Personuppgiftsbiträdesavtal

Preauditor Sweden AB, Senast uppdaterad: 2026-11-16, gäller från: 2026-12-17

Detta personuppgiftsbiträdesavtal ("Biträdesavtalet") utgör en del av avtalet mellan Kunden och Preauditor Sweden AB avseende Kundens användning av Tjänsten.

1. Parter

1.1 Kunden är antingen personuppgiftsansvarig för den behandling av personuppgifter som sker inom ramen för Kundens användning av Tjänsten, eller personuppgiftsbiträde åt en eller flera Slutkunder som är personuppgiftsansvariga för sådan behandling. Kunden ansvarar för att avgöra i vilken roll Kunden behandlar personuppgifter i Tjänsten och för att vid var tid känna till denna roll.

1.2 Preauditor Sweden AB, org.nr 556520-7536 ("Preauditor"), är personuppgiftsbiträde för sådan behandling av personuppgifter som Preauditor utför för Kundens räkning när Kunden är personuppgiftsansvarig, och underbiträde enligt artikel 28.4 GDPR när Kunden är personuppgiftsbiträde åt Slutkund.

1.3 Med "Slutkund" avses ett bolag, en enskild näringsidkare eller annan juridisk eller fysisk person som bedriver näringsverksamhet och för vars räkning Kunden använder Tjänsten inom ramen för ett uppdrags- eller redovisningsavtal, och som är personuppgiftsansvarig för de personuppgifter som Kunden eller någon på Kundens vägnar gör tillgängliga i Tjänsten för Slutkundens räkning.

1.4 Där detta Biträdesavtal anger att en åtgärd ska vidtas gentemot Kunden, på instruktion av Kunden eller för Kundens räkning, gäller detta även när Kunden agerar för Slutkunds räkning. Preauditor har inget avtalsförhållande med Slutkunden och ska, om inte annat uttryckligen anges i detta Biträdesavtal eller följer av tvingande lag, uteslutande ta emot instruktioner från och lämna information till Kunden.

2. Syfte och företräde

2.1 Biträdesavtalet reglerar Preauditors behandling av personuppgifter för Kundens

räkning i enlighet med artikel 28 i Europaparlamentets och rådets förordning (EU) 2016/679 ("GDPR").

2.2 Vid motstridighet mellan detta Biträdesavtal och övriga avtalsdokument mellan parterna ska detta Biträdesavtal ha företräde i frågor som rör behandling av personuppgifter för Kundens räkning.

3. Behandlingens art, ändamål och varaktighet

3.1 Preauditor får behandla personuppgifter endast i den utsträckning som är nödvändig för att tillhandahålla Tjänsten till Kunden och i övrigt enligt dokumenterade instruktioner från Kunden.

3.2 Behandlingens ändamål är att möjliggöra Kundens användning av Tjänsten, inklusive lagring, strukturering, sökning, sammanställning, analys, export, återlämning, radering, support och andra åtgärder som är nödvändiga för Tjänstens funktion. Biträdesavtalet omfattar däremot inte sådan behandling där Preauditor är personuppgiftsansvarig, exempelvis Preauditors egen support-, onboarding- och kommunikationshantering av auktoriserade användare via Intercom i inloggat läge, utom i den mån Preauditor inom ramen för ett sådant ärende behandlar personuppgifter för Kundens räkning i Tjänsten enligt Kundens dokumenterade instruktioner.

3.3 Behandlingen omfattar även att Preauditor, på Kundens instruktion, hämtar uppgifter från de Partnertjänster, banker och myndigheter som Kunden ansluter till Tjänsten, såsom Kundens bokföringsprogram, lönesystem, bank och Skatteverket, samt hämtar eller verifierar uppgifter från externa datakällor om företag, företrädare, ägare, verkliga huvudmän, styrelse, bolagsengagemang och därmed sammanhängande företagsinformation, i den utsträckning sådana funktioner ingår i Tjänsten. Behandlingen får även omfatta att Preauditor skapar rapporter eller PDF-filer, eller delar dem med av Kunden utsedd mottagare, såsom Kundens revisor.

3.4 Behandlingen omfattar även inläsning och tolkning av underlag och dokument samt generering av analyser, förklaringar och förslag med hjälp av AI-modeller, i de kontroller i Tjänsten som bygger på sådan behandling, enligt punkterna 7.7 - 7.11.

3.5 Biträdesavtalet gäller så länge Preauditor behandlar personuppgifter för Kundens räkning.

4. Kategorier av registrerade och personuppgifter

4.1 Biträdesavtalet omfattar behandling av personuppgifter som Kunden eller någon på Kundens vägnar gör tillgängliga i Tjänsten eller instruerar Preauditor att behandla inom ramen för Tjänsten. Detta omfattar inte sådan behandling av personuppgifter om auktoriserade användare eller andra kontaktpersoner som Preauditor utför som personuppgiftsansvarig för egen support-, onboarding- eller kommunikationsfunktion, såsom via Intercom i inloggat läge, annat än när Preauditor behandlar personuppgifter för Kundens räkning i Tjänsten.

