

# Personuppgiftsbiträdesavtal

Uppdaterad den 28 mars 2025

Detta personuppgiftsbiträdesavtal ("PUB-avtal") utgör ett integrerat tillägg till Limes abonnemangsvillkor ("Avtalet") som ingåtts mellan Lime och Kunden, såsom angivna och identifierade i Avtalet. Syftet med detta PUB-avtal är att reglera parternas överenskommelse avseende Behandling av Personuppgifter, i enlighet med kraven i Tillämplig Dataskyddslagstiftning. Alla begrepp som inleds med versal ska ha den betydelse som anges i Avtalet eller PUB-avtalet, beroende på vad som är tillämpligt.

Vid tillhandahållande av Tjänsterna till Kunden enligt Avtalet kan Lime komma att Behandla Personuppgifter för Kundens räkning, vilken parterna är överens om ska regleras under detta PUB-avtal. Lime kommer hädanefter att benämnas som "Personuppgiftsbiträde" och Kunden som "Personuppgiftsansvarig", alternativt som "part" eller gemensamt som "parterna".

1	Definitioner.....	2
2	Behandling av Personuppgifter .....	2
3	Personuppgiftsbiträdets skyldigheter .....	3
4	Den Personuppgiftsansvariges skyldigheter.....	4
5	Säkerhetsåtgärder.....	4
6	Granskning och tillsyn.....	5
7	Stöd till den Personuppgiftsansvarige.....	5
8	Användning av underleverantörer.....	6
9	Överföring av personuppgifter till Tredje Land.....	7
10	Avtalstid.....	8
11	Åtgärder vid PUB-avtalets upphörande.....	8
12	Sekretess.....	9
13	Ändringar och tillägg.....	9
14	Ansvarsskyldighet.....	9
15	Lagval och rättsligt forum.....	10
	Bilaga A – Instruktion för behandling av personuppgifter .....	11
	Bilaga B – Tekniska och organisatoriska säkerhetsåtgärder .....	12

# 1 Definitioner

Utöver de begrepp som definieras i löptext i PUB-avtalet ska följande definitioner ha nedan innebörd.

- 1.1 **Behandling (av Personuppgifter):** Varje åtgärd eller serie av åtgärder som vidtas i fråga om Personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, anpassning eller ändring, sökning, konsultering, användning, överföring, spridning eller annat tillhandahållande, sammanställning eller samkörning, blockering, radering eller förstöring.
- 1.2 **Känsliga personuppgifter:** Ras eller etniskt ursprung, eller politisk, filosofisk eller religiös övertygelse, medlemskap i fackföreningar, att en person är misstänkt, åtalad eller dömd för brott, hälsa, genetiska uppgifter, biometriska uppgifter som används för att entydigt identifiera en person, en persons sexualliv eller sexuell läggning, eller andra känsliga personuppgifter.
- 1.3 **Personuppgifter:** All slags information som rör en identifierad eller identifierbar person (den registrerade).
- 1.4 **Personuppgiftsansvarig:** Fysisk eller juridisk person, myndighet, institution eller annat organ som ensamt eller tillsammans med andra fastslår ändamålen och medlen för Behandling av Personuppgifter.
- 1.5 **Personuppgiftsbiträde:** Fysisk eller juridisk person, myndighet, institution eller annat organ som behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
- 1.6 **Registrerad:** En identifierad eller identifierbar fysisk person. En identifierbar person är någon som kan identifieras, direkt eller indirekt, i synnerhet genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för personens fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.
- 1.7 **Tillämplig Dataskyddslagstiftning:** Europaparlamentet och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG ("GDPR") och nationella lagar som implementerar eller kompletterar GDPR som är tillämpliga på Behandling av Personuppgifter under detta PUB-avtal.
- 1.8 **Tredje Land:** Ett land utanför EU/EES.

## 2 Behandling av Personuppgifter

- 2.1 Personuppgiftsbiträdet ska endast Behandla Personuppgifterna i enlighet med detta PUB-avtal och i enlighet med dokumenterade instruktioner från den Personuppgiftsansvarige, såvida inte Personuppgiftsbiträdet har en skyldighet enligt

EU-rätten (inklusive nationella lagar i dess medlemsstater) att Behandla Personuppgifterna.

