Personuppgiftsbiträdesavtal

Detta personuppgiftsbiträdesavtal (“Avtal”) har ingåtts den [åååå/mm/dd] (“Avtalsdagen”) mellan: Automile AB, 556775-5698, Box 190, SE 101 23 Stockholm, Sverige (“Automile”) och (“Personuppgiftsansvarig”):
[Kund]
[XXXXXX-XXXX]
[Postadress, Postnummer, Postort]
Detta Avtal är ett tillägg till gällande tjänsteavtal mellan Personuppgiftsansvarig och Automile, (“Tjänsteavtalet”), som avser Personuppgiftsansvariges användning av den tjänst som tillhandahålls av Automile (“Tjänsten”).

Parterna har avtalat om följande.

1. Definitioner

1.1 Begrepp som används i detta personuppgiftsbiträdesavtal (”PUB-avtalet”) ska, utöver vad som anges i övrigt, ha den innebörd som framgår nedan:

a) ”Avtalet”: avser det ramavtal som Automile och den personuppgiftsansvarige ingått [ange datum] avseende tillhandahållande av tjänster och funktioner som omfattas av detta PUB-avtal.
b) ”GDPR”: avser Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
c) ”Personuppgifterna”: avser de personuppgifter som Automile, i egenskap av personuppgiftsbiträde, behandlar för den personuppgiftsansvariges räkning i enlighet med detta PUB-avtal.
d) ”Personuppgiftsansvarig”: avser den eller de juridiska personer som är personuppgiftsansvariga för Automiles behandling av personuppgifterna enligt detta PUB-avtal.
e) ”Tillämplig dataskyddslagstiftning”: avser all lagstiftning som vid var tid är tillämplig på behandlingen av personuppgifterna enligt detta PUB-avtal, innefattande men inte begränsat till GDPR, nationella lagar, förordningar och föreskrifter som kompletterar GDPR, samt bindande beslut, rekommendationer, vägledningar och liknande som utfärdats av behöriga tillsynsmyndigheter.
f) ”Underbiträde(n)”: avser varje underleverantör eller annat personuppgiftsbiträde som anlitas av Automile för att utföra specifik behandling av personuppgifterna i enlighet med detta PUB-avtal.
g) ”Tredjeland”: avser land utanför Europeiska unionen (EU) eller Europeiska ekonomiska samarbetsområdet (EES).

1.2 I övrigt ska begrepp som används i detta PUB-avtal ha den innebörd som följer av tillämplig dataskyddslagstiftning.

2. Instruktioner för behandling av personuppgifter.

2.1. Automile får endast behandla personuppgifterna i enlighet med de dokumenterade instruktioner som den Personuppgiftsansvarige lämnar, såvida inte annan behandling krävs enligt tillämplig lag. I sådant fall ska Automile informera den Personuppgiftsansvarige om den rättsliga grunden för behandlingen, om inte sådan information är förbjuden enligt lag. Automile åtar sig att

utföra behandlingen i enlighet med tillämplig dataskyddslagstiftning, detta avtal och PUB-avtalet, och ska därför hålla sig informerad om gällande dataskyddsregler.

Parterna är överens om att detta PUB-avtal tillsammans med Bilaga 1 utgör den Personuppgiftsansvariges fullständiga och slutliga instruktioner till Automile avseende behandling av personuppgifter. Bilaga 1 utgör en integrerad del av avtalet och anger, i enlighet med tillämplig dataskyddslagstiftning, behandlingens föremål, varaktighet, art och ändamål, typer av personuppgifter samt kategorier av registrerade.

Om den Personuppgiftsansvarige lämnar särskilda instruktioner som går utöver vad som följer av tillämplig dataskyddslagstiftning, ska den Personuppgiftsansvarige bära eventuella merkostnader som följer därav.

Den Personuppgiftsansvarige har rätt att säga upp detta PUB-avtal om Automile vägrar att följa instruktioner från den Personuppgiftsansvarige som går utöver vad som omfattas av avtalet.

Automile ska säkerställa att dess anställda och andra personer som arbetar under Automiles överinseende och som har tillgång till personuppgifter endast behandlar dessa i enlighet med den Personuppgiftsansvariges dokumenterade instruktioner, Bilaga 1 samt detta PUB-avtal. Automile ska vidare säkerställa att sådana personer har åtagit sig sekretess eller omfattas av lagstadgad tystnadsplikt, är informerade om sina skyldigheter enligt PUB-avtalet och har genomgått adekvat utbildning i tillämplig dataskyddslagstiftning.