4.2 Registrerade kan bland annat omfatta:

- Auktoriserade användare och andra företrädare för Kunden.
- Enskild näringsidkare som är Kund eller Slutkund.
- Kundens anställda, uppdragstagare, kunder (även privatpersoner, till exempel köpare av ROT- och RUT-arbeten), leverantörer och andra affärskontakter.
- Verkliga huvudmän, ägare, styrelseledamöter och andra personer vars uppgifter behandlas som en del av Kundens användning av Tjänsten.
- Personer vars uppgifter förekommer i underlag och dokument som behandlas i Tjänsten, såsom kvitton, fakturor, avtal, lönebesked, deklarationer och årsredovisningar.
- Revisor eller annan mottagare som Kunden instruerar Preauditor att dela rapporter eller sammanställningar med.
- Slutkundens företrädare, anställda, uppdragstagare, kunder, leverantörer och andra affärskontakter, när Kunden använder Tjänsten för Slutkunds räkning.
- Närstående och andra personer vars uppgifter förekommer i externa datakällor och behandlas som en del av Kundens användning av Tjänsten.

4.3 Personuppgifter kan bland annat omfatta:

- Namn, e-postadress, telefonnummer och andra kontaktuppgifter.
- Kontouppgifter, användar-ID och inloggningsrelaterade uppgifter.
- Bokföringshändelser, transaktionsuppgifter, verifikationer och deras underlag, kund- och leverantörsreskontror, rapportunderlag och annan data som Kunden använder i Tjänsten.

• Lönedata från Kundens lönesystem, såsom anställningsnummer, anställningsform, löneform, arbetstid, lönerader, närvaro och frånvaro samt semesterlöneskuld, inklusive sjukfrånvaro per dag enligt punkt 7.11.
• Uppgifter från Kundens bank, såsom konton, saldon och transaktioner.
• Uppgifter från Skatteverket, såsom skattekonto, moms- och arbetsgivardeklarationer, inkomstdeklarationer och registreringsuppgifter.
• Dokument som Kunden laddar upp, såsom årsredovisningar, anläggningsregister, lagerlistor, uppdragsregister, leasingavtal och deklarationer.
• Uppgifter om verkliga huvudmän, ägarstruktur, styrelseledamöter, bolagsengagemang och liknande företagsinformation som hämtas eller verifieras från externa datakällor.
• Personnummer i den utsträckning som anges i punkt 7.2.
• Det som läses ut ur underlag och dokument med AI-modeller, samt Kundens frågor, svar och förklaringar i Tjänsten.

5. Kundens ansvar och instruktioner

5.1 Kunden ansvarar för att behandlingen av personuppgifter som Kunden initierar genom Tjänsten har en giltig rättslig grund och i övrigt uppfyller tillämplig dataskyddslagstiftning.

5.2 Kunden ansvarar för riktigheten, aktualiteten och lagenligheten i de personuppgifter som Kunden tillhandahåller eller instruerar Preauditor att behandla.

5.3 Kundens instruktioner framgår av detta Biträdesavtal, huvudavtalet, användningen av Tjänsten, supportärenden som avser behandling av personuppgifter för Kundens räkning i Tjänsten och andra skriftliga instruktioner från Kunden. Användning av Tjänsten av Auktoriserade Användare, inklusive sådana företrädare för Slutkund som Kunden gett behörighet i Tjänsten, utgör Kundens instruktion. När Kunden är personuppgiftsbiträde åt Slutkund ska Slutkundens instruktioner i övrigt förmedlas till Preauditor genom Kunden, och en instruktion som Slutkunden lämnar direkt till Preauditor på annat sätt än genom sådan användning av Tjänsten ska inte anses utgöra en instruktion enligt detta Biträdesavtal förrän Kunden skriftligen har bekräftat den, om inte Preauditor är skyldigt att följa instruktionen enligt lag eller annat följer av punkt 5.10. Allmän support, onboarding och kommunikation via Intercom i Preauditors egen regi ska inte i sig anses utgöra Kundens instruktion enligt detta Biträdesavtal.

5.4 Om Preauditor saknar instruktion i en fråga som är nödvändig för att utföra uppdraget ska Preauditor utan onödigt dröjsmål begära sådan instruktion från Kunden.

5.5 Om Kunden är personuppgiftsbiträde åt Slutkund garanterar Kunden att Kunden har ingått uppdrags- eller redovisningsavtal med Slutkunden, att Kunden enligt det avtalet har rätt att lägga upp Slutkunden i Tjänsten, att Kunden har ingått personuppgiftsbiträdesavtal med Slutkunden enligt artikel 28.3 GDPR, vilket får ingå i uppdrags- eller redovisningsavtalet, och att Kunden har Slutkundens skriftliga tillstånd enligt artikel 28.2 GDPR att anlita Preauditor som underbiträde samt att Kunden i förekommande fall har underrättat Slutkunden om att Preauditor anlitas.

