATTNING]
Telefonnummer	[TELEFONNUMMER]
E-post	[E-POST]

Kontaktpersonen hos den personuppgiftsansvarige uppmanas att prenumerera på vårt GDPR-informationsbrev, eftersom personuppgiftsbitrådet informerar om ändringar i vårt personuppgiftsbitrådesavtal via denna kanal:

<https://www.vitec-mv.com/se/nyhetsbrev/>.

I GDPR-informationsbrevet informerar personuppgiftsbitrådet även om annat GDPR-relaterat innehåll.

Om den personuppgiftsansvarige inte önskar prenumerera på denna informationskanal, vänligen informera Vitec MV om detta, så att vi kan kontakta den personuppgiftsansvariges kontaktperson direkt.

Kontakt hos den personuppgiftsansvarige vid personuppgiftsincident enligt avsnitt 10

E-post: [E-POST]

Namn	Hans-Erik Schou
Befattning	Verkställande direktör
Telefonnummer	+ 45 63 12 60 15
E-post	support.mv@vitecsoftware.com

Bilaga A Uppgifter om behandlingen

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

Personuppgiftsbitrådet tillhandahåller, som ett led i fullgörandet av Huvudavtalet, följande digitala hjälpmedel/programvaruprodukter till den personuppgiftsansvarige:

- IntoWords

Personuppgiftsbitrådets programvaruprodukter stödjer och förenklar användarens **bearbetning av text**. Med bearbetning av text avses följande processer:

- **Textförståelse:** Produkten hjälper användaren att förstå skriven text genom funktioner som uppläsning och markering av text.
- **Textproduktion:** Användaren får stöd genom funktioner såsom ordprediktion, stavningsstöd, översättning och tal-till-text.

A.2. Personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning avser huvudsakligen (behandlingens art)

Personuppgiftsbitrådets behandling av personuppgifter avser huvudsakligen att, för den personuppgiftsansvariges räkning, autentisera inloggningsuppgifter i syfte att tillhandahålla de tjänster som anges i punkt A.1.

Personuppgiftsbitrådets programvaruprodukter stödjer och förenklar användarens **bearbetning av text** i enlighet med punkt A.1.

Personuppgiftsbitrådets produkter samlar in och registrerar uppgifter om användaren vid skapandet av inloggnings- eller användarkonto samt vid användningen av produkterna och tjänsterna för att kunna tillhandahålla den avtalade tjänsten.

Vid användning av **MV-Login** skapar den personuppgiftsansvariges administratör själv användarinloggningar.

A.3. Behandlingen omfattar följande kategorier av personuppgifter om de registrerade

Kommunkunder

Samtliga kommunkunder i Danmark använder UNI-C, i Norge används Feide, i Sverige används Skolfederationen och i Nederländerna används Entree. För vissa offentliga kunder används

Google IdP eller Microsoft IdP, och i dessa fall exponeras endast tenant-ID eller rotomän. Dessa uppgifter likställs med skolkod.

De uppgifter om användaren som görs tillgängliga för personuppgiftsbiträdet vid inloggning och användning av tjänsten omfattar följande:

- Roll (t.ex elev eller lärare)
- Skolekod (institutionsnummer)
- Klassbeteckning
- Inloggning/hash
- Textförståelse: I samband med tillhandahållandet av tjänsterna kan uppläsning av markerad text innehålla personuppgifter som förekommer i själva texten.
- Textproduktion: I samband med tillhandahållandet av tjänsterna kommer texten att innehålla de uppgifter, inklusive personuppgifter, som slutanvändaren skriver.
- Tal-till-text: I samband med tillhandahållandet av tjänsterna kommer ljudfilen att innehålla slutanvändarens röst samt de uppgifter som slutanvändaren eventuellt dikterar och uppgifter som kan härledas från rösten eller ljudet, exempelvis uppgifter om kön och språk.
- Översättning: I samband med tillhandahållandet av tjänsterna kommer den översatta texten att innehålla de uppgifter, inklusive personuppgifter, som slutanvändaren skriver.

Personuppgiftsbiträdet behandlar som utgångspunkt inte särskilda kategorier av personuppgifter (känsliga personuppgifter enligt artikel 9) enligt dessa Bestämmelser, om inte den personuppgiftsansvarige har lämnat instruktion om detta i Avtalet, i andra särskilt ingångna avtal eller i tillägg till dessa.