- 2.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.
- 2.3 Personuppgiftsbiträdet ska Behandla Personuppgifterna under hela den avtalstid som framgår av Avtalet samt under en begränsad period därefter (se avsnitt 11). **Bilaga A** innehåller information om Behandlingen av Personuppgifter, inklusive i) kategorier av personuppgifter, ii) kategorier av registrerade, iii) Behandlingens art och syfte, iv) plats för Behandling och v) varaktighet av Behandlingen.
- 2.4 Detta PUB-avtal gäller inte för Personuppgifter som har överförts från Tjänsten till en Tredjeparts Programvara (enligt definitionen i Avtalet), eftersom det regleras i Personuppgiftsansvariges separata avtal med den relevanta leverantören av Tredjeparts Programvaran.

### **3 Personuppgiftsbitrådets skyldigheter**

- 3.1 Personuppgiftsbiträdet ska endast utföra Behandlingen i enlighet med PUB-avtalet och instruktioner. För tydlighets skull får Personuppgiftsbiträdet behandla Personuppgifter om en sådan behandling krävs enligt tillämplig lag som gäller för Personuppgiftsbiträdet. Personuppgiftsbiträdet ska informera den Personuppgiftsansvarige om sådana krav om det inte är förbjudet att lämna sådan information med anledning av ett viktigt allmänintresse. Vid Behandling av Personuppgifter enligt PUB-avtalet ska Personuppgiftsbiträdet följa Tillämplig Dataskyddslagstiftning.
- 3.2 Personuppgiftsbiträdet ska säkerställa att samtliga fysiska personer som arbetar under dess ledning och som får tillgång till Personuppgifter följer PUB-avtalet och den Personuppgiftsansvariges instruktioner.
- 3.3 Personuppgiftsbiträdet och dennes personal ska vid Behandlingen iaktta tystnadsplikt och sekretess rörande de Personuppgifter som de får tillgång till enligt detta PUB-avtal. Denna bestämmelse gäller även efter PUB-avtalets upphörande.
- 3.4 Personuppgiftsbiträdet ska vidta de säkerhetsåtgärder som krävs enligt artikel 32 GDPR.
- 3.5 I den mån det är möjligt ska Personuppgiftsbiträdet, genom att vidta lämpliga tekniska och organisatoriska åtgärder, hjälpa den Personuppgiftsansvarige att fullgöra sina skyldigheter gentemot de Registrerade.
- 3.6 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 GDPR fullgörs med beaktande av typen av behandling och den information Personuppgiftsbiträdet har att tillgå.

- 3.7 Personuppgiftsbiträdet ska omedelbart informera den Personuppgiftsansvarige om Personuppgiftsbiträdet anser att den Personuppgiftsansvariges instruktioner är otydliga eller på något sätt strider mot Tillämplig Dataskyddslagstiftning. Personuppgiftsbiträdet ska inte utföra en sådan instruktion förrän den Personuppgiftsansvarige har bekräftat att instruktionen är laglig.

## 4 Den Personuppgiftsansvariges skyldigheter

- 4.1 Den Personuppgiftsansvarige ska vid användningen av de tjänster som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet behandla Personuppgifterna i enlighet med Tillämplig Dataskyddslagstiftning. Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta instruktioner så att Personuppgiftsbiträdet (och dess underleverantörer) kan fullgöra sina åtaganden och skyldigheter enligt PUB-avtalet och om tillämpligt Avtalet.
- 4.2 Den Personuppgiftsansvarige har befogenhet att behandla och lämna ut de Personuppgifter som omfattas av Avtalet till Personuppgiftsbiträdet (inklusive till dennes eventuella underleverantörer).
- 4.3 Den Personuppgiftsansvarige har ensamt ansvar för riktigheten, integriteten, innehålllet, tillförlitligheten och lagligheten i de Personuppgifter som lämnas ut till Personuppgiftsbiträdet. Personuppgiftsbiträdet har inte något ansvar för eventuella följder av att erhålla Personuppgifter visat sig vara felaktiga.
- 4.4 Den Personuppgiftsansvarige har fullgjort sina skyldigheter att lämna obligatorisk information till de Registrerade om Behandling av Personuppgifter och om överlämnande av Personuppgifter till Personuppgiftsbiträdet och dennes Behandling av Personuppgifterna enligt Tillämplig Dataskyddslagstiftning.
- 4.5 Den Personuppgiftsansvarige får vid användningen av de tjänster som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet inte lämna över några Känsliga Personuppgifter till Personuppgiftsbiträdet, såvida det inte uttryckligen överenskommit i skrift.
- 4.6 Den Personuppgiftsansvarige ska utan dröjsmål informera Personuppgiftsbiträdet om det sker en ändring av dennes kontaktperson eller dennes kontaktinformation.