2.2 Automile ska, på begäran och i skälig omfattning, bistå den Personuppgiftsansvarige med att uppfylla sina skyldigheter enligt gällande dataskyddslagstiftning, inklusive dataskyddsförordningen (GDPR).

Detta innefattar att Automile aktivt ska stödja den Personuppgiftsansvarige i att säkerställa att registrerade kan utöva sina rättigheter enligt GDPR. Dessa rättigheter kan omfatta, men är inte begränsade till, rätt till information, tillgång till personuppgifter, rättelse, radering, dataportabilitet, begränsning av behandling och invändning mot viss behandling.

Automile ska tillhandahålla relevant information samt vidta de tekniska och organisatoriska åtgärder som krävs för att möjliggöra detta, inom de tidsramar och på det sätt som föreskrivs i tillämplig dataskyddslagstiftning. Om personuppgifter behandlas av underbiträden, ska Automile i förekommande fall vidarebefordra sådana begäranden till dessa.

2.3 Sekretess. Parterna förbinder sig att inte röja personuppgifter eller annan konfidentiell information till tredje man, annat än i den utsträckning detta krävs enligt tillämplig lag, en lagakraftvunnen dom eller ett bindande myndighetsbeslut.

Om domstol eller myndighet begär utlämnande av personuppgifter eller annan konfidentiell information, ska den part som mottagit begäran – i den mån det är möjligt och förenligt med lag – i första hand hänvisa myndigheten till den andra parten. För detta syfte får den mottagande parten lämna ut den andra partens kontaktuppgifter till myndigheten.

Om en part är skyldig att lämna ut personuppgifter eller annan konfidentiell information till en myndighet, ska parten – om det är förenligt med lag – utan dröjsmål underrätta den andra parten i förväg, så att denna ges möjlighet att vidta nödvändiga eller lämpliga åtgärder.

2.4 Överföring till tredje land.

Automile får endast överföra Personuppgifter till länder utanför EU/EES (s.k. tredjeland) om sådan överföring sker i enlighet med tillämplig dataskyddslagstiftning, inklusive kapitel V i dataskyddsförordningen (GDPR).
Sådan överföring får endast ske om:
• Europeiska kommissionen har fattat beslut om att tredjelandet säkerställer en adekvat skyddsnivå, eller
• Överföringen omfattas av andra godkända skyddsåtgärder enligt GDPR, såsom ingående av EU-kommissionens standardavtalsklausuler (SCCs) mellan Automile och relevant mottagare i tredjeland.

Automile ska på begäran tillhandahålla den Personuppgiftsansvarige dokumentation som visar att lämpliga skyddsåtgärder har vidtagits för att säkerställa en skyddsnivå som motsvarar den inom EU/EES.

Om en överföring sker med stöd av standardavtalsklausuler eller andra godkända mekanismer, förbinder sig Automile att genomföra eventuella kompletterande tekniska och organisatoriska skyddsåtgärder som krävs för att uppnå en i praktiken likvärdig och adekvat skyddsnivå.

3. Tekniska och organisatoriska säkerhetsåtgärder

3.1 Automile ska som minimum efterleva de krav på tekniska och organisatoriska säkerhetsåtgärder som framgår av Bilaga 3 (Tekniska och organisatoriska säkerhetsåtgärder). Automile ska vidare uppfylla sina skyldigheter i egenskap av personuppgiftsbiträde enligt tillämplig dataskyddslagstiftning, inklusive artikel 32 GDPR.

3.2 Automile ska bistå den Personuppgiftsansvarige med att säkerställa efterlevnad av den Personuppgiftsansvariges skyldigheter enligt artikel 32 GDPR genom att tillhandahålla information om de tekniska och organisatoriska åtgärder som Automile har vidtagit samt den ytterligare information som Automile har tillgång till och som krävs för att den Personuppgiftsansvarige ska kunna uppfylla sina skyldigheter.

3.3 Om Personuppgiftsansvarig önskar att Automile ska vidta ytterligare tekniska- och organisatoriska säkerhetsåtgärder, så kommer Automile göra det i skälig utsträckning, mot ersättning från Personuppgiftsansvarig för alla eventuellt tillkommande kostnader.