Om den personuppgiftsansvarige eller den personuppgiftsansvariges slutanvändare överför eller på annat sätt tillgängliggör särskilda kategorier av personuppgifter till eller via personuppgiftsbiträdet, inklusive dess underbiträden, och omfattningen av sådan behandling bestäms och kontrolleras av den personuppgiftsansvarige, ska den personuppgiftsansvarige anses ha instruerat personuppgiftsbiträdet att behandla dessa särskilda kategorier av personuppgifter i enlighet med dessa Bestämmelser.

Det bör noteras att de uppgifter som slutanvändaren överför i samband med tillhandahållandet av tjänsterna endast lagras under 7 (sju) dagar i syfte att tillhandahålla tjänsten samt eventuell support. Därefter raderas uppgifterna.

Företagskunder

I detta fall fungerar inloggningen på samma sätt som exempelvis via Skolfederationen, men det är helt upp till kunden vilka uppgifter som medföljer vid inloggningen.

De uppgifter om användaren som görs tillgängliga för personuppgiftsbiträdet vid inloggning omfattar följande:

- Roll (t.ex medarbetare eller administratör)
- Inloggning/hash
- Textförståelse: I samband med tillhandahållandet av tjänsterna kan uppläsning av markerad text innehålla personuppgifter som förekommer i själva texten.
- Textproduktion: I samband med tillhandahållandet av tjänsterna kommer texten att innehålla de uppgifter, inklusive personuppgifter, som slutanvändaren skriver.
- Tal-till-text: I samband med tillhandahållandet av tjänsterna kommer ljudfilen att innehålla slutanvändarens röst samt de uppgifter som slutanvändaren eventuellt dikterar och uppgifter som kan härledas från rösten eller ljudet, exempelvis uppgifter om kön och språk.
- Översättning: I samband med tillhandahållandet av tjänsterna kommer den översatta texten att innehålla de uppgifter, inklusive personuppgifter, som slutanvändaren skriver.

Personuppgiftsbiträdet behandlar som utgångspunkt inte särskilda kategorier av personuppgifter (känsliga personuppgifter enligt artikel 9) enligt dessa Bestämmelser, om inte den personuppgiftsansvarige har lämnat instruktion om detta i Avtalet, i andra särskilt ingångna avtal eller i tillägg till dessa.

Om den personuppgiftsansvarige eller den personuppgiftsansvariges slutanvändare överför eller på annat sätt tillgängliggör särskilda kategorier av personuppgifter till eller via personuppgiftsbiträdet, inklusive dess underbiträden, och omfattningen av sådan behandling bestäms och kontrolleras av den personuppgiftsansvarige, ska den personuppgiftsansvarige anses ha instruerat personuppgiftsbiträdet att behandla dessa särskilda kategorier av personuppgifter i enlighet med dessa Bestämmelser.

Det bör noteras att de uppgifter som slutanvändaren överför i samband med tillhandahållandet av tjänsterna endast lagras under 7 (sju) dagar i syfte att tillhandahålla tjänsten samt eventuell support. Därefter raderas uppgifterna.

A.4. Behandlingen omfattar följande kategorier av registrerade

Anställda hos den personuppgiftsansvarige	
Elever/studerande hos den personuppgiftsansvarige över 18 år	
Elever/studerande hos den personuppgiftsansvarige under 18 år	
Övriga registrerade, exempelvis medborgare	

A.5. Personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning får påbörjas efter att dessa Bestämmelser har trätt i kraft. Behandlingen har följande varaktighet:

Personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning påbörjas när Huvudavtalet träder i kraft och pågår till senast 30 dagar efter att Huvudavtalet har upphört. Personuppgiftsbiträdet ska dessförinnan ha raderat samtliga personuppgifter som tillhör den personuppgiftsansvarige.

När det gäller radering av specifika slutanvändare hos kommun- och företagskunder är raderingen beroende av att den personuppgiftsansvarige informerar personuppgiftsbiträdet om detta, varefter radering kommer att ske.