## 5 Säkerhetsåtgärder

Personuppgiftsbiträdet ska implementera adekvata tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Tillämplig Dataskyddslagstiftning för att säkerställa att Behandlingen uppfyller en lämplig säkerhetsnivå (enligt bland annat artikel 32 GDPR) för att skydda sekretess, integritet och tillgänglighet till Personuppgifterna, så som beskrivs i **Bilaga B**. Personuppgiftsbiträdet ska fortlöpande granska sina tekniska och organisatoriska säkerhetsåtgärder och vid behov uppdatera dem i enlighet med Tillämplig Dataskyddslagstiftning.

## 6 Granskning och tillsyn

- 6.1 Personuppgiftsbiträdet ska ge den Personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som följer av PUB-avtalet har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den Personuppgiftsansvarige eller av den Personuppgiftsansvarige utsedd tredje part.
- 6.2 Den Personuppgiftsansvarige får granska Personuppgiftsbiträdes efterlevnad av PUB-avtalet upp till en (1) gång per år. Om Tillämplig Dataskyddslagstiftning kräver det kan den Personuppgiftsansvarige kräva granskningar oftare.
- 6.3 För att begära en granskning ska den Personuppgiftsansvarige minst fyra veckor före den föreslagna granskningen lämna in en detaljerad granskningsplan till Personuppgiftsbiträdet där omfattning, varaktighet och föreslaget startdatum för granskningen redovisas. Om granskningen ska utföras av tredje part måste detta som huvudregel avtalas mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet. Om behandling sker i en miljö med Personuppgifter härrörande från andra personuppgiftsansvariga eller liknande, kan Personuppgiftsbiträdet, efter eget gottfinnande, på grund av säkerhetsskäl besluta att revision ska utföras av ett allmänt väl ansett granskningsföretag som Personuppgiftsbiträdet väljer.
- 6.4 Om den begärda granskningen redan utförts och redovisats i en rapport enligt ISAE 3402, ISO eller liknande av en kvalificerad tredjepartsgranskare under de senaste tolv månaderna, och Personuppgiftsbiträdet bekräftar att de granskade kontrollerna inte väsentligt förändrats, ska den Personuppgiftsansvarige godta dessa resultat i stället för att begära en granskning av de kontroller som omfattas av rapporten.
- 6.5 Granskningen ska utföras under anläggningens normala kontorstider enligt Personuppgiftsbiträdets policyer och får inte på ett oskäligt sätt störa Personuppgiftsbiträdes verksamhet.
- 6.6 Den Personuppgiftsansvarige är ansvarig för alla kostnader som uppkommer i samband med av den Personuppgiftsansvariges begärda granskningen och Personuppgiftsbiträdets assistans i detta avseende.
- 6.7 Personuppgiftsbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning. Personuppgiftsbiträdet och dess personal ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter.

## 7 Stöd till den Personuppgiftsansvarige

- 7.1 Med beaktande av Behandlingens art och i den mån det är möjligt ska Personuppgiftsbiträdet bistå den Personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder så att den Personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter.