4. Personuppgiftsansvariges allmänna skyldigheter

4.1 Den Personuppgiftsansvarige ska lämna Automile dokumenterade instruktioner för Automiles behandling av personuppgifterna. Den Personuppgiftsansvarige ansvarar vidare för att i övrigt efterleva tillämplig dataskyddslagstiftning i egenskap av personuppgiftsansvarig samt, i förekommande fall, i egenskap av personuppgiftsbiträde.

4.2 I den mån den Personuppgiftsansvarige inte själv är personuppgiftsansvarig för den behandling som Automile anlitas att utföra enligt detta PUB-avtal (d.v.s. i den mån den Personuppgiftsansvarige själv agerar som personuppgiftsbiträde), ska den Personuppgiftsansvarige inhämta och vidarebefordra dokumenterade instruktioner från den faktiska personuppgiftsansvarige.

5. Personuppgiftsbiträdets allmänna skyldigheter

5.1 Ändamål och instruktioner

Automile ska endast behandla personuppgifter för den Personuppgiftsansvariges räkning i den utsträckning som är nödvändig för att tillhandahålla, upprätthålla och förbättra de tjänster som omfattas av avtalet. Automile får inte behandla personuppgifter för egna ändamål eller i större omfattning än vad som följer av den Personuppgiftsansvariges dokumenterade instruktioner, detta PUB-avtal eller tillämplig lag. Automile ska hålla sig informerad om tillämplig dataskyddslagstiftning och fullgöra sina skyldigheter i enlighet med GDPR, avtalet och detta PUB-avtal.

5.2 Information om bristande instruktioner eller olagliga instruktioner
Automile ska utan dröjsmål och skriftligen underrätta den Personuppgiftsansvarige om Automile anser att en instruktion strider mot tillämplig dataskyddslagstiftning eller annan lagstiftning, eller om Automile saknar tillräckliga instruktioner för att kunna fullgöra sina skyldigheter enligt detta personuppgiftsbiträdesavtal.

5.3 Tillgång och användning
Automile ska inte ha tillgång till eller använda personuppgifter i större omfattning än vad som är nödvändigt för att utföra tjänsterna på den Personuppgiftsansvariges uppdrag. Den Personuppgiftsansvarige godkänner att Automile får samla in och använda viss teknisk data, användarstatistik och liknande information i den mån detta är nödvändigt för att göra uppdateringar, tillhandahålla support och leverera tjänster med anknytning till de avtalade tjänsterna. Automile och dess underleverantörer får behandla sådan information för att förbättra tjänsterna och användarupplevelsen, dock alltid i enlighet med tillämplig dataskyddslagstiftning.

5.4 Personal och sekretess
Automile ska säkerställa att dess anställda och andra personer som utför arbete under Automiles överinseende och som har tillgång till personuppgifter endast behandlar dessa i enlighet med den Personuppgiftsansvariges dokumenterade instruktioner, bilagorna till detta PUB-avtal samt avtalet i övrigt. Automile ska vidare säkerställa att personer med behörighet att behandla personuppgifter har åtagit sig att iaktta sekretess eller omfattas av lagstadgad tystnadsplikt, att de är informerade om sina skyldigheter enligt detta PUB-avtal och att de har genomgått adekvat utbildning i tillämplig dataskyddslagstiftning.

5.5 Informationsplikt vid konkurs eller liknande förfarande
Om personuppgifter som Automile behandlar för den Personuppgiftsansvariges räkning skulle komma att omfattas av konkurs, ackord eller liknande förfarande, ska Automile omedelbart skriftligen underrätta den Personuppgiftsansvarige. Automile ska vidare utan dröjsmål informera berörda parter
såsom konkursförvaltare eller borgenärer om att personuppgifterna tillhör den Personuppgiftsansvarige med full förfoganderätt.

5.7 Bistånd till den personuppgiftsansvarige

a) **Bistånd med att säkerställa registrerades rättigheter**
Personuppgiftsbiträdet ska, med beaktande av behandlingens art och den information som biträdet har tillgång till, bistå den personuppgiftsansvarige med att säkerställa att registrerades rättigheter enligt kapitel III i GDPR följs.

b) **Bistånd med säkerhetsåtgärder och incidenthantering**
Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att säkerställa att skyldigheterna enligt artiklarna 32–36 i GDPR uppfylls.