Bilag B Underbiträden

B.1. Godkända underbiträden

Ved Vid Bestämmelsernas ikraftträdande har den personuppgiftsansvarige godkänt användningen av följande underbiträden:

NAMN	ORGANISATIONS-NUMMER	ADRESS	BESKRIVNING AV BEHANDLING
UpCloud OY	2431560-5	Aleksanterinkatu 15B, 7th floor, 00100 Helsinki, Finland	Serverhosting

Vid bestämmelsernas ikraftträdande har den personuppgiftsansvarige godkänt användningen av ovan nämnda underbiträden för den beskrivna behandlingsaktiviteten. Personuppgiftsbiträdet får inte, utan den personuppgiftsansvariges skriftliga godkännande, anlita ett underbiträde för någon annan behandlingsaktivitet än den som beskrivits och avtalats, eller anlita ett annat underbiträde för denna behandlingsaktivitet.

B.2. Underrättelse för godkännande av underbiträden

I enlighet med punkt 7.3 ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige om eventuella planerade ändringar avseende de underbiträden som anges i B.1 ovan med minst trettio (30) dagars varsel. Därigenom ges den personuppgiftsansvarige möjlighet att invända mot sådana ändringar innan de genomförs i samband med tillhandahållandet av tjänsterna för den personuppgiftsansvariges räkning.

Bilaga C Instruktion avseende behandling av personuppgifter

C.1. Behandlingens föremål/instruktion

Personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning sker genom att personuppgiftsbiträdet utför följande:

Personuppgiftsbiträdet möjliggör för den personuppgiftsansvarige och dennes användare att skapa användarkonton/inloggning så att användaren kan nyttja de tjänster som personuppgiftsbiträdets produkter och tjänster tillhandahåller, enligt beskrivningen i Bilaga A.

C.2. Behandlingssäkerhet

Personuppgiftsbiträdet ska genomföra lämpliga tekniska och organisatoriska kontroller och åtgärder för att säkerställa konfidentialitet, integritet och tillgänglighet för de personuppgifter som behandlas för den personuppgiftsansvariges räkning. Personuppgifter ska klassificeras korrekt och lämpliga säkerhetskontroller ska genomföras utifrån denna klassificering.

I samband med tillhandahållandet av tjänster för den personuppgiftsansvariges räkning ska personuppgiftsbiträdet som ett minimum genomföra följande säkerhetskontroller, vilka baseras på principerna i ISO 27001-standarden samt kontrollerna i kontrollmål B avseende behandlingssäkerhet i ISAE 3000-utlåtandet:

C.2.1. Informationssäkerhetspolicy

C.2.1.1. Personuppgiftsbiträdet, inklusive dess leverantörer och medarbetare, ska vid var tid följa den interna informationssäkerhetspolicy, som är anpassad till principerna i ISO 27001-standarden och innehåller rutiner som syftar till att skydda den personuppgiftsansvariges data och personuppgifter så länge dessa förvaras eller på annat sätt behandlas av personuppgiftsbiträdet.

C.2.1.2. Personuppgiftsbiträdet ska, efter att ha genomfört en formell riskbedömning, regelbundet testa interna säkerhetspolicyer, planer och kontroller. Resultatet av sådana tester ska kommuniceras till personuppgiftsbiträdets ledning, och resultat som direkt påverkar behandlingen av personuppgifter ska åtgärdas utan oskäligt dröjsmål.

C.2.1.3. Personuppgiftsbiträdet ska upprätthålla och följa principerna i ISO 27001- eller ISO 27701-standarderna inom ramen för sitt interna efterlevnadsprogram för informationssäkerhet och dataskydd.

C.2.2. Organisering av informationssäkerhet

C.2.2.1. Personuppgiftsbitrådets informationssäkerhetsorganisation ska vara organiserad på ett sådant sätt att informationssäkerheten kan styras effektivt och att målen för informationssäkerheten kan uppnås.

Vidare ska personuppgiftsbitrådet:

- a. upprätthålla tillräckligt kvalificerad personal med tydligt definierade roller och ansvarsområden inom informationssäkerhetsorganisationen för att samordna införandet av säkerhetsrutiner inom personuppgiftsbitrådets organisation.
- b. fastställa krav avseende informationens känslighet, skydd och utlämnande samt årligen ompröva sådana krav.
- c. separera arbetsuppgifter, roller och ansvar för att förhindra obehörig användning av personuppgiftsbitrådets verksamhetskritiska informationstillgångar.

C.2.3. Personfrågor

C.2.3.1. Bakgrundskontroller av medarbetare med tillgång till personuppgifter ska genomföras i enlighet med tillämplig lagstiftning, övriga regulatoriska krav och etiska riktlinjer och ska utföras för varje enskild person som ett minimum vid anställning, såvida detta inte strider mot gällande lagstiftning. Omfattningen av bakgrundskontrollerna ska stå i proportion till den aktuella medarbetarens roll, känsligheten hos de uppgifter som rollen ger tillgång till samt de risker som kan uppstå vid missbruk av uppgifterna.