- 7.2 I den mån det är praktiskt möjligt och lagligt ska Personuppgiftsbiträdet meddela den Personuppgiftsansvarige om (i) begäran om utlämnande av Personuppgifter som erhållits från en Registrerad utom då den Personuppgiftsansvarige godkänt Personuppgiftsbiträdet att svara på en sådan förfrågan, och (ii) begäran om utlämnande av Personuppgifter av myndigheter utom då den Personuppgiftsansvarige godkänt Personuppgiftsbiträdet att svara på en sådan förfrågan.
- 7.3 Emellertid kan Personuppgiftsbiträdet vara förhindrad att meddela den Personuppgiftsansvarige p.g.a. förundersökningssekretess vid en brottsbekämpande utredning. Personuppgiftsbiträdet ska inte lämna ut information om detta PUB-avtal till myndigheter vad avser Personuppgifter, förutom då det är tvingande enligt lag, eller med stöd av domstolsbeslut, order om husrannsakan eller liknande.
- 7.4 Med beaktande av Behandlingens art och den information som finns tillgänglig för Personuppgiftsbiträdet ska Personuppgiftsbiträdet bistå den Personuppgiftsansvarige med att tillse att skyldigheterna enligt Tillämplig Dataskyddslagstiftning fullgörs, inklusive (om tillämpligt) den Personuppgiftsansvariges skyldighet att i) vidta lämpliga tekniska och organisatoriska åtgärder, ii) anmäla personuppgiftsincidenter till tillsynsmyndigheten, iii) informera Registrerade om Personuppgiftsincidenter, iv) genomföra konsekvensbedömningar avseende dataskydd, och v) samråda med tillsynsmyndigheten före Behandling.
- 7.5 Personuppgiftsbiträdet ska utan onödigt dröjsmål och skriftligen meddela den Personuppgiftsansvarige om att Personuppgiftsbiträdet har fått vetskap om en personuppgiftsincident. Personuppgiftsbiträdet ska tillhandahålla Personuppgiftsansvarig en beskrivning av personuppgiftsincidenten. För det fall Personuppgiftsbiträdet inte förfogar över all relevant information om personuppgiftsincidenten vid Personuppgiftsbitrådets första meddelande om inträffad personuppgiftsincident får Personuppgiftsbiträdet tillhandahålla sådan information i omgångar.
- 7.6 Personuppgiftsbiträdet har rätt att debitera den Personuppgiftsansvarige för nedlagt arbete och rimliga kostnader som uppkommit i samband med Personuppgiftsbitrådets stöd enligt ovan och enligt Tillämplig Dataskyddslagstiftning, med undantag för fullgörande av skyldigheter enligt punkt 7.5 ovan då Personuppgiftsincidenten inte beror på den Personuppgiftsansvarige. Detta innefattar t.ex. arbete och kostnader som uppkommit på grund av att Registrerade har begärt registerutdrag avseende Behandlingen av den Registrerades Personuppgifter, radering av Personuppgifter, överföring av Personuppgifter (portabilitet) eller lämnande av obligatorisk information till de Registrerade.

## 8 Användning av underleverantörer

- 8.1 Som en del av leveransen av de tjänster som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet till den Personuppgiftsansvarige får Personuppgiftsbiträdet härmed ett

allmänt skriftligt förhandstillstånd att använda sig av underleverantörer för behandling av Personuppgifter för den Personuppgiftsansvariges räkning.

- 8.2 Personuppgiftsbiträdet ska tillse att samtliga underleverantörer är bundna av skriftliga avtal som säkerställer att underleverantören åläggs skyldigheter i fråga om Behandling av Personuppgifter som minst motsvarar de skyldigheter som fastställs i detta PUB-avtal.
- 8.3 Om underleverantören inte fullgör sina skyldigheter i enlighet med Tillämplig Dataskyddslagstiftning ska Personuppgiftsbiträdet vara fullt ansvarig gentemot den Personuppgiftsansvarige för utförandet av underleverantörens skyldigheter.
- 8.4 Personuppgiftsbiträdet ska tillgängliggöra en uppdaterad och aktuell lista av underleverantörer som används för att utföra de tjänster som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet. Listan ska innehålla information om identiteten på underleverantörerna, kontaktperson hos underleverantören, var Personuppgifterna behandlas och en allmän beskrivning av vilken typ av tjänst respektive underleverantör tillhandahåller. Underleverantörslistan är tillgänglig på Limes hemsida <https://www.lime-technologies.com/subprocessors/>. Genom att underteckna detta PUB-avtal godkänner den Personuppgiftsansvarige Personuppgiftsbitrådets användning av de listade underleverantörerna.
- 8.5 Personuppgiftsbiträdet ska meddela den Personuppgiftsansvarige om planer på att anlita en ny eller ersätta en befintlig underleverantör. Personuppgiftsansvarige får invända mot sådana ändringar. Om ingen invändning görs inom tio (10) dagar från att meddelandet har mottagits antas Personuppgiftsansvarige inte ha gjort någon invändning.
- 8.6 Personuppgiftsbiträdet har rätt att vidta lämpliga korrigerande åtgärder vid en sådan invändning. Om Personuppgiftsansvarige finner att inga korrigerande åtgärder finns eller om invändningen inte har avhjälpats inom trettio (30) dagar har Parterna rätt att genom skriftligt meddelande säga upp PUB-avtalet. Även Avtalet får sägas upp om PUB-avtalet är nödvändigt för att Personuppgiftsbiträdet ska kunna utföra sina skyldigheter enligt Avtalet.