5.6 Kunden garanterar att de instruktioner som Kunden lämnar till Preauditor ryms inom och inte går utöver de dokumenterade instruktioner som Slutkunden har lämnat till Kunden, samt att varje behandling som Kunden initierar i Tjänsten för Slutkunds räkning har en giltig rättslig grund hos Slutkunden. Preauditor är inte skyldigt att kontrollera Kundens behörighet gentemot Slutkunden och har rätt att förlita sig på Kundens uppgifter i detta avseende. Preauditor får dock begära att Kunden styrker sin behörighet och vidta åtgärder enligt punkterna 3.16 och 3.27 i huvudavtalet. Sådana åtgärder inskränker inte Kundens ansvar enligt punkterna 5.5 - 5.8.

5.7 Preauditor är inte bundet av Kundens avtal med Slutkunden, och Kunden ansvarar själv för sina åtaganden enligt det avtalet. Om det avtalet innehåller mer långtgående dataskyddsskyldigheter än detta Biträdesavtal ska Kunden meddela Preauditor skriftligen innan Slutkunden läggs upp i Tjänsten. Preauditor får då skriftligen acceptera skyldigheterna, neka uppläggningen eller, med trettio (30) dagars varsel, upphöra att behandla personuppgifter för den Slutkundens räkning, varvid punkt 14.5 tillämpas.

5.8 Kunden ska hålla Preauditor skadeslöst för krav, skada, sanktionsavgift och kostnad som drabbar Preauditor till följd av att Kunden saknat erforderligt uppdragsavtal, personuppgiftsbiträdesavtal, tillstånd, fullmakt eller rättslig grund enligt punkterna 5.5 och 5.6. Sådant ansvar regleras av punkt 3.18 i huvudavtalet.

5.9 Om Kundens uppdrag för en Slutkund upphör, eller om Slutkundens tillstånd att anlita Preauditor som underbiträde återkallas, ska Kunden utan onödigt dröjsmål informera Preauditor och lämna instruktion enligt punkt 14.

5.10 Om Slutkunden, genom företrädare som styrkt sin behörighet enligt punkt 3.24 i huvudavtalet, gör gällande att Kunden saknar uppdrag eller tillstånd enligt punkt 5.5, eller begär utlämnande eller överlåtelse enligt punkterna 3.23 - 3.25 i huvudavtalet, eller om

Kunden inte styrkt sin behörighet enligt punkt 3.16 i huvudavtalet, har Preauditor rätt att ta emot instruktioner direkt från Slutkunden avseende den Slutkundens personuppgifter och att lämna information direkt till Slutkunden. Slutkundens instruktion har i sådant fall företräde framför Kundens instruktion avseende den Slutkundens personuppgifter. Punkterna 1.4, 5.3, 10.4 och 14.4 gäller inte i den utsträckning de strider mot denna punkt.

6. Preauditors åtaganden som personuppgiftsbiträde

6.1 Preauditor får endast behandla personuppgifter i enlighet med Kundens dokumenterade instruktioner, om inte annat krävs enligt unionsrätt eller svensk rätt. När Kunden är personuppgiftsbiträde åt Slutkund utgör Kundens dokumenterade instruktioner till Preauditor även Preauditors instruktioner i förhållande till Slutkundens personuppgiftsansvar. Preauditor kontrollerar inte att instruktionerna ryms inom Kundens uppdrag från Slutkunden, vilket Kunden ansvarar för enligt punkt 5.6.

6.2 Om Preauditor enligt lag är skyldigt att behandla personuppgifter på annat sätt än enligt Kundens instruktioner ska Preauditor informera Kunden om detta innan behandlingen sker, om inte sådan information är förbjuden enligt lag.

6.3 Preauditor ska säkerställa att personer som är behöriga att behandla personuppgifter har åtagit sig att iaktta konfidentialitet eller omfattas av lämplig lagstadgad tystnadsplikt.

6.4 Preauditor ska föra lämplig intern dokumentation över behandlingen i den utsträckning som krävs enligt tillämplig lag.

6.5 Om Preauditor anser att en instruktion från Kunden strider mot GDPR eller annan tillämplig dataskyddslagstiftning ska Preauditor utan onödigt dröjsmål informera Kunden. Preauditor har rätt att avvakta med att verkställa instruktionen till dess att frågan har klarlagts.

7. Särskilt om personnummer, externa datakällor, AI-funktioner och känsliga personuppgifter

7.1 Personnummer används inte i Tjänstens kontroll av närståendetransaktioner, där

behandling sker med utgångspunkt i fullständigt namn.

7.2 Personnummer får behandlas av Preauditor endast i den utsträckning det är nödvändigt för att, på Kundens instruktion, (a) identifiera en enskild näringsidkare som är Kund eller Slutkund, vars organisationsnummer är näringsidkarens personnummer, och hämta uppgifter om näringsidkaren från Skatteverket och andra källor som Kunden har anslutit, (b) behandla underlag, dokument och data där personnummer förekommer, såsom lönedata, deklarationer, kundfakturor avseende ROT- och RUT-arbeten och uppgifter från extern datakälla, och (c) entydigt identifiera en fysisk person vid inhämtning eller verifiering av uppgifter från extern datakälla.