5.8 Register över behandlingsaktiviteter
Automile ska föra ett register över de kategorier av behandlingsaktiviteter som utförs för den Personuppgiftsansvariges räkning. Registret ska åtminstone innehålla den information som krävs enligt artikel 30.2 GDPR. Automile ska på begäran tillhandahålla den Personuppgiftsansvarige eller behörig tillsynsmyndighet en kopia av registret för att visa efterlevnad av tillämplig dataskyddslagstiftning.

5.7 Behandling för att efterleva unionsrätten eller nationell rätt
Automile får, utan dokumenterade instruktioner från den Personuppgiftsansvarige, endast behandla personuppgifter i den utsträckning sådan behandling krävs enligt unionsrätten eller enligt nationell lagstiftning i den medlemsstat som Automile omfattas av. Automile ska i sådant fall, innan behandlingen påbörjas, skriftligen informera den Personuppgiftsansvarige om kravet och ange vilka personuppgifter som ska behandlas, för vilka ändamål samt hänvisa till de relevanta bestämmelserna i den aktuella lagstiftningen. På begäran ska Automile tillhandahålla den ytterligare information som den Personuppgiftsansvarige behöver för att bedöma om behandlingen är förenlig med tillämplig dataskyddslagstiftning.

Automiles skyldighet att informera den Personuppgiftsansvarige gäller dock inte i den mån Automile är förhindrad att lämna sådan information med hänvisning till ett viktigt allmänintresse enligt den lagstiftning som kräver behandlingen av personuppgifterna.

6. Tillsyn och granskning

6.1 Automile ska tillhandahålla den Personuppgiftsansvarige all information som krävs för att visa att Automile uppfyller sina skyldigheter enligt dataskyddsförordningen (GDPR), särskilt artikel 28, samt detta personuppgiftsbiträdesavtal. Automile ska också möjliggöra och aktivt medverka vid granskningar, inklusive platsinspektioner, som utförs av den Personuppgiftsansvarige eller av en extern revisor som utsetts av den Personuppgiftsansvarige. Sådan extern revisor får inte vara konkurrent till Automile.

6.2 Den Personuppgiftsansvarige har rätt att genomföra en revision en gång per kalenderår. Ytterligare revision kan begäras vid särskilda omständigheter, exempelvis vid misstanke om att Automile inte efterlever detta avtal eller vid en personuppgiftsincident.

6.3 Den Personuppgiftsansvarige ska lämna skriftligt meddelande om föreslagen revision minst två (2) veckor i förväg. Revisionen ska genomföras under ordinarie kontorstid och på ett sätt som begränsar störningar i Automiles verksamhet. Resultatet av revisionen ska hållas konfidentiellt och diskuteras gemensamt av parterna.

6.4 Den Personuppgiftsansvarige ska bära samtliga kostnader och utgifter för revisionen.

6.5 Oavsett ovanstående ska den Personuppgiftsansvarige eller dess revisor inte ges tillgång till serverrum eller andra utrymmen eller uppgifter, i den mån detta kan innebära risk för Automiles säkerhetsnivå eller avslöjande av konfidentiell information. Bedömningen av sådan risk görs uteslutande av Automile.

6.6 Konsekvensbedömningar avseende dataskydd och förhandssamråd.
Automile ska, på begäran av den Personuppgiftsansvarige och med beaktande av behandlingens art samt den information Automile har tillgång till, bistå den

Personuppgiftsansvarige med att fullgöra sina skyldigheter att genomföra konsekvensbedömningar avseende dataskydd och att genomföra förhandssamråd med tillsynsmyndigheten i den utsträckning som krävs enligt tillämplig dataskyddslagstiftning.