## **9 Överföring av personuppgifter till Tredje Land**

- 9.1 Personuppgiftsbiträdet och dess underleverantörer får överföra Personuppgifter till ett Tredje Land i den mån det är nödvändigt för att utföra de tjänster som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet och under förutsättning att överföringen sker i enlighet med kapitel V GDPR.
- 9.2 Vid användning av standardavtalsklausuler (Kommissionens genomförandebeslut (EU) 2021/91 av den 4 juni 2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679, eller beslut och standardavtalsklausuler som ersätter dessa)

har Personuppgiftsbiträdet eller underleverantören rätt att efter eget bestämmande avgöra vilken version och vilka moduler av standardavtalsklausulerna som är tillämpliga i det enskilda fallet.

- 9.3 I enlighet med de krav som ställs enligt Tillämplig Dataskyddslagstiftning på överföringar som baseras på att lämpliga skyddsåtgärder vidtas ska Personuppgiftsbiträdet i varje enskilt fall genomföra en riskbedömning för att säkerställa att lagstiftning i det aktuella Tredje Landet inte negativt påverkar effektiviteten av de lämpliga skyddsåtgärderna samt att det finns effektiva rättsmedel för Registrerade. Om nödvändigt ska Personuppgiftsbiträdet identifiera och implementera ytterligare skyddsåtgärder, t.ex. tekniska, organisatoriska eller avtalsrättsliga åtgärder, för att säkerställa att skyddsnivån i det aktuella Tredje Landet är väsentligen likvärdig med skyddsnivån inom EU/EES.
- 9.4 På den Personuppgiftsansvariges rimliga förfrågan ska Personuppgiftsbiträdet redogöra för den information som riskbedömningen baseras på. Den Personuppgiftsansvarige har rätt att skriftligen invända mot Personuppgiftsbitrådets riskbedömningar om de ändras efter PUB-avtalets ikraftträdande och den Personuppgiftsansvarige bedömer att de nya riskbedömningarna inte uppfyller de krav som ställs på den Personuppgiftsansvariges Behandling av Personuppgifter enligt Tillämplig Dataskyddslagstiftning. Den Personuppgiftsansvarige har rätt att begära att Personuppgiftsbiträdet vidtar lämpliga korrigerande åtgärder. Om parterna inte kommer överens om riskbedömningen och/eller lämpliga korrigerande åtgärder inom trettio (30) dagar har Parterna rätt att genom skriftligt meddelande säga upp PUB-avtalet. Även Avtalet får sägas upp om PUB-avtalet är nödvändigt för att Personuppgiftsbiträdet ska kunna utföra sina skyldigheter enligt Avtalet.
- 9.5 För det fall EU-domstolen, EU-kommissionen eller någon annan behörig EU-institution eller nationell domstol eller myndighet skulle finna överföringsmekanismen som används för överföringen till Tredje Land är ogiltig eller olaglig ska Personuppgiftsbiträdet säkerställa att all Behandling av Personuppgifter i ett Tredje Land baseras på en annan (giltig) överföringsmekanism.

## 10 Avtalstid

- 10.1 Detta PUB-avtal är giltigt så länge Personuppgiftsbiträde behandlar Personuppgifter för den Personuppgiftsansvariges räkning enligt Avtalet.
- 10.2 Detta PUB-avtal upphör att gälla per automatik då Avtalet avslutas.

## 11 Åtgärder vid PUB-avtalets upphörande

- 11.1 Vid upphörandet av detta PUB-avtal ska Personuppgiftsbiträdet, beroende på vad den Personuppgiftsansvarige skriftligen meddelar Personuppgiftsbiträdet, radera eller återlämna samtliga Personuppgifter som Behandlats för den Personuppgiftsansvariges räkning enligt PUB-avtalet samt alla kopior av uppgifterna,

såvida inte lagring av Personuppgifterna krävs enligt Tillämplig Dataskyddslagstiftning.

- 11.2 Om den Personuppgiftsansvarige inte lämnar någon instruktion eller inte svarar på Personuppgiftsbiträdets begäran om instruktion trettio (30) dagar efter PUB-avtalets upphörande får Personuppgiftsbiträdet välja att återlämna samtliga Personuppgifter till den Personuppgiftsansvarige och/eller radera personuppgifterna.