7.3 Preauditor ska begränsa behandling av personnummer till vad som är nödvändigt för ändamålet och vidta särskilda tekniska och organisatoriska skyddsåtgärder med hänsyn till uppgifternas känslighet. Preauditor använder inte personnummer för att identifiera företag i Tjänstens databaser och filer, tar bort personnummer ur det som läses ut ur underlag och dokument innan det sparas, och tolkar eller sparar inte de anställdas personnummer, namn, adresser eller bankuppgifter från Kundens lönesystem.

7.4 Preauditor får använda externa datakällor i den utsträckning det är nödvändigt för att utföra funktioner eller behandlingar som Kunden initierar genom sin användning av Tjänsten, såsom att hämta, verifiera, sammanställa eller dela information enligt detta Biträdesavtal. Sådan användning ska anses ske inom ramen för Kundens dokumenterade instruktioner enligt detta Biträdesavtal, huvudavtalet och Kundens användning av Tjänsten, utan krav på separat godkännande av varje extern datakälla.

7.5 I den mån en inhämtning från extern datakälla utgör en kreditupplysning om en fysisk person enligt kreditupplysningslagen (1973:1173) kan kreditupplysningsföretaget vara skyldigt att sända ett meddelande (omfrågekopia) till den registrerade med uppgift om vem som har begärt upplysningen. Kunden eller, när Kunden är personuppgiftsbiträde åt Slutkund, Slutkunden ansvarar i egenskap av personuppgiftsansvarig för att beakta detta och för att lämna registrerade sådan information som krävs enligt artiklarna 13 och 14 GDPR.

7.6 Preauditor ska på Kundens begäran informera Kunden om vilka externa datakällor som vid var tid används i Tjänsten. Sådan information lämnas i den form och omfattning som anges i punkterna 12.1 och 12.4.

7.7 Vissa av Tjänstens kontroller bygger på att underlag och dokument, såsom kvitton, fakturor, avtal, lönebesked, register, listor, deklarationer och årsredovisningar, läses in och tolkas med hjälp av AI-modeller, och att AI-modeller genererar analyser, förklaringar, förslag och andra utfall på grundval av personuppgifter som behandlas för Kundens räkning ("AI-funktioner"). AI-funktionerna är en del av de kontroller som bygger på dem och kräver ingen separat aktivering. Kundens användning av en sådan kontroll, och Kundens anslutning av de källor som underlagen hämtas från, utgör Kundens dokumenterade instruktion om sådan behandling enligt punkt 5.3. Sådan behandling utgör behandling för Kundens räkning enligt detta Biträdesavtal.

7.8 Behandling av personuppgifter i AI-funktionerna sker i datacenterregion inom EU/EES. Preauditor får inte förlägga sådan behandling utanför EU/EES utan att först informera Kunden och säkerställa en giltig överföringsmekanism enligt punkterna 13.1 och 13.2.

7.9 Personuppgifter som behandlas i AI-funktionerna används inte för att träna, finjustera, utvärdera eller på annat sätt utveckla AI-modeller, vare sig hos Preauditor, hos modelleverantören eller hos annan tredje man. Preauditors rätt enligt huvudavtalet att skapa anonymiserad statistik innefattar inte rätt att använda personuppgifter som behandlas för Kundens räkning, eller data som härletts ur sådana personuppgifter, för sådan modellträning.

7.10 Uppgifter som lämnas till eller genereras av AI-modellen får lagras hos modelleverantören tillfälligt för att leverera svaret till Preauditor, och då högst i tjugofyra (24) timmar. Därutöver kan modelleverantören enligt sina villkor logga uppgifter i syfte att upptäcka missbruk av sina tjänster. Preauditor ska konfigurera AI-funktionerna så att lagring och manuell granskning hos modelleverantören begränsas i den utsträckning modelleverantören tillhandahåller sådan konfiguration. Preauditor ska på Kundens begäran informera om vid var tid gällande villkor för loggning, lagring och missbruksövervakning hos modelleverantören samt utan onödigt dröjsmål underrätta Kunden om dessa villkor ändras väsentligt.

7.11 Tjänsten är inte avsedd för behandling av särskilda kategorier av personuppgifter enligt artikel 9 GDPR eller personuppgifter som rör fällande domar i brottmål och lagöverträdelser enligt artikel 10 GDPR. Kunden får inte, och ska säkerställa att Slutkunden och Auktoriserade Användare inte, ladda upp eller mata in sådana uppgifter i Tjänsten utan att parterna först har träffat särskild skriftlig överenskommelse om detta. Från detta gäller följande undantag. Uppgifter om sjukfrånvaro per dag i lönedata som

hämtas från Kundens lönesystem behandlas endast för att beräkna betalda timmar i de kontroller som bygger på lönedata, finns endast i arbetsminnet under beräkningen och sparas inte i Tjänsten. Om sådana uppgifter i övrigt förekommer i underlag som hämtas från Kundens bokföringsprogram eller lönesystem, till exempel i ett lönebesked, behandlas de endast i den utsträckning det krävs för kontrollen. Kunden, eller när Kunden är personuppgiftsbiträde åt Slutkund, Slutkunden, ansvarar i egenskap av personuppgiftsansvarig för att det finns en rättslig grund och ett tillämpligt undantag enligt artikel 9.2 GDPR för sådan behandling, såsom artikel 9.2 b GDPR.