7. Säkerhetsincident

Om Automile får kännedom om antingen:

(a) en otillåten åtkomst till Personuppgifter som lagras på Automiles utrustning eller i Automiles lokaler, eller
(b) obehörig åtkomst till sådan utrustning eller sådana lokaler, där sådan åtkomst kan leda till förlust, ändring, otillåten tillgång eller röjande av Personuppgifter (var för sig en "Säkerhetsincident"), ska Automile utan onödigt dröjsmål och under alla omständigheter senast inom 72 timmar från det att incidenten upptäckts:

a) Skriftligen underrätta den Personuppgiftsansvarige om Säkerhetsincidenten. Underrättelsen ska minst innehålla följande:
• En beskrivning av incidentens art, inklusive om möjligt kategorier och antal berörda registrerade samt kategorier och antal berörda personuppgifter
• Namn och kontaktuppgifter till kontaktperson hos Automile
• En beskrivning av de sannolika konsekvenserna av Säkerhetsincidenten
• En beskrivning av de åtgärder som har vidtagits eller föreslås vidtas för att hantera incidenten och begränsa dess eventuella negativa effekter

b) Utan dröjsmål vidta alla skäliga tekniska och organisatoriska åtgärder för att begränsa, åtgärda och förebygga ytterligare skada till följd av Säkerhetsincidenten.

c) Tillhandahålla löpande uppdateringar till den Personuppgiftsansvarige om incidentens hantering och utredning, samt samarbeta fullt ut för att möjliggöra den Personuppgiftsansvariges skyldigheter enligt artiklarna 33 och 34 i dataskyddsförordningen.

d) Parterna är överens om att ett enbart försök till Säkerhetsincident inte omfattas av denna punkt. Med försök avses en händelse som inte leder till att någon obehörigen får tillgång till personuppgifter eller till någon av Automiles utrustning och lokaler där personuppgifter lagras. Detta kan till exempel innefatta ping-attacker, portskanning, misslyckade inloggningsförsök, DoS-attacker, packet sniffing eller annan obehörig åtkomst till trafikdata som inte resulterar i tillgång utöver IP-adresser eller headers.

e) Automiles skyldighet att rapportera eller svara på en Säkerhetsincident enligt denna punkt ska inte tolkas som att Automile har åtagit sig ansvar för själva Säkerhetsincidenten.

f) Automile ska meddela en eller flera av den Personuppgiftsansvariges administratörer om att en Säkerhetsincident har inträffat. Sådant besked ska lämnas på det sätt Automile själv väljer, inklusive men inte begränsat till e-post. Den Personuppgiftsansvarige ansvarar för att administratörernas kontaktuppgifter hålls uppdaterade i Automiles hanteringskonsol.

8. Underbiträden

8.1 Rätt att anlita underbiträden

Automile har en allmän rätt att anlita och byta underbiträden för att uppfylla sina avtalsenliga förpliktelser enligt detta PUB-avtal och för att tillhandahålla relaterade tjänster, såsom support och drift. Automile ska hålla en aktuell förteckning över de underbiträden som vid var tid används och vilka typer av tjänster de tillhandahåller. På begäran ska Automile tillhandahålla den Personuppgiftsansvarige sådan information. De underbiträden som Automile använder vid avtalets ingående framgår av bilaga 2.

8.2 Underbiträdenas skyldigheter
Om Automile anlitar ett underbiträde gäller följande:

a) Automile ska begränsa underbiträdets tillgång till personuppgifter till vad som är nödvändigt för att tillhandahålla tjänsterna. Underbiträdet får inte behandla personuppgifterna för något annat ändamål.

b) Automile ska ingå ett skriftligt avtal med underbiträdet genom vilket underbiträdet åläggs minst samma dataskydds- och säkerhetsförpliktelser som gäller för Automile enligt detta PUB-avtal och tillämplig dataskyddslagstiftning, inklusive skyldighet att iaktta sekretess och att möjliggöra tillsyn.

c) Om ett underbiträde brister i fullgörandet av sina skyldigheter avseende personuppgifter ska Automile vara fullt ansvarig gentemot den Personuppgiftsansvarige för underbiträdets handlingar och underlåtenheter.

9. Skadestånd och vite
Parterna är överens om att vardera parten ansvarar för de administrativa sanktionsavgifter, skadestånd och andra sanktioner som åläggs till följd av den partens egen överträdelse av tillämplig dataskyddslagstiftning.

Om den Personuppgiftsansvarige hålls ansvarig gentemot registrerade eller tredje man för en skada som uppkommit till följd av Automiles agerande, ska Automile endast ersätta den Personuppgiftsansvarige i den utsträckning skadan orsakats av Automiles underlåtenhet att fullgöra de skyldigheter som enligt GDPR uttryckligen åligger personuppgiftsbiträden, eller om Automile har agerat utanför eller i strid med den Personuppgiftsansvariges lagliga instruktioner.