## 12 Sekretess

Personuppgiftsbiträdet ska inte, under avtalstiden och därefter, lämna upplysningar om Behandling av Personuppgifter som sker enligt detta PUB-avtal till tredje part eller på annat sätt avslöja information som mottagits till följd av PUB-avtalet. Sekretessskyldigheten gäller inte information som Personuppgiftsbiträdet är skyldig att lämna till myndigheter. Utöver detta avsnitt 12 ska sekretessåtagandena i Avtalet också vara tillämpliga.

## 13 Ändringar och tillägg

- 13.1 Ändringar i detta PUB-avtal kan ske på grund av förändrad lagstiftning, förändrade säkerhetskrav eller ändrade praktiska omständigheter i övrigt. I händelse av att en ändring påverkar Behandlingen av Personuppgifter enligt detta PUB-avtal, ska den andra parten meddelas per email till dennes kontaktperson enligt ovan. Sådant meddelande om ändring ska anses som accepterat av den andra parten, såtillvida den andra parten inte gjort rimliga invändningar skriftligen senast trettio (30) dagar från dagen för tillkännagivandet.
- 13.2 Om behörig domstol, myndighet eller skiljenämnd skulle finna att någon bestämmelse i detta PUB-avtal är icke-verkställbar eller ogiltig, påverkas inte övriga bestämmelser. Parterna skall härtill ersätta den icke-verkställbara eller ogiltiga bestämmelsen med en lagenlig bestämmelse som återspeglar syftet med den icke-verkställbara eller ogiltiga bestämmelsen.

## 14 Ansvarsskyldighet

- 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 Tillämplig Dataskyddslagstiftning, ska artikel i 82 i GDPR tillämpas.
- 14.2 Sanktionsavgifter enligt artikel 83 i GDPR, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.
- 14.3 Utan att begränsa skyldigheterna under 14.1 och 14.2, ska det kontraktsrättsliga ansvaret i Avtalet även gälla för detta PUB-avtalet.

14.4 Om någon av parterna får kännedom om omständighet som kan leda till skada för den andra parten ska parten omedelbart informera den andra parten om förhållandet och aktivt arbeta tillsammans med den andra parten för att förhindra och minimera sådan skada.

## **15 Lagval och rättsligt forum**

15.1 Detta PUB-avtal ska tolkas och tillämpas i enlighet med bestämmelser om lagval i Avtalet.

15.2 Tvist som uppstår i anledning av PUB-avtalet ska slutligt avgöras i enlighet med bestämmelser om tvistelösning i Avtalet.

\*\*\*

## Bilaga A – Instruktion för behandling av personuppgifter

<b>Kategorier av personuppgifter</b>	<p>Den Personuppgiftsansvarige kan föra in Personuppgifter i den tjänst som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet. Vilka Personuppgifter som förs in i tjänsten är helt upp till den Personuppgiftsansvarige och kan t.ex. inkludera följande kategorier av Personuppgifter:</p> <ul style="list-style-type: none"> <li>- Namn.</li> <li>- Telefonnummer.</li> <li>- E-postadress.</li> <li>- Kundhistorik.</li> </ul>
<b>Kategorier av Registrerade</b>	<p>Den Personuppgiftsansvarige kan föra in Personuppgifter i den tjänst som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet. Vilka Personuppgifter som förs in i tjänsten är helt upp till den Personuppgiftsansvarige och kan t.ex. inkludera personuppgifter som berör följande kategorier av registrerade:</p> <ul style="list-style-type: none"> <li>- Den personuppgiftsansvariges anställda, kunder, leverantörer och konsulter.</li> <li>- Den Personuppgiftsansvariges potentiella kunders anställda.</li> </ul>
<b>Behandlingens art och syfte</b>	<p>Behandling av Personuppgifter för att tillhandahålla de tjänster som tillhandahålls av Personuppgiftsbiträdet enligt Avtalet och i enlighet med Personuppgiftsansvariges instruktioner.</p>
<b>Plats för Behandling</b>	<ul style="list-style-type: none"> <li>- Personuppgiftsbiträdet Behandlar Personuppgifterna inom EU/EES.</li> <li>- För underleverantörers Behandling, se underleverantörslistan.</li> </ul>
<b>Varaktighet av behandlingen</b>	<p>Behandling av Personuppgifter kommer att ske under Avtalets giltighetstid och för en begränsad period därefter i enlighet med PUB-avtalet. Personuppgiftsbiträdet ska samarbeta med den Personuppgiftsansvarige för att bestämma hur länge Personuppgifterna ska lagras hos den Personuppgiftsansvarige.</p>