C.2.3.2. Personuppgiftsbitrådet ska säkerställa att all personal har undertecknat en sekretessförbindelse som en del av sitt anställningsavtal.

C.2.3.3. Personuppgiftsbitrådet ska säkerställa att dess användare har tillräcklig medvetenhet om informationssäkerhet och endast har behörig åtkomst till data, så att de förstår sina ansvarsområden beträffande säkerheten för den personuppgiftsansvariges data och personuppgifter.

C.2.3.4. Personuppgiftsbitrådet ska säkerställa att alla nödvändiga rutiner genomförs för personuppgiftsbitrådets medarbetare vid förändring av arbetsroll, upphörande av arbetsuppgifter samt vid avslutande av anställning, kontrakt eller annat avtalsförhållande.

C.2.4. Hantering av tillgångar

C.2.4.1. Personuppgiftsbitrådet ska upprätthålla rutiner för identifiering, kontroll samt hantering av ägarskap och säkerhetsklassificering av kritiska tillgångar samt den personuppgiftsansvariges data och personuppgifter som lagras i personuppgiftsbitrådets datacenterinfrastruktur.

C.2.4.2. Personuppgiftsbiträdet ska utarbeta policyer för godtagbar användning av data och tillgångar samt kommunicera dessa till samtliga relevanta användare av dess tillgångar och data.

C.2.4.3. Personuppgiftsbiträdet ska implementera formella och dokumenterade rutiner för systemhärdning och grundkonfigurering (baseline-konfigurering). Programvara eller hårdvara som inte längre stöds får inte användas.

C.2.5. Åtkomstkontroll

C.2.5.1. Personuppgiftsbiträdet ska implementera kontroller för att säkerställa åtkomsten till de personuppgifter som behandlas för den personuppgiftsansvariges räkning.

C.2.5.2. Användaråtkomsten till de av personuppgiftsbitrådets system och applikationer som lagrar eller ger åtkomst till personuppgifter ska kontrolleras genom en säker inloggningsprocess.

C.2.5.3. Personuppgiftsbitrådets personal ska ges åtkomst till sådana personuppgifter endast utifrån verksamhetsmässigt behov och enligt principen om minsta privilegium (least privilege), med beaktande av respektive persons roll och ansvarsområde.

C.2.5.4. Personuppgiftsbiträdet ska övervaka och begränsa åtkomsten till hjälpprogram som kan kringgå säkerhetskontroller i system eller applikationer. Administrativa behörigheter på slutenheter (endpoints) ska vara begränsade.

C.2.5.5. Åtkomst till samtliga av personuppgiftsbitrådets system skyddas genom multifaktorautentisering (MFA), och samtliga medarbetare hos personuppgiftsbiträdet med åtkomst till driftmiljöer har undertecknat en utökad sekretessförbindelse.

C.2.5.6. Den formella processen för att i rätt tid återkalla åtkomst till personuppgifter ska följas när en person inte längre har behov av åtkomst till uppgifterna.

C.2.6. Kryptografi

C.2.6.1. Personuppgiftsbiträdet ska säkerställa att personuppgifter som behandlas för den personuppgiftsansvariges räkning skyddas under lagring och överföring genom användning av stark kryptering. Krypteringen ska motsvara allmänt vedertagna branschstandarder och implementeras i enlighet med personuppgiftsbitrådets krypteringsstandard.

C.2.6.2. Leverantören ska implementera rutiner för hantering av krypteringsnycklar som omfattar:

- a. Generering av krypteringsnycklar med godkänd nyckellängd.
- b. Säker distribution, aktivering, lagring, återställning samt utbyte/uppdatering av krypteringsnycklar.
- c. Omedelbar återkallelse (avaktivering) av krypteringsnycklar vid kompromettering eller vid förändring av en medarbetares ansvarsområde.
- d. Återställning av krypteringsnycklar som har gått förlorade, skadats eller upphört att gälla.
- e. Säkerhetskopiering och arkivering av krypteringsnycklar samt upprätthållande av historik över krypteringsnycklar.
- f. Fastställande av tidpunkter för aktivering och avaktivering av definierade krypteringsnycklar.
- g. Begränsning av åtkomst till krypteringsnycklar till behöriga personer.

C.2.6.3. Produkterna använder kryptering både "in transit" och "at rest". Detta innebär bland annat att samtliga anslutningar till backend-system är krypterade med TLS v1.2/1.3 vid överföring ("in transit"). Krypteringen vid lagring ("at rest") beror på lagringsmediet, men AES-256 används i de flesta fall.

C.2.7. Fysisk säkerhet och miljösäkerhet

C.2.7.1. Personuppgiftsbiträdet ska genomföra lämpliga fysiska säkerhetskontroller i syfte att säkerställa konfidentialitet, integritet och tillgänglighet för de personuppgifter som behandlas för den personuppgiftsansvariges räkning på personuppgiftsbitrådets anläggningar, kunders lokaler eller andra externa platser. Kontrollerna ska regelbundet ses över för att säkerställa deras effektivitet.

C.2.7.2. Personuppgiftsbiträdet ska dock som minst genomföra följande fysiska säkerhetsåtgärder på sina kontor:

- a. Fysisk passerkontroll för byggnader och kritiska områden
- b. Receptionsområden som övervakas av receptionspersonal eller säkerhetsvakter
- c. Loggning av fysisk åtkomst eller försök till sådan åtkomst.

C.2.7.3. Personuppgiftsbiträdet använder en kontrollerad driftmiljö placerad inom EU/EES. Personuppgiftsbiträdet har implementerat tekniska och organisatoriska åtgärder som säkerställer loggning av åtkomst till och aktiviteter i drift- och produktionsmiljöer. Loggningen möjliggör spårbarhet av behöriga medarbetares åtkomst och åtgärder i syfte att upprätthålla informationssäkerhet, hantera incidenter och genomföra revision.

Logguppgifter lagras under en begränsad och dokumenterad period i enlighet med personuppgiftsbitrådets interna policyer och raderas eller anonymiseras därefter.

C.2.8. Driftssäkerhet

C.2.8.1. Personuppgiftsbiträdet ska implementera kontroller som identifierar och förhindrar skadlig programvara (malware), skadlig kod och obehörig körning av kod. Kontrollerna ska regelbundet uppdateras med den senaste tillgängliga tekniken (t.ex. uppdatering av de senaste signaturerna och definitionerna).

C.2.8.2. Personuppgiftsbiträdet ska utföra penetrationstester av system och applikationer som lagrar personuppgifter eller ger åtkomst till personuppgifter.

C.2.8.3. Personuppgiftsbiträdet ska implementera en process för hantering av uppdateringar och sårbarheter i system och applikationer för identifiering, rapportering och avhjälpande av sårbarheter.

C.2.8.4. Personuppgiftsbiträdet ska generera administratörs- och händelseloggar för system och applikationer som lagrar personuppgifter eller ger åtkomst till personuppgifter.

C.2.8.5. Personuppgiftsbiträdet ska regelbundet granska systemloggar (minst en gång per månad) för att identifiera systemavbrott, fel eller möjliga säkerhetsincidenter som påverkar personuppgifterna. Avhjälpande åtgärder ska vidtas för att lösa eller hantera sådana förhållanden inom den erforderliga tidsramen.

C.2.9. Kommunikationssäkerhet

C.2.9.1. Personuppgiftsbiträdet ska etablera en säker VPN-anslutning (Virtual Private Network) som medarbetarna ska använda vid fjärråtkomst till personuppgiftsbitrådets interna nätverk. Användare ska använda tvåfaktorsautentisering för att få åtkomst via VPN-anslutningen.

C.2.9.2. Personuppgiftsbiträdet ska använda avancerade brandväggar för att skydda sitt nätverk, inklusive skydd mot skadlig programvara och avancerade intrångsförsök i nätverket, samt för segmentering av nätverket för att säkerställa dess robusthet.

C.2.9.3. Personuppgiftsbiträdet ska implementera lösningar som är utformade för att övervaka och logga aktiviteten i sitt nätverk. Loggarna ska övervakas löpande för att säkerhetsincidenter ska kunna identifieras och hanteras i rätt tid, och de ska lagras i enlighet med personuppgiftsbitrådets formella policyer och rutiner.

C.2.9.4. Personuppgiftsbiträdet ska synkronisera systemklockor på nätverksservrar till en universell tidsstandard (t.ex. UTC) eller via Network Time Protocol (NTP).