Om Automile hålls ansvarigt enligt artikel 82 GDPR för en skada som den Personuppgiftsansvarige ensam bär ansvar för, ska den Personuppgiftsansvarige hålla Automile skadeslöst för sådant ansvar. Automile ansvarar endast för skador som Automile har orsakat genom att bryta mot bestämmelserna i GDPR eller genom att ha agerat utanför eller utöver den Personuppgiftsansvariges lagliga instruktioner.

Parterna bekräftar att denna ansvarsfördelning inte inskränker registrerades rätt till ersättning enligt artikel 82 GDPR, utan enbart reglerar ansvarsfördelningen internt mellan Parterna.

10. Följder av avtalets upphörande
När Automile inte längre behandlar personuppgifter för den Personuppgiftsansvariges räkning, exempelvis till följd av att behandlingen har avslutats, vid uppsägning av Tjänsteavtalet eller när den Personuppgiftsansvarige begär det, ska Automile återlämna alla personuppgifter till den Personuppgiftsansvarige eller till annan part i enlighet med den Personuppgiftsansvariges instruktioner. Den Personuppgiftsansvarige kan även begära att Automile raderar personuppgifterna och skriftligen intygar att detta har skett.

Om Automile är förhindrad att återlämna eller radera personuppgifter enligt tillämplig dataskyddslagstiftning, unionsrätten eller en medlemsstats nationella lagstiftning, ska Automile säkerställa att personuppgifterna förblir konfidentiella och inte behandlas för något annat ändamål än vad som krävs enligt sådan lagstiftning.

11. Fullständig reglering

Detta avtal påverkar inte giltigheten av Tjänsteavtalet, vilket fortsatt ska gälla mellan Parterna. Vid motstridigheter mellan detta PUB-avtal och Tjänsteavtalet ska dock detta PUB-avtal äga företräde.

12. Tillämplig lag och tvistelösning

12.1 PUB-avtalet ska tolkas och tillämpas i enlighet med svensk materiell rätt.

12.2 Tvister med anledning av PUB-avtalet ska avgöras i enlighet med Tjänsteavtalets bestämmelser om tvistlösning. För det fall att Tjänsteavtalet saknar sådana bestämmelser ska tvister med anledning av PUB-avtalet avgöras i svensk domstol med Stockholms tingsrätt som första instans.

13. Kontaktperson för dataskydd

Automile har utsett ett dataskyddsombud (”DPO”) som ansvarar för frågor rörande behandling av personuppgifter och efterlevnad av detta personuppgiftsbiträdesavtal. DPO kan kontaktas via e-post: **dpo@automile.com**.

14. Underskrifter

Detta avtal har upprättats i elektronisk form och undertecknats genom elektronisk signatur. Parterna har erhållit var sitt (1) exemplar, antingen i PDF-format eller i annan elektronisk form, vilka båda ska anses utgöra original. Avtalet anses vara slutet mellan Parterna per dagen för undertecknandet.

_____ _____

Bilaga 1
Personuppgiftsansvariges instruktioner

Ändamål och rättsliga grunder för behandling av personuppgifter
Personuppgifterna kommer att behandlas av Automile endast för uttryckligen angivna, berättigade och dokumenterade ändamål. All behandling sker i enlighet med dataskyddsförordningen (GDPR). Nedan anges respektive ändamål samt den rättsliga grund som stöder behandlingen.

Typ av behandling	Ändamål	Rättslig grund
Tillhandahållande av avtalade tjänster	För att Automile ska kunna uppfylla sina skyldigheter enligt Tjänsteavtalet, inklusive men inte begränsat till elektronisk körjournal, spårning och administration av fordon.	Behandlingen är nödvändig för att fullgöra avtalet med kunden.
Kundsupport och användarhjälp	För att kunna besvara frågor, hantera felanmälningar samt ge teknisk och administrativ support till användare.	Behandlingen är nödvändig för att tillhandahålla support och uppfylla avtalet.
Tekniskt underhåll och driftssäkerhet	För att säkerställa systemens funktion, förebygga och åtgärda tekniska problem samt upprätthålla en hög driftsäkerhet.	Behandlingen grundas på Automiles berättigade intresse av att tillhandahålla en säker och fungerande tjänst.
Informationssäkerhet och skydd mot missbruk	För att upptäcka, förebygga och hantera obehörig användning, intrångsförsök och andra säkerhetsrelaterade incidenter.	Behandlingen grundas på Automiles berättigade intresse av att skydda system, kunder och användare.
Säkerhetskopiering och återställning	För att skydda data mot förlust, säkerställa möjligheten att återskapa information och upprätthålla tjänstens kontinuitet.	Behandlingen grundas på Automiles berättigade intresse av att säkerställa tillförlitliga och kontinuerliga tjänster.
Loggning av programvaruanvändning	För att samla in statistik och analysdata avseende användningen av tjänsten, inklusive vilka funktioner användaren klickar på, klicksekvenser samt information såsom IP-adress. Detta görs i syfte att förbättra tjänsten och användarupplevelsen.	Behandlingen sker med stöd av samtycke.

Kategorier av personuppgifter

Kategori	Uppgifter
Plats- och positioneringsdata	Tidsstämplar, GPS-koordinater, reseuppgifter, höjdangivelser, färdriktning samt annan positioneringsinformation.
Fordonsdata	Registreringsnummer och tillhörande fordonsuppgifter (såsom fabrikat, modell, bränsletyp, chassinummer/VIN, motorstorlek, koldioxidutsläpp), körsträcka samt uppgifter om leasing, försäkring och besiktning.
Användaruppgifter	Användarnamn, användar-ID, namn, telefonnummer, e-postadress, mobiltelefonnummer samt ID-kort/tagg.
Körhändelsedata	Uppgifter om acceleration, inbromsning, kurvtagning, tomgångskörning och hastighetsöverträdelser.

Kategorier av registrerade

Automile kommer att behandla personuppgifter som rör följande kategorier av registrerade:

1) Anställda, konsulter och andra personer som är verksamma inom den personuppgiftsansvariges organisation.
2) Användare av Automiles tjänster, däribland förare och administratörer som nyttjar tjänsten i enlighet med Tjänsteavtalet.
3) Eventuella andra personer vars uppgifter förekommer i samband med användningen av tjänsten, exempelvis kontaktpersoner.

Behandlingsaktiviteter

Automile kommer att utföra följande typer av behandling av personuppgifter:

1) Insamling, registrering och organisering.
2) Lagring och bevarande.
3) Åtkomst, användning och analys.
4) Överföring, utlämnande och tillhandahållande till den personuppgiftsansvarige.
5) Säkerhetskopiering, drift och tekniskt underhåll.
6) Radering eller avidentifiering när personuppgifterna inte längre är nödvändiga.

Plats för behandling av personuppgifter

Personuppgifterna kommer att behandlas i Automiles egna servrar belägna i Fredrikshamn, Finland. Därutöver kan personuppgifter komma att behandlas av underbiträden i andra länder.

1) Inom EU/EES: Behandlingen sker med stöd av att EU:s dataskyddsförordning (GDPR) är direkt tillämplig och en adekvat skyddsnivå därmed föreligger.
2) Utanför EU/EES (tredje land): Överföring sker endast till länder för vilka EU-kommissionen har fattat adekvansbeslut eller, i avsaknad av sådant beslut, med stöd av EU-kommissionens standardavtalsklausuler eller annan tillämplig överföringsmekanism i enlighet med GDPR.

Behandlingens varaktighet

Personuppgifterna kommer att behandlas under den tid Tjänsteavtalet är giltigt samt därefter så länge det är nödvändigt för att fullgöra lagstadgade skyldigheter eller för att tillvarata rättsliga anspråk. Som längst kommer personuppgifterna att bevaras i sju (7) år efter det att Tjänsteavtalet har upphört att gälla.

Bilaga 2
Lista över tillåtna underbiträden vid avtals ingående

Nedan redovisas de underbiträden som är tillåtna enligt avtalet. Tabellen innehåller uppgifter om respektive underbiträde och deras behandling av personuppgifter. För att säkerställa tydlighet för alla parter anges nedan en kort förklaring av varje kolumn i tabellen:

1) **Leverantör** – Namn på den juridiska personen, organisationsnummer (om tillämpligt), adress och kontaktuppgifter för dataskyddsrelaterade frågor.
2) **Behandling** – Övergripande (deskriptiv) beskrivning av den specifika behandling som Underbiträdet ska utföra.
3) **Kategorier av personuppgifter:**– Kategorier av personuppgifter och registrerade som Underbiträdets behandling avser.
4) **Plats** – Geografisk plats för Underbiträdets behandling (t.ex. plats för åtkomst till personuppgifter).
5) **Mekanism** – Överföringsmekanism/adekvansbeslut från Kommissionen som ska tillämpas vid ev. överföring till Tredjeland.
6) **Dokumentation** – Hänvisning till ev. ytterligare dokumentation* och särskilda krav** vid ev. överföring till Tredjeland.

Leverantör	Behandling	Kategorier av personuppgifter:	Plats	Mekanism	Dokumentation
Intercom R&D Unlimited Company (USA)	Intercom används för chatt mellan kunder och vår kundsupport.	Namn, E-post, Mobilnummer	USA	EU–USA Data Privacy Framework	Standardavtalsklausuler (SCC)
Zendesk, Inc (USA)	Zendesk används för e-postkommunikation mellan kunder och vår kundsupport.	Namn, E-post, Mobilnummer	USA	EU–USA Data Privacy Framework	Standardavtalsklausuler (SCC)
FrontApp, Inc (USA)	Front används för e-postkommunikation mellan kunder och vår ekonomiavdelning.	Namn, E-post, Mobilnummer	USA	EU–USA Data Privacy Framework	Standardavtalsklausuler (SCC)
Hubspot Ireland Ltd (Irland)	Hubspot används för e-post, marknadsföring, CRM och kundkommunikation.	Namn, E-post, Mobilnummer	Irland	Ej tillämpligt (Inom EU/EES)	Ej tillämpligt (Inom EU/EES)

* Med ”dokumentation” avses t.ex. hänvisning till Underbiträdets ”privacy notice” (eller motsvarande dokument) där det framgår att behandlingen omfattas av EU-U.S. Data Privacy Framework-certifiering.

** Med ”särskilda krav” avses t.ex. sådana kompletterande skyddsåtgärder som beskrivs i EDPB:s rekommendationer 01/2020.

Bilaga 3
General Technical and Organizational Measures

Purpose and background
Under Article 32 (1) of the GDPR, the Processor shall implement appropriate technical and organizational measures to ensure a level of security proportionate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing. These measures shall be designed to protect the rights and freedoms of natural persons, taking into account the risks of varying likelihood and severity,including the risk of a Personal Data Breach.

ABAX Group (the processor) and its suppliers (sub-processors) guarantee a level of security no lower than what is set out in the technical and organizational measures (TOM) below.

The technical and organizational measures (TOMs) provided below apply to all standard service offerings offered by ABAX Group.

Technical & Organizational measures
Employee confidentiality
We protect our customers' data confidentiality by ensuring that all employees and external consultants sign confidentiality agreements upon starting their engagement.

Information security control protocols
We build our information security controls based on ISO 27001:2022 and have maintained ISO 27001 certification since 2012.

Physical access
We host our product infrastructure with outsourced infrastructure providers and do not own hardware located in their data centers. All production infrastructure is logically and physically secured from our internal corporate IT systems. Our infrastructure providers' physical and environmental security controls are all audited for well-known standards like SOC 2 Type II and ISO 27001 compliance.
Our offices are all secured with physical access control and visitor management provided by us or the facility owner.

Remote access
When our product infrastructure is accessed from remote locations by our employees, all communication is encrypted using industry-standard TLS encryption, and access is controlled through a centralized identity provider (IdP) with strong authentication. All employee devices used to access our environments are centrally managed and protected by standardized security software with endpoint detection and management (EDR) functionality.

Product/services access
All our standard service offerings provide strong authentication, enabling the logical separation of data between customers based on the implemented authorization scheme. Authentication is either provided by our identity platform or by a third-party identity provider through single sign-on (SSO).

If our employees require access to our customers' data, it is granted on a per-need basis and only to a limited group of personnel.

Perimeter, network, host, and application disclosure control
We implement the following technical protections to ensure that the confidentiality of customer data is protected during processing, transmission, and storage:

a) Firewalls protecting the perimeter
b) Protections against Distributed Denial of Services (DDoS) attacks
c) Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
d) Vulnerability management via vulnerability scanning
e) Cloud security posture management through automated CSPM tooling
f) Applicable security patches are applied based on criticality
g) Logically separated networks for development, testing, and production
h) Anti-virus/anti-malware protection via endpoint detection and response tools (EDR)