## Bilaga B – Tekniska och organisatoriska säkerhetsåtgärder

Lime ska implementera och upprätthålla följande säkerhetsåtgärder:

<b>Informationssäkerhetshanteringssystem (ISMS)</b>	Lime upprätthåller ett ISMS som är i linje med ISO 27001 och täcker viktiga delar av verksamheten. Säkerhetspolicys och rutiner – inklusive riskhantering, incidenthantering, kontinuitetsplanering och säkerhet i leveranskedjan – granskas regelbundet och är föremål för interna och externa revisioner.
<b>Organisatorisk säkerhet och styrning</b>	Lime har en utsedd säkerhetsansvarig och en etablerad struktur för att övervaka säkerhetsarbetet. Anställda måste genomföra obligatorisk säkerhetsutbildning vid anställningens start och årligen därefter.
<b>Behörighetskontroller</b>	Behörighet till system och data beviljas enligt principen om minsta privilegium och baserat på arbetsrollens krav. Åtkomstbegäran måste godkännas av systemägare och behörigheter granskas regelbundet. Single Sign-On (SSO) och Multifaktorautentisering (MFA) är obligatoriskt för nyckelsystem.
<b>Lösenordshantering</b>	Lime kräver en minsta lösenordslängd på åtta (8) tecken med specificerade komplexitetskrav. Lösenord får inte återanvändas eller lagras i klartext. Delade inloggningsuppgifter är inte tillåtna.
<b>Systemövervakning och loggning</b>	Lime loggar åtkomst och systemaktivitet i centrala tjänster. Aviseringar och automatiska utlösare är konfigurerade för att upptäcka avvikelser eller misstänkt beteende som stöd för incidentdetektion och analys.
<b>Incidenthantering</b>	Lime har en dokumenterad och testad incidenthanteringsplan. Alla incidenter klassificeras efter allvarlighetsgrad och hanteras av relevanta team. Kunder informeras utan onödigt dröjsmål om en incident påverkar deras data.
<b>Säkerhetskopiering, kontinuitet och katastrofåterställning</b>	Lime upprätthåller kontinuitets- och katastrofåterställningsplaner för kritiska system. Dagliga, oföränderliga säkerhetskopior behålls i upp till 90 dagar (kan förlängas till maximalt 365 dagar).
<b>Enhets- och endpoint-säkerhet</b>	Organisationens enheter hanteras centralt och är konfigurerade med kryptering, antivirusprogram och brandväggar. Endast

	kompatibla enheter får ansluta till Limes tjänster.
<b>Leverantörssäkerhet</b>	Lime bedömer leverantörer vid onboarding och genom återkommande granskningar. Leverantörer med åtkomst till Limes data eller system måste uppfylla definierade säkerhets- och efterlevnadskrav.
<b>Molnsäkerhet och datahosting</b>	Lime CRM (SaaS) är hostat på Amazon Web Services (AWS), som upprätthåller branschledande fysiska och miljömässiga kontroller samt innehar flera säkerhetscertifieringar. Data krypteras under överföring med TLS 1.2/1.3 och i vila med AES-256-kryptering.
<b>Säkra utvecklingsmetoder</b>	Lime följer en säker mjukvaruutvecklingslivscykel (software development lifecycle, SDLC) som inkluderar riskbedömningar, kodgranskningar, sårbarhetsskanning samt separering av utvecklings-, test- och produktionsmiljöer. Utvecklare utbildas i säkra kodningsmetoder, inklusive kännedom om OWASP Top 10.
<b>Penetrationstester</b>	Limes molntjänster genomgår årliga penetrationstester av oberoende tredje part.
<b>Loggning och revisionsspår</b>	Viktiga händelser i Limes molntjänster och stödinфраstruktur loggas, inklusive åtkomst och ändringar av data. Kunder kan begära utdrag av loggar för utredningar.
<b>Identitets- och åtkomsthantering</b>	Autentisering till Lime CRM stöder Single Sign-On (SSO) via Microsoft Entra ID eller andra OIDC-leverantörer, med stöd för MFA beroende på den externa identitetsleverantören.
<b>Produktsäkerhet och patch-hantering</b>	Lime uppdaterar regelbundet sina molntjänster regelbundet med säkerhetspatchar och förbättringar. Automatiserade verktyg används för att hantera beroenden och identifiera kända sårbarheter.