8. Säkerhetsåtgärder

8.1 Preauditor ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken enligt artikel 32 GDPR.

8.2 Sådana åtgärder ska, i den mån det är lämpligt, omfatta:

- Lagring av personuppgifter som behandlas för Kundens räkning i datacenter inom EU/EES.
- Behörighetsstyrning och åtkomstkontroll enligt principen om minsta åtkomst, både för Auktoriserade Användare och för Preauditors personal.
- Loggning och uppföljning av åtkomst till personuppgifter.
- Kryptering vid överföring och lagring.
- Rutiner för säkerhetskopiering, återställning, testning och incidenthantering.
- Rutiner för att separera Kundens data från andra kunders data.

8.3 En översiktlig beskrivning av säkerhetsarbetet finns på www.preauditor.se/sakerhet. Närmare information lämnas enligt punkt 12.1.

9. Underbiträden

9.1 Kunden ger Preauditor ett generellt förhandsgodkännande att anlita underbiträden för behandling av personuppgifter, under förutsättning att Preauditor säkerställer att underbiträdet omfattas av skriftligt avtal som ålägger underbiträdet minst samma dataskyddsskyldigheter som följer av detta Biträdesavtal.

9.2 De underbiträden som används för behandling av personuppgifter för Kundens räkning

när detta Biträdesavtal träder i kraft anges i Bilaga 1. Bilaga 1 hålls aktuell, och ändringar meddelas enligt punkt 9.6. Preauditor ska på begäran informera Kunden om vilka underbiträden som används.

9.3 Kunden är införstådd med att Preauditor anlitar extern datakälla, för närvarande The Intelligence Company AB, för att hämta eller verifiera uppgifter om företag, företrädare, ägare, verkliga huvudmän och övrig företagsinformation i Tjänsten. Leverantören av den externa datakällan bestämmer självständigt ändamål och medel för den behandling som sker i dess egen upplysnings- eller informationsverksamhet, behandlar därmed personuppgifter som självständigt personuppgiftsansvarig och inte enligt instruktioner från Preauditor eller Kunden, och är därför inte underbiträde enligt detta Biträdesavtal. Detta gäller även när Preauditor lämnar sökbegrepp, såsom namn, organisationsnummer eller personnummer, till leverantören; ett sådant utlämnande sker på Kundens instruktion och, när Kunden är personuppgiftsbiträde åt Slutkund, inom ramen för Slutkundens instruktion enligt punkt 5.6, varvid rättslig grund för utlämnandet ska finnas hos den personuppgiftsansvarige. Preauditor lämnar inga utfästelser om leverantörens tillstånd, registrering eller efterlevnad av tillämplig lagstiftning, utan ska på begäran enligt punkt 7.6 upplysa Kunden om vilken leverantör som används.

9.4 Revisor eller annan mottagare som Kunden instruerar Preauditor att dela rapport eller sammanställning med ska inte anses vara underbiträde till Preauditor för sådan mottagning, utan mottagare på Kundens instruktion.

9.5 Kunden är införstådd med att Intercom kan användas av Preauditor för support, onboarding och kommunikation med auktoriserade användare i inloggat läge. I den mån sådan användning avser Preauditors egen personuppgiftsansvariga behandling och inte behandling av personuppgifter för Kundens räkning ska Intercom inte anses vara underbiträde enligt detta Biträdesavtal.

9.6 Om Preauditor avser att lägga till eller byta ut ett underbiträde ska Kunden informeras skriftligen minst trettio (30) dagar innan ändringen träder i kraft.

9.7 Om ett underbiträde inte uppfyller sina dataskyddsskyldigheter ska Preauditor förbli fullt ansvarigt gentemot Kunden för underbiträdets behandling i den utsträckning som följer av GDPR och detta Biträdesavtal.

9.8 Kunden är införstådd med att Preauditor för Tjänstens AI-funktioner anlitar Google Cloud EMEA Limited (Google Cloud Platform, Vertex AI) som underbiträde, med behandling i datacenterregion inom EU/EES. Underbiträdet får behandla personuppgifter endast för att leverera svar till Preauditor och på de villkor som anges i punkterna 7.7 - 7.11. Kunden har rätt att invända mot att ett underbiträde läggs till eller byts ut enligt artikel 28.2 GDPR inom trettio (30) dagar från information enligt punkt 9.6, varvid parterna ska söka en lösning i samförstånd och Kunden, om sådan inte nås, har rätt att säga upp huvudavtalet med verkan från den tidpunkt då ändringen träder i kraft.

9.9 När Kunden är personuppgiftsbiträde åt Slutkund lämnas det generella förhandsgodkännandet enligt punkt 9.1 av Kunden för Slutkundens räkning, och Kunden garanterar att Slutkunden har godkänt att underbiträden anlitas på motsvarande sätt. Information enligt punkterna 9.2, 9.6 och 9.8 lämnas till Kunden, som ansvarar för att vidarebefordra informationen till berörda Slutkunder i den utsträckning Slutkundens avtal med Kunden kräver det, och för att inhämta Slutkundens ställningstagande innan invändning framställs enligt punkt 9.8.

9.10 Partnertjänster, banker och myndigheter som Kunden ansluter till Tjänsten, såsom Kundens bokföringsprogram, lönesystem, bank och Skatteverket, är inte underbiträden till Preauditor. Kunden har ett eget avtals- eller rättsförhållande med dem, och Preauditor hämtar uppgifter därifrån på Kundens instruktion. Detsamma gäller när Preauditor på Kundens instruktion lämnar uppgifter till dem, till exempel en enskild näringsidkares personnummer till Skatteverket för att hämta uppgifter om näringsidkaren.

10. Bistånd till Kunden

10.1 Preauditor ska, med beaktande av behandlingens art och den information som Preauditor har tillgång till, bistå Kunden genom lämpliga tekniska och organisatoriska åtgärder så att Kunden kan fullgöra sina skyldigheter att svara på begäran om registrerades rättigheter.

10.2 Preauditor ska vidare bistå Kunden med den information som skäligen krävs för att Kunden ska kunna uppfylla sina skyldigheter avseende säkerhet, personuppgiftsincidenter, konsekvensbedömningar och samråd med tillsynsmyndighet.

10.3 Om en registrerad, tillsynsmyndighet eller annan tredje man kontaktar Preauditor i en

fråga som rör behandling för Kundens räkning ska Preauditor utan onödigt dröjsmål hänvisa frågan till Kunden, om inte Preauditor är skyldigt att agera enligt lag. Om en tillsynsmyndighet inleder tillsyn av Preauditor som avser behandling för Kundens räkning ska Preauditor, i den mån det inte är förbjudet enligt lag, utan onödigt dröjsmål informera Kunden om detta.

10.4 När Kunden är personuppgiftsbiträde åt Slutkund fullgör Preauditor sina skyldigheter enligt punkterna 10.1 och 10.2 gentemot Kunden, som i sin tur ansvarar för att bistå Slutkunden. Om en registrerad, tillsynsmyndighet eller annan tredje man vänder sig direkt till Preauditor i en fråga som rör behandling för en Slutkunds räkning ska Preauditor utan onödigt dröjsmål hänvisa frågan till Kunden, som ansvarar för att involvera Slutkunden, om inte Preauditor är skyldigt att agera enligt lag.

10.5 Preauditor ska på Kundens begäran tillhandahålla sådan teknisk och praktisk assistans som skäligen krävs för att Kunden ska kunna bistå Slutkunden med att besvara en begäran som Slutkunden har mottagit från en registrerad, och ska lämna assistansen utan onödigt dröjsmål och i sådan tid att Slutkunden kan svara inom de frister som följer av GDPR.

10.6 Preauditors bistånd enligt punkt 10.1 omfattar personuppgifter som behandlas i Tjänsten, inklusive uppgifter som hämtats från extern datakälla och lagras där. Preauditor kan däremot inte rätta, radera eller begränsa behandlingen av personuppgifter i register som förs av en extern datakälla i egenskap av självständigt personuppgiftsansvarig, och registrerades rättigheter i förhållande till sådan behandling kan vara begränsade enligt lag. Begäran som avser den behandlingen ska riktas till den externa datakällan, och Preauditor ska på Kundens begäran lämna de uppgifter om datakällan som krävs för att den registrerade ska kunna hänvisas dit.

11. Personuppgiftsincidenter

11.1 Om Preauditor upptäcker en personuppgiftsincident avseende personuppgifter som behandlas för Kundens räkning ska Preauditor utan onödigt dröjsmål underrätta Kunden.

11.2 Underrättelsen ska, i den mån informationen finns tillgänglig vid tidpunkten, innehålla:

- En beskrivning av incidentens art.

- Vilka kategorier av registrerade och personuppgifter som berörs.
- De sannolika konsekvenserna av incidenten.
- Vilka åtgärder som har vidtagits eller planeras för att hantera incidenten och begränsa dess effekter.

11.3 När Kunden är personuppgiftsbiträde åt Slutkund lämnas underrättelse enligt punkt 11.1 till Kunden, som utan onödigt dröjsmål ansvarar för att underrätta berörd Slutkund. Preauditor ska i underrättelsen, i den mån det är möjligt, ange vilka Slutkunder som berörs och ska på Kundens begäran lämna sådan kompletterande information som Slutkunden skäligen behöver för att kunna fullgöra sina skyldigheter enligt artiklarna 33 och 34 GDPR.

12. Revision och information

12.1 Preauditor ska på Kundens begäran tillhandahålla sådan information som skäligen krävs för att visa att Preauditor uppfyller sina skyldigheter enligt detta Biträdesavtal och artikel 28 GDPR. Sådan information kan omfatta beskrivningar av relevanta tekniska och organisatoriska säkerhetsåtgärder, tillämpliga rutiner samt information om eventuella underbiträden i den mån sådan information avser behandling för Kundens räkning.

12.2 Kunden har rätt att kontrollera att Preauditor behandlar personuppgifter för Kundens räkning i enlighet med detta Biträdesavtal och tillämplig dataskyddslagstiftning. Sådan kontroll ska i första hand ske genom information enligt punkt 12.1 och, om detta inte skäligen är tillräckligt, genom annan lämplig verifiering enligt punkt 12.4.

12.3 Om Kundens kontrollbehov inte skäligen kan tillgodoses enligt punkterna 12.1 och 12.4 har Kunden rätt att, själv eller genom oberoende extern granskare som omfattas av sekretess och som inte är konkurrent till Preauditor, genomföra revision av sådan behandling som omfattas av detta Biträdesavtal.

12.4 Preauditor har rätt att i första hand erbjuda annan lämplig verifiering, såsom sammanställningar, ifyllda frågeformulär, intyg, tredjepartsrapporter eller annan dokumentation, om detta skäligen kan tillgodose Kundens behov av kontroll. Om sådan verifiering är tillräcklig med hänsyn till omständigheterna ska den användas i stället för revision på plats.

12.5 Revision ska genomföras högst en gång per tolvmånadersperiod, om inte särskild anledning föreligger, under normal kontorstid, med minst trettio (30) dagars skriftligt varsel

och på ett sätt som inte oskäligt stör Preauditors verksamhet eller röjer information om andra kunder, interna säkerhetsuppgifter utöver vad som skäligen krävs eller annan information som omfattas av sekretess. Revisionen ska vara proportionerlig i förhållande till Kundens kontrollbehov och begränsas till sådan behandling som omfattas av detta Biträdesavtal. Parterna ska i god tid samråda om revisionens praktiska genomförande, omfattning och metod. Kunden står för sina egna kostnader för revision enligt punkt 12.3 och ska ersätta Preauditor för skäliga kostnader för den tid och de resurser som revisionen kräver från Preauditor. Information enligt punkt 12.1 tillhandahålls utan särskild kostnad.

12.6 När Kunden är personuppgiftsbiträde åt Slutkund utövas rätten till information och kontroll enligt denna punkt 12 av Kunden. Slutkundens rätt enligt artikel 28.3 h GDPR att låta granska den behandling som Preauditor utför ska utövas genom Kunden, varvid Kunden har rätt att låta en representant för Slutkunden delta vid Kundens revision enligt punkt 12.3 under förutsättning att representanten omfattas av sekretess, inte är konkurrent till Preauditor och i övrigt uppfyller villkoren i punkterna 12.3 och 12.5. Denna punkt inskränker inte Slutkundens rättigheter eller tillsynsmyndighets befogenheter enligt tvingande dataskyddslagstiftning.

12.7 Begränsningen till en revision per tolvmånadersperiod enligt punkt 12.5 räknas samlat för Kunden och samtliga Slutkunder som Kunden företräder. Kunden ska samordna Slutkundernas kontrollbehov och i första hand tillgodose dem genom sådan information och verifiering som Preauditor tillhandahåller enligt punkterna 12.1 och 12.4.

13. Överföring till tredje land

13.1 Preauditor får endast överföra personuppgifter utanför EU/EES om detta är tillåtet enligt Kundens instruktioner och tillämplig dataskyddslagstiftning.

13.2 Om överföring till tredje land sker ska Preauditor säkerställa att lämpliga skyddsåtgärder finns på plats, såsom adekvansbeslut, standardavtalsklausuler eller annan giltig överföringsmekanism.

13.3 Behandling av personuppgifter i Tjänstens AI-funktioner sker inom EU/EES enligt punkt 7.8. Om Preauditor framöver avser att använda modelleverantör eller datacenterregion utanför EU/EES ska Kunden informeras enligt punkt 9.6 innan ändringen träder i kraft och överföring ske endast med stöd av en giltig överföringsmekanism enligt

punkt 13.2.

13.4 Preauditor ska välja externa datakällor vars inhämtning enligt punkt 7 kan ske utan överföring av personuppgifter till tredje land, och ska, om överföring ändå blir aktuell, säkerställa att punkterna 13.1 och 13.2 iakttas.

13.5 När Kunden är personuppgiftsbiträde åt Slutkund och överföring till tredje land sker ska den överföringsmekanism användas som är tillämplig för överföring från personuppgiftsbiträde till underbiträde. Preauditor ska på Kundens begäran lämna sådan information om överföringen som Kunden behöver för att informera Slutkunden.

13.6 Personuppgifter som behandlas för Kundens räkning lagras i datacenter inom EU/EES, för närvarande i Sverige. Preauditor ska på Kundens begäran informera om var uppgifterna lagras.

14. Radering och återlämning

14.1 När huvudavtalet upphör ska Preauditor, enligt Kundens val och i den mån inte lag kräver annat, återlämna eller radera personuppgifter som behandlats för Kundens räkning. Radering ska ske senast tre (3) månader efter att huvudavtalet upphört, i enlighet med huvudavtalet.

14.2 Preauditor får dock behålla personuppgifter i den utsträckning det krävs enligt lag, myndighetsbeslut, intern backup-rutin eller för att fastställa, göra gällande eller försvara rättsliga anspråk.

14.3 Redan delade rapporter eller sammanställningar som gjorts tillgängliga för revisorn eller annan mottagare på Kundens instruktion omfattas inte av Preauditors skyldighet att radera hos mottagaren.

14.4 Instruktion om återlämning eller radering enligt punkt 14.1 lämnas av Kunden. När Kunden är personuppgiftsbiträde åt Slutkund ansvarar Kunden för att inhämta Slutkundens ställningstagande innan instruktion lämnas, och Preauditor har rätt att förlita sig på att Kundens instruktion återspeglar Slutkundens vilja, om inte annat följer av punkt 5.10.

14.5 Om Kundens uppdrag för en Slutkund upphör medan huvudavtalet består ska Kunden instruera Preauditor om huruvida Slutkundens data ska återlämnas, raderas eller föras över till ett konto som Slutkunden eller en av Slutkunden anvisad ny uppdragstagare förfogar över. Överföring till nytt konto förutsätter att Slutkunden eller den nya uppdragstagaren ingår avtal med Preauditor. Om Kunden inte lämnar instruktion inom trettio (30) dagar från Preauditors begäran, eller om Kunden och Slutkunden lämnar Preauditor motstridiga besked, har Preauditor rätt att begränsa behandlingen till lagring i avvaktan på att frågan klarläggs, dock längst i tre (3) månader, varefter uppgifterna raderas eller återlämnas i enlighet med punkterna 14.1 och 14.2. Om Slutkunden har framställt begäran eller invändning enligt punkt 5.10 begränsas i stället behandlingen till lagring till dess begäran har verkställts eller Slutkunden lämnat instruktion om radering, dock längst tolv (12) månader, varefter uppgifterna raderas om inte lag, myndighetsbeslut eller domstolsavgörande kräver annat.

15. Ansvar

15.1 Parternas ansvar enligt detta Biträdesavtal ska bedömas i enlighet med GDPR och övrig tillämplig dataskyddslagstiftning.

15.2 Ingen bestämmelse i detta Biträdesavtal ska tolkas som att den inskränker registrerads rättigheter enligt GDPR eller partens ansvar i den utsträckning sådant ansvar följer av tvingande lag.

16. Kontakt och meddelanden

16.1 Meddelanden enligt detta Biträdesavtal ska lämnas skriftligen till de kontaktpersoner som parterna från tid till annan anvisar.

17. Giltighet

17.1 Detta Biträdesavtal träder i kraft när det godkänns av parterna eller när Preauditor börjar behandla personuppgifter för Kundens räkning, om detta inträffar tidigare.

17.2 Biträdesavtalet upphör när Preauditor inte längre behandlar personuppgifter för

Kundens räkning, med undantag för bestämmelser som till sin natur ska fortsätta att gälla därefter.

Bilaga 1. Förteckning över leverantörer

Bilagan förtecknar de leverantörer som används i Tjänsten. Ändringar av underbiträden meddelas enligt punkt 9.6.

Underbiträden som behandlar personuppgifter för Kundens räkning:

- Microsoft Ireland Operations Limited (Microsoft Azure). Drift av Tjänsten, inklusive databaser, dokument, loggar och säkerhetskopior. Plats: Sverige.
- Google Cloud EMEA Limited (Google Cloud Platform, Vertex AI). Inläsning och tolkning av underlag och dokument med AI-modeller enligt punkterna 7.7 - 7.11. Plats: EU/EES.
- Okta, Inc. (Auth0). Inloggning och användarkonton för Auktoriserade Användare. Plats: EU/EES.
- Enable Banking Oy. Hämtning av konton, saldon och transaktioner från Kundens bank när Kunden ansluter banken till Tjänsten. Plats: EU/EES.

Övriga leverantörer och källor i Tjänsten, som inte är underbiträden:

- Intercom. Support, onboarding och meddelanden till Auktoriserade Användare i inloggat läge, som Preauditors egen behandling enligt punkt 9.5. Plats: USA.
- The Intelligence Company AB. Extern datakälla för uppgifter om företag, företrädare, ägare och verkliga huvudmän, som självständigt personuppgiftsansvarig enligt punkt 9.3. Plats: Sverige.
- Partnertjänster, banker och myndigheter som Kunden ansluter, för närvarande bokföringsprogrammen Fortnox, Spiris, Bokio och Accounted, Kundens bank och Skatteverket, enligt punkt 9.10.

De leverantörer som Preauditor använder för sin egen verksamhet, till exempel för kundkontakter, fakturering och webbplatsen, behandlar inte personuppgifter för Kundens räkning och framgår av Preauditors integritetspolicy.