C.2.10. Anskaffning, utveckling och underhåll av system

C.2.10.1. Personuppgiftsbitrådets inköpsprocess för hårdvara, programvara och tjänster ska dokumenteras och omfatta identifiering och bedömning av informationssäkerhetsrisker.

C.2.10.2. Personuppgiftsbiträdet ska implementera formella, dokumenterade rutiner för styrning av förändringar i informationssystem, stödjande infrastruktur och anläggningar.

C.2.10.3. Personuppgiftsbiträdet ska etablera en logisk eller fysisk separering mellan utvecklings- test- och produktionsmiljöer. Användares åtkomst till programkällkod ska begränsas och loggas.

C.2.10.4. Personuppgiftsbiträdet ska etablera ett säkert tillvägagångssätt för systemdesign och kodning som dokumenteras och integreras i systemutvecklingens livscykel (SDLC). Utvecklare ska regelbundet delta i utbildning om säker utveckling.

C.2.10.5. Personuppgiftsbitrådets ändringar i system och applikationer ska testas och uppfylla fastställda godkännandekriterier innan de implementeras. Testerna ska omfatta relevanta säkerhetskontroller.

C.2.10.6. Personuppgiftsbitrådets produktionsdata får inte användas i andra miljöer än produktionsmiljön. Om sådan användning är oundviklig ska uppgifterna maskeras (t.ex. döljas, rensas, pseudonymiseras eller anonymiseras), eller så ska säkerhetskontroller motsvarande dem som finns i produktionsmiljön införas i de övriga miljöerna.

C.2.10.7. Automatiserad statisk analys av källkod samt avhjälpande av sårbarheter ska genomföras för personuppgiftsbitrådets källkod före implementering.

C.2.10.8. Personuppgiftsbiträdet ska övervaka outsourcad systemutveckling som omfattas av styrningskontroll hos extern leverantör.

C.2.11. Hantering av leverantörsrelationer

C.2.11.1. Personuppgiftsbiträdet ska upprätta och upprätthålla formella avtal med de leverantörer som är involverade i hanteringen av tjänster relaterade till personuppgiftsbitrådets informationssystem och, där så är relevant, införliva nödvändiga säkerhetskontroller, säkerhetspolicyer och tjänstenivåavtal.

C.2.11.2. Personuppgiftsbiträdet ska regelbundet granska sina externa parter informationssäkerhetskontroller och säkerställa att dessa kontroller fortsatt är relevanta i förhållande till de risker som är förknippade med de externa parternas behandling av personuppgifter, med beaktande av den tekniska utvecklingsnivån och kostnaderna för implementering.

C.2.11.3. Personuppgiftsbiträdet ska begränsa externa parter åtkomst till personuppgifter. När åtkomst till uppgifter är nödvändig för att fullgöra avtalet om tillhandahållande av tjänster ska personuppgiftsbiträdet:

- a. ge den personuppgiftsansvarige en förteckning över de externa parter som behöver åtkomst till personuppgifter
- b. endast ge tillstånd att få åtkomst till personuppgifter när det är nödvändigt för att tillhandahålla de tjänster som den externa parten har avtalat att leverera
- c. registrera den externa partens åtkomst till personuppgifter i systemloggar som omfattas av personuppgiftsbitrådets kontroller för loggning och övervakning.

C.2.12. Hantering av informationssäkerhetsincidenter

C.2.12.1. Personuppgiftsbiträdet ska utarbeta och upprätthålla en incidentberedskapsplan samt ett program som innehåller rutiner och instruktioner som ska följas vid en incident relaterad till personuppgiftsbitrådets datorinfrastruktur. De nödvändiga åtgärderna och kommunikationskanalerna som ska användas ska dokumenteras.

C.2.12.2. Personuppgiftsbiträdet ska säkerställa att instruktionerna omfattar lämpliga rutiner för omedelbar underrättelse till personuppgiftsbitrådets kunder och andra nödvändiga intressenter om det fastställs att en säkerhetsincident har orsakat en personuppgiftssäkerhetsincident som innefattar personuppgifter.

C.2.13. Informationssäkerhetssaspekter vid kontinuitets-- beredskaps- og återställningshantering

C.2.13.1. Personuppgiftsbiträdet ska ha en plan för verksamhetskontinuitet och katastrofberedskap som ska användas för att inom rimlig tid återställa personuppgiftsbitrådets kritiska system, applikationer och komponenter vid en fysisk eller teknisk incident.

C.2.13.2. Personuppgiftsbiträdet ska regelbundet, minst en gång per år, testa ovanstående planer och säkerställa att de hålls uppdaterade.

C.2.13.3 Personuppgiftsbiträdet ska införa rutiner för identifiering och validering av säkerhetskopior som är nödvändiga för att stödja katastrofberedskapen.

C.2.13.4 Personuppgiftsbiträdet ska säkerställa lämplig lagring av säkerhetskopior för att upprätthålla katastrofberedskapen samt implementera ändamålsenliga rutiner för bortskaffande som uppfyller gällande krav på lagring och bevarande.

C.3 Bitrådets bistånd till den personuppgiftsansvarige

Personuppgiftsbiträdet ska i möjligaste mån, inom nedan angiven omfattning, bistå den personuppgiftsansvarige i enlighet med Bestämmelse 9.1 och 9.2 genom att genomföra följande tekniska och organisatoriska åtgärder:

På begäran av den personuppgiftsansvarige kan personuppgiftsbiträdet radera alla uppgifter som är kopplade till slutanvändaren. För företags- och kommunkunder förutsätter detta bistånd att uppgifter från identitetsleverantören (IdP) tillhandahålls av den personuppgiftsansvarige, eftersom personuppgiftsbiträdet inte har tillgång till direkt personidentifierande uppgifter om dessa användare.

För att radera uppgifter på den personuppgiftsansvariges vägnar krävs ett antal tekniska åtgärder beroende på användartyp:

Kommunkunder

Som huvudregel kan en specifik användare inte identifieras i personuppgiftsbitrådets system, eftersom inga direkt personidentifierande uppgifter lagras i samband med användarinloggningen. Det är därför nödvändigt att den personuppgiftsansvarige begär att Skolfederationen identifierar den aktuella användaren och därigenom gör det möjligt för personuppgiftsbiträdet att lokalisera och radera uppgifterna.

Företagskunder

Användaren kan identifieras med hjälp av exempelvis e-postadress och kan lokaliseras och raderas med stöd av dessa uppgifter.

C.4 Lagringsperiod och raderingsrutiner

Personuppgifter lagras till dess att ett användarkonto avslutas eller under den period som Huvudavtalet gäller, dock längst till och med 30 dagar efter dess upphörande.

Observera att uppgifter som uppkommer i samband med tillhandahållandet av tjänsterna raderas efter 7 (sju) dagar, se punkt A.3.

C.5 Plats för behandling

Behandling av de personuppgifter som omfattas av Bestämmelserna får inte, utan den personuppgiftsansvariges föregående skriftliga godkännande, ske på andra platser än följande:

Vitec MV A/S
CVR-nr. 15 31 44 00
Cortex Park Vest 3
5530 Odense M
Danmark

Härutöver får behandling när som helst ske på de platser där personuppgiftsbitrådets medarbetare har hemarbetsplatser eller liknande arbetsplatser.

De personuppgifter som omfattas av Bestämmelserna behandlas på följande platser av följande underbiträde, som lagrar (hostar) uppgifterna för personuppgiftsbitrådets räkning:

NAMN	ADRESS	DATACENTRETS PLACERING	MODERBOLAGETS GEOGRAFISKA PLACERING
UpCloud OY	Aleksanterinkatu 15B, 7th floor, 00100 Helsinki, Finland	Personuppgifter behandlas i UpClouds datacenter inom EU	Finland

C.6 Instruktion avseende överföring av personuppgifter till tredjeland

Om den personuppgiftsansvarige inte i dessa Bestämmelser eller senare lämnar en dokumenterad instruktion avseende överföring av personuppgifter till ett tredjeland, har personuppgiftsbitrådet inte rätt att inom ramen för dessa Bestämmelser genomföra sådana överföringar.

C.7 Förfaranden för den personuppgiftsansvariges revisioner, inklusive inspektioner, av den personuppgiftsbehandling som personuppgiftsbitrådet utför

Personuppgiftsbitrådet ska varje år på egen bekostnad inhämta ett revisionsintyg från en oberoende tredje part avseende personuppgiftsbitrådets efterlevnad av dataskyddsförordningen, dataskyddsbestämmelser i annan EU-rätt eller medlemsstaternas nationella rätt samt dessa Bestämmelser.

Parterna är överens om att följande typer av revisionsintyg får användas i enlighet med dessa Bestämmelser:

ISAE 3000 eller annan rapportering baserad på jämförbara eller strängare standarder.

Revisionsintyget ska utan onödigt dröjsmål översändas till den personuppgiftsansvarige för kännedom efter begäran härom. Intyget publiceras dessutom på personuppgiftsbiträdet webbplats, <https://www.vitec-mv.com/se/>.

Baserat på resultaten i revisionsintyget har den personuppgiftsansvarige rätt att begära att ytterligare åtgärder genomförs i syfte att säkerställa efterlevnaden av dataskyddsförordningen, dataskyddsbestämmelser i annan EU-rätt eller medlemsstaternas nationella rätt samt dessa Bestämmelser.

Den personuppgiftsansvarige eller deras representant har därutöver rätt att genomföra inspektioner, inklusive fysiska inspektioner, av de platser från vilka personuppgiftsbiträdet behandlar personuppgifter, inklusive fysiska lokaler och system som används för eller i samband med behandlingen. Sådana inspektioner får genomföras när den personuppgiftsansvarige finner det nödvändigt.

Begäran om fysisk inspektion ska lämnas med minst 30 dagars varsel. Den personuppgiftsansvarige ska själv bära eventuella kostnader i samband med en fysisk inspektion. Personuppgiftsbiträdet är skyldigt att avsätta den tid som krävs för att den personuppgiftsansvarige ska kunna genomföra sin inspektion. Den personuppgiftsansvarige debiteras för personuppgiftsbiträdet nedlagda tid samt kostnader förenade med en sådan tillsyn.

C.8 Förfaranden för revisioner, inklusive inspektioner, av behandling av personuppgifter som har anförtratts underpersonuppgiftsbiträden

Personuppgiftsbiträdet ska en gång per år, på underpersonuppgiftsbiträdet bekostnad, inhämta ett revisionsintyg från en oberoende extern part avseende de säkerhetsåtgärder som underpersonuppgiftsbiträdet har implementerat för att uppfylla dataskyddsförordningen, dataskyddsbestämmelser i annan EU-rätt eller medlemsstaternas nationella rätt samt dessa Bestämmelser.

Parterna är överens om att följande typer av revisionsintyg får användas i enlighet med dessa Bestämmelser:

ISAE 3000, SOC 1 och SOC 2, typ I eller typ II, eller annan rapportering baserad på jämförbara eller strängare standarder, eller tillsyn baserad på personuppgiftsbiträdet egna krav avseende

externa leverantörers policy för behandling och informationssäkerhet.

Om underpersonuppgiftsbiträdet är certifierat enligt ISO 27001 eller ISO 27701 under Bestämmelsernas giltighetstid ska certifieringen, eventuellt kompletterad med ledningsintyg eller liknande dokumentation, anses utgöra en tillräcklig form av tillsyn.

Personuppgiftsbiträdet ska, på den personuppgiftsansvariges skriftliga begäran, utan onödigt dröjsmål uppmana underpersonuppgiftsbiträdet att tillhandahålla revisionsintyg, ISO 27001-certifikat eller ISO 27701-certifikat, beroende på vad som är relevant.

Förfaranden för revisioner, inklusive inspektioner, av behandling av personuppgifter som har anförtrotts personuppgiftsbiträden och underpersonuppgiftsbiträden får när som helst genomföras med utgångspunkt i den tillsynsform som bedöms vara lämplig i enlighet med Integritetsskyddsmyndighetens vägledning om tillsyn av personuppgiftsbiträden.

Bilaga D Parternas reglering av andra förhållanden

Sekretess

Information avseende innehållet i dessa Bestämmelser, det underliggande Huvudavtalet eller den andra Partens verksamhet, som antingen vid utlämnandet till den mottagande Parten har angetts som konfidentiell information eller som till sin natur eller i övrigt tydligt måste uppfattas som konfidentiell, ska behandlas konfidentiellt och med minst samma omsorg och diskretion som parten iakttar för sina egna konfidentiella uppgifter. Data, inklusive personuppgifter, utgör alltid konfidentiell information.

Sekretessförpliktelsen gäller dock inte för information som är eller blir offentligt tillgänglig utan att detta beror på brott mot en Parts sekretessförpliktelse, eller information som redan innehas av den mottagande Parten utan motsvarande sekretessförpliktelse, eller information som självständigt har utvecklats av den mottagande Parten.