PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1]

1 PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	**Personuppgiftsbiträde**
Region Västmanland	WeDoBooks Sverige AB
Organisationsnummer	**Organisationsnummer**
232100–0172	556600-2126
Postadress	**Postadress**
Regionhuset, 721 89 Västerås	WeDoBooks Sverige AB c/o iOffice Sveavägen 34, 111 34 Stockholm
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: Erik Gurenwacht E-post: erik.gurenwacht@regionvastmanland.se Tfn: 021-961 42 66	Namn: Søren Eskildsen E-post: gdpr@wedobooks.io Tfn: +46858639000 (svenskt supportnummer)
Kontaktperson för parternas samarbete om dataskydd	**Kontaktpersoner för parternas samarbete om dataskydd**
Namn: Agata Cierzniak E-post: dataskyddsombudet@regionvastmanland.se Tfn: 021-17 65 69	Namn: Søren Eskildsen E-post: gdpr@wedobooks.io Tfn: +46858639000 (svenskt supportnummer)
Affärsavtal/Huvudavtal som detta personuppgiftsbiträdesavtal gäller och diarienummer	

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

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 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

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.

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 lokaliseringsuppgift 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. PUBavtalets 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 22 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 PUBavtalet 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, Instruktioner och Dataskyddslagstiftningen.

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.

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 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets 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 begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

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 Personuppgiftsbiträdets 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 Personuppgiftbiträdet 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 RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets 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 Personuppgiftbiträdet 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 Personuppgiftbiträdet 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 Personuppgiftincidentens 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, bilaga 2.

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 Underbiträdets 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 Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

a. Underbiträdets 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 Personuppgiftsbiträdets 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 Underbiträdets 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 PUBavtalets 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 tillsvidare. 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 PUBavtalet 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 12.7, 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 och

b. all tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

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 eller tillhörande information 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 epost 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 epost 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 lagvalsreglerna. Tvister med anledning av PUB-avtalet ska avgöras av behörig svensk domstol.

22 PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt undertecknande eller i pappersformat för egenhändigt undertecknande. I sistnämnda fall upprättas avtalet i två likalydande exemplar, varav parterna erhåller varsitt.

22.2 Om PUB-avtalet undertecknas elektroniskt lämnas signatursidan utan avseende.

Personuppgiftsansvarig

Region Västmanland

Ort och datum: [Ange ort och datum för signatur] Västerås 2025-09-17

Christer Alzén

Namnförtydligande

Signatur

Personuppgiftsbiträde

WeDoBooks Sverige AB

Ort och datum: [Ange ort och datum för signatur] Aarhus N, 15. juni 2025

Lasse Madsen Nyrup

Namnförtydligande

Signatur

Versionshantering

Versionshantering				
Dokument	Version	Datum	Ändringar	Ansvarig
Avtal, Bilaga 1, Bilaga 2	2.0	2022-12-21	1, 2, 3.1, 3.3, 5.1, 6.1, 6.5, 10.2, 12.2, 12.3, 12.4, 12.5, 12.7, 12.8, 12.9, 12.10, 14.3, 15, 16, 17, 18, 19, 20, 21, 22	HA, EW, FS (SKR)
Avtal	2.1	2023-04-06	Ändrat i hänvisning i 16.4 till 12.7	HA,PR (SKR)
Avtal	2.0	2023-09-27	Tillägg om diarienumret till affärsavtal/huvudavtal	MC (RV)
Bilaga 2	1.1	2023-09-27	Modul 1 Redogör ifall biträdet ingår i en koncern Modul 1 och 2 tillägg av organisationsnummer Ändamål som biträdet eller koncern behandlar personuppgifter	MC (RV)

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:

E-litteraturtjänsten är en gemensam sådan för de tio kommunbiblioteken i Västmanland. Personer som har ett användarkonto i bibliotekssamarbetet "Bibliotek i Västmanland", har tillgång till tjänsten och de som önskar kan nyttja den. Det som finns som grund i tjänsten är möjligheten att låna e-böcker samt e-ljudböcker, som tillval finns möjlighet att välja att spara boklån, minneslistor samt få personligt anpassade boktips.

1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Behandlingen omfattar uppgifter på bibliotekspersonal som administrerar tjänsten samt uppgifter på biblioteksanvändare som väljer att nyttja tjänsten. För att verifiera biblioteksanvändare rätt till åtkomst görs en slagning mot biblioteksdatasystemet. För att kunna få anpassade lästips krävs att biblioteksanvändaren lämnar uppgifter om födelsedatum, kön samt tidigare lån.

1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur):

Leverantören tillhandahåller:
- Drift
- Support
- Utveckling
- Kontohantering
- (På biblioteksanvändares begäran) Bearbetning och analys av tidigare lån för att tillhandahålla personifierade lästips

2. Behandlingen omfattar följande typer av Personuppgifter

Personuppgiftsbiträdet har rätt att behandla följande typer av Personuppgifter för den Personuppgiftsansvariges räkning:

- Namn
- Bibliotekskontonummer alt. personnummer
- Pin-kod

Dessa uppgifter nedan är frivilliga att lämna om man önskar personifierade lästips:
- Födelsedatum
- Kön

Dessa uppgifter nedan är frivilliga att lämna om man önskar kunna använda dem som inloggningsmetod:
- E-postadress
- Lösenord

3. Behandlingen omfattar vissa kategorier av Registrerade

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

- Anställda som administrerar webben.
- Biblioteksanvändare som önskar låna e-litteratur
- Biblioteksanvändare som även önskar spara tidigare lån samt minneslistor
- Biblioteksanvändare som även önskar personifierade lästips

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:

Se punkt 5

5. Ange de särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbiträdets Behandling av Personuppgifter

Personuppgiftbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna:

- Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC 27001:2022 eller motsvarande. Dessa dokument har godkänts och har kommunicerats till berörd personal och relevanta externa parter, samt ses över varje år och om betydande ändringar sker.

- Leverantören ska ha en dokumenterad organisation där roller och ansvar avseende informationssäkerhet är tydligt definierade.

- Leverantören ska ha tillsett att ansvar och arbetsuppgifter som står i konflikt med varandra och kan leda till missbruk är identifierade och tekniskt eller organisatoriskt åtskilda.

- Leverantören ska ha behörighetsstyrning med utpekade roller och ansvar som är åtkomst till regionen uppgifter.

- Leverantören ska ha dokumenterade rutiner och funktioner för att återlämna beställarens fysiska och elektroniska tillgångar då anställning, uppdrag eller avtal upphör. Format ska vara specificerat i förväg. Leverantören ska på begäran kunna uppvisa underlag på att så skett.

- Leverantören ska ha en formell och dokumenterad process för hur användaridentiteter hanteras (registrering och avregistrering). Leverantören ska säkerställa att användaridentiteterna hos leverantör och beställare är personliga och unika över tid. Se Diggs tillitsnivåer för e-legitimering för mer information.

- Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation ska skyddas och hanteras. De delar av verksamheten som berörs av leveransen informeras om sitt ansvar att skydda och hantera sina inloggningsuppgifter.

- Leverantören ska begränsa åtkomst till information. Behörigheterna ska tilldelas enligt principen där minsta möjliga behörighet tilldelas utifrån en användares roll och arbetsuppgifter. Detta gäller även konton som används vid kommunikation mellan systemkomponenter samt priviligierade konton. Endast information eller tjänster som ska vara publika ska kunna nås i system utan godkänd autentisering.
  Leverantören ska granska sina användares åtkomsträttigheter halvårsvis. Obehöriga eller användare som inte längre behöver åtkomst ska tas bort. Förändringar av åtkomsträttigheter ska dokumenteras av Leverantören och på begäran uppvisa underlag på att så skett.

- Leverantörens ansvar ska omfatta underleverantörer. Beställaren ska informeras om vilka underleverantörer som nyttjas.

- Beställaren ska årligen i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.

- Leverantören ska bedöma och besluta ifall en informationssäkerhetshändelse ska klassas som en informationssäkerhetsincident. Om händelsen i någon mån påverkar beställaren så ska beställaren inkluderas i detta beslut.

- Leverantörens ska dokumentera och utvärdera informationssäkerhetsincidenter senast inom en månad för att minska sannolikheten för liknande framtida händelser.

- Leverantören ska införa och upprätthålla:
  a) informationssäkerhetsåtgärder, stödsystem och verktyg enligt planer för kontinuitet,
  b) processer för att upprätthålla befintliga informationssäkerhetsåtgärder vid störning,
  c) ytterligare säkerhetsåtgärder för att komplettera de som inte kan upprätthållas under en störning.

- Leverantören ska ha en kontinuitetsplan som innehåller information som hjälper personalen att veta vad den ska göra vid en störning i en resurs eller aktivitet.

- Leverantören får ej återanvända information i system (texter, bilder etc.) eller tjänster i andra sammanhang än de avtalade.

- Leverantören ska tillse att beställarens information skyddas mot förlust, destruktion, förfalskning, obehörig åtkomst och otillåten utgivning.

- Leverantören ska utveckla och implementera regler för skydd av personuppgifter i enlighet med gällande lagar och förordningar, inklusive principerna om inbyggt dataskydd och dataskydd som standard. Dessa regler ska kommuniceras till alla medarbetare hos leverantören som berörs av leveransen och hanterar personuppgifter.

- Leverantören ska tillse att granskning av informationssäkerheten genomförs av oberoende part (exempelvis intern revisor eller specialiserad extern part). Granskningen sker minst vartannat år.

- Leverantören ska tillse att det finns dokumentation över informationssystem såsom användarmanualer och arkitekturdiagram. Dokumentationen ska vara tillgänglig för behörig personal i syfte att säkerställa:
  - informationssystemets konfiguration, installation och drift
  - effektiv användning av systemets säkerhetsfunktioner
  - användarhantering och användarrättigheter

  Dokumentationen hålls uppdaterad och ses över årligen eller vid större förändringar.

- Leverantören ska ha processer och rutiner på plats för bakgrundskontroll av personal.

- Leverantören ska för sin personal årligen genomföra utbildningar för ökad medvetenhet kring informationssäkerhet samt hålla sig uppdaterad kring beställarens policys, regler och rutiner.

- Leverantören ska säkerställa att dess anställda och eventuella underleverantörer behandlar information om och från beställaren konfidentiellt. T.ex. genom avtal om sekretess med medarbetare eller underleverantör.

- Leverantören ska ha dokumenterade rutiner för distansarbete. Informationsbehandlingen ska vara lika säker på distans som den är vid behandling på leverantörens arbetsplats.

- Leverantören ska tillse att endast behöriga personer får åtkomst till Beställarens information och andra relaterade tillgångar.
  Leverantören ska tillse att fysiska avgränsningar är definierade och tillämpade för skydd av områden med känslig eller kritisk information. Om det avser en datahall eller motsvarande ska leverantören tillse att den uppfyller minst skyddsnivå 3 ("datahall" enligt "MSB629 Vägledning för fysisk informationssäkerhet i it-utrymmen") eller likvärdigt.

- Leverantören har dokumenterade och kommunicerade regler för tillåten användning av lagrings- och informationsbehandlingsutrustning utanför leverantörens lokaler (t.ex. för persondatorer, planeringskalendrar, mobiltelefoner och smarta kort). Uppgifter får aldrig exporteras ut utanför systemet.

- Leverantören ska tillse att beställarens information som lagras på flyttbar lagringsmedia exempelvis mobiltelefoner, USB-minnen och externa hårddiskar hanteras i enlighet med fastställda rutiner (t.ex. kryptering, säkerhetskopiering, låsa in lagringsmedia etc.). Informationen ska raderas på ett sätt som gör att den inte är möjlig att återställa. Krävs kommunicering och godkännande från Region Västmanland.

- Leverantören ska tillse att informationsbehandlingsresurser (utrustning, it-stöd m.m.) är skyddad från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem exempelvis med hjälp av en UPS, "uninterruptible power supply".

- Leverantören ska tillse att kablage och utrustning avsedd för strömförsörjning och nätverksöverföring är skyddade mot otillbörlig åtkomst samt avsiktlig och oavsiktlig skada.

- Leverantören ska genomföra förebyggande underhåll av utrustning (exempelvis hårdvara) enligt underhållsplan.

- Leverantören ska använda särskilda personliga användaridentiteter för konton med höga behörigheter såsom administratörer eller andra roller med privilegierad behörighet. Kontona ska vara spårbara och enkla att urskilja från vanliga användarkonton. Vidare ska särskilda säkerhetsåtgärder tillämpas såsom tids- och godkännandebegränsningar.

- Leverantören ska tilldela behörigheter restriktivt och åtkomst begränsas till det som krävs för att utföra sitt uppdrag (t.ex. läs- eller skrivbehörigheter). Det finnas en dokumenterad behovs- och riskanalys för behörighetstilldelning. Samma princip gäller för beställarens egen personal.

- Leverantören ska tillse att tillgången till källkod för program begränsas. Förändringar i källkod kan härledas genom versionshantering och spårning.

- Leverantören ska tillse att åtkomst till informationstillgångar kräver flerfaktorsautentisering. Det finns regler för hur autentiseringsinformation får hanteras i system och av användaren.

- Leverantören ska skydda mot skadlig kod igenom att ha säkerhetsåtgärder som inbegriper följande områden: förebygga, upptäcka, hantera och återställa. Säkerhetsåtgärderna ska uppdateras kontinuerligt.

- Leverantören har utpekade roller och ansvar för hantering av tekniska sårbarheter såsom övervakning av sårbarheter, riskbedömning av sårbarheter, uppdateringar av system och övervakning av tillgångar.

  Granskning av teknisk efterlevnad för system (t.ex. penetrationstester och sårbarhetsgranskningar) genomförs årligen eller vid större förändringar.

- Leverantören ska tillse att konfigurationer, inklusive säkerhetskonfigurationer, av hårdvara, programvara, tjänster och nätverk är fastställda, dokumenterade och implementerade. Konfigurationerna övervakas och granskas regelbundet och uppdateras när nya hot eller sårbarheter behöver hanteras, eller när nya program- eller maskinvaruversioner lanseras.

- Leverantören ska genomföra oåterkallelig radering av beställarens information enligt de tidsfrister som är avtalade. Om inga tidsfrister är avtalade ska radering ske senast 30 dagar efter avslutat avtal eller på skriftlig begäran av beställaren.

  Informationen ska raderas på ett sätt som gör att den inte är möjlig att återställa.

- Leverantören ska ha verktyg för att upptäcka och förhindra att personer eller system utan behörighet röjer eller extraherar information. Det innebär bland annat (men är inte begränsat till) att leverantören ska ha en baslinje för vad sin utgör normalt dataflöde, förmåga att identifiera dataflöden och datarörelser som ligger inom och utanför baslinjen (onormalt beteende) samt åtgärder för att hantera avvikelser och potentiella incidenter.

- Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt avtalade tillgänglighetskrav (SLA - service level agreement). Säkerhetskopior ska skyddas på motsvarande sätt som originalinformationen och förvaras på annan plats med tillräckligt avstånd för att inte utsättas för eventuella skador vid katastrof på det ordinarie driftstället. Hur länge säkerhetskopiorna sparas ska vara dokumenterat i överenskommelse eller avtal.

  Återläsningstester ska dokumenteras och leverantören ska på beställarens begäran redovisa när återläsningstester genomförts och resultatet av dessa.

- Leverantören ska tillse att informationsbehandlingsresurser har tillräcklig redundans för att uppfylla verksamhetens tillgänglighetskrav (SLA - service level agreement). Redundanta informationssystem testas, helst i produktionsläge, för att säkerställa att felöverlämningen från en enhet till en annan fungerar som avsett.

- Leverantören ska övervaka nätverk, system och applikationer i fråga om onormalt beteende och lämpliga åtgärder vidtas för att utvärdera potentiella informationssäkerhetsincidenter.

- Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll och säkerhetskonfiguration för information, tjänster och system.

- Leverantören ska ha regler för användning av nätverk och nätverkstjänster, dessa omfattar bland annat tillåten åtkomst till nätverk och autentiseringskrav för åtkomst till olika nättjänster.

- Leverantören ska tillhandahålla en (logisk eller fysiskt) separerad kundmiljö inklusive behörighetskontrollsystem, loggar och lagring avseende beställarens information.

- Leverantören ska ha riktlinjer för hur kryptografiska säkerhetsåtgärder ska användas för skydd av information.
  Dokumentation ska omfatta krav för hantering av krypteringsnycklar för hela deras livscykel inklusive generering, lagring, arkivering, hämtning, distribution, återkallande och destruering av nycklar. (Krav på hur privata nycklar skapas och sparas).

- Leverantören ska ha regler för säker utveckling av program och system inom organisationen. Dessa regler omfattar bland annat system- och säkerhetstestning, t.ex. regressionstestning, kodskanning och penetrationstester.

- Leverantören ska identifiera och specificera informationssäkerhetskrav när applikationer utvecklas eller anskaffas. Detta kan ske i enlighet med Secure Software Development Lifecycle (SSDLC) eller motsvarande.

- Leverantören ska ha fastställd dokumentation för säker systemutveckling och kontrollera att dessa efterlevs.

- Leverantören ska tillse att principer för säker kodning både vid nyutveckling och återanvändning av kod (dokumentation, parprogrammering, testdriven utveckling, kodgranskning m.m.) tillämpas.

- Leverantören ska tillse att nya och uppdaterade informationssystem testas grundligt och verifieras under utvecklingsprocessen, inklusive utarbetandet av en detaljerad aktivitetsplan samt testning av indata och förväntad utdata under en rad villkor.

- Leverantören ska övervaka och styra systemutveckling som är utlagd till en underleverantör.

- Leverantören ska säkerställa att utvecklings-, test- och driftmiljöer är separerade för att minska risken för obehörig åtkomst och ändringar i driftmiljön.

- Leverantören ska ha en dokumenterad process för ändringshantering som tillämpas vid behov. Det finns även rutiner för att avbryta och återställa vid misslyckade ändringar. Testning ska utföras i en separat miljö för att minimera påverkan på produktionssystemen.

- Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i produktionsmiljö. Känslig information (bl.a. personuppgifter eller verksamhetskritisk information) ska inte kopieras in i utvecklings- och testmiljöer.

- Leverantören ska tillse att granskning och test av system planeras så att störningar på beställarens verksamhet minimeras.

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 logghantering:

- Leverantören ska ha dokumenterade regler för att kontrollera fysisk och logisk åtkomst till informationstillgångar. Granskning av åtkomsträttigheter genomförs minst årligen. Leverantören ska följa en överenskommelse för användaråtkomst till beställarens system, tjänster och information. Endast behöriga och enligt överenskommelsen godkända individer ska inneha åtkomst. Hanteringen ska vara spårbar.

- Leverantören ska tillse att information, tjänster och system har loggningsfunktioner för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Loggning ska ske i samråd med beställaren. Leverantören ska aktivt använda loggarna för att upptäcka och hantera incidenter. Beställaren ska kunna genomföra granskning av loggar vid behov. Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst som även omfattar leverantörens personal.

7. Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgiftsbiträdet ska iaktta följande krav avseende lokalisering av Personuppgifter:

- Inga tredjelandsöverföringar ska förekomma. Vid de fall där det är absolut nödvändigt för att kunna utföra behandlingen ska det särskilt överenskommas med Personuppgiftsansvarig och ett av nedanstående kriterier måste uppfyllas, dokumenteras och godkännas.
- Leverantören ska ha ett av Integritetsskyddsmyndigheten eller annan tillsynsmyndighet inom EU godkänt BCR (Binding corporate rules)
- Om leverantören är registrerad och lokaliserad i ett land som EU-kommissionen godkänt som ett land med adekvata skyddsnivå eller om det tecknats SCC (Standard contractual clauses som är framtagen av EU-kommissionen) med underbiträdet i samband med tredjelandsöverföring.
- Tredjelandsöverföring som uppkommer i samband med nyttjande av underbiträde ska biträdet tillse att lämpliga skyddsåtgärder vidtas enligt artikel 46 allmänna dataskyddsförordningen och enligt EDPBs riktlinjer om säkerhetsåtgärder.

8. Behandlingens varaktighet
• Personuppgiftsbiträde får behandla personuppgifter åt den Personuppgiftsansvarige under affärsavtalets giltighet.
9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet
• Vid utökning eller införande med behandling av ny eller innovativ teknik så som AI funktionalitet eller annan liknande automatiserad teknik/funktion skall detta regleras genom separat instruktion som särskilt beaktar den nya AI förordningen (AI- Act) • Vid upptäckt personuppgiftsincident ska Personuppgiftsbiträdet ska skriftligen informera kontaktperson för detta personuppgiftsbiträdesavtal och Region Västmanlands dataskyddsombud. • Anlitande av personuppgiftsunderbiträde enligt Personuppgiftsbiträdesavtal 12.6 ska informera kontaktperson för detta personuppgiftsbiträdesavtal och Region Västmanlands dataskyddsombud.

Bilaga 2 - Lista över godkända Underbiträden

Personuppgiftsbiträdet redogör för följande om bolaget ingår i en koncern.

Bolag/ organisation och organisationsnummer	**Adress och kontaktuppgifter**	**Lokalisering av Personuppgifter (adress, land)**	**Typer av Personuppgifter som koncernen kan ha insyn och tillgång till**
WeDoBooks A/S	P. O. Pedersens Vej 14E DK-8200 Aarhus (+45) 70 22 05 04	Danmark	Personnummer E-post Namn Kön (valfritt) Ålder (valfritt)

Den Personuppgiftsansvarige godkänner att Personuppgiftsbiträdet anlitar nedanstående Underbiträden för Behandling av Personuppgifter.

Bolag/ organisation och organisations-nummer	**Adress och kontaktuppgifter**	**Lokalisering av Personuppgifter (adress, land)**	**Typer av Personuppgifter som Behandlas av Underbiträdet**	**Ändamål med Underbiträdets Behandling**	**Behandlingstid**	**Ytterligare information om Underbiträdets Behandling av Personuppgifter**
Google Cloud EMEA Ltd.	70 Sir John Rogerson's Quay, D02 R296, Dublin, Ireland	Tyskland och Belgien	Personnummer E-post Namn Kön (valfritt) Ålder (valfritt)	Google ansvarar för all hosting och digital infrastruktur för tjänsten Biblio. Servrar och liknande är uppsatta i molntjänster för hantering av data och information för att vi ska kunna tillhandahålla tjänsten Biblio.	Behandlingen pågår under hela den tid som avtalet är giltigt.	https://www.google.com/about/datacenters/data-security/
Hubspot Ireland Limited	HubSpot House, 1 Sir John Rogerson's Quay, D02 CR67, Dublin, Ireland	Tyskland	E-post Namn	Hubspot tillhandhåller system för CRM och support. Där registreras alla supportärenden samt marknadsföringsaktiviteter riktade mot kunder.	Behandlingen pågår under hela den tid som avtalet är giltigt.	
Twilio Inc.	645 Harrison Street, Third Floor, 94107,	USA	E-post Namn	Twilio hanterar e-post som skickas ut från våra tjänster till	Behandlingen pågår under hela den tid som	

	San Francisco, CA, United States of America			både bibliotekets anställda och slutanvändare. Det kan vara exempelvis mejl för hantering av användare (glömt lösenord etc.)	avtalet är giltigt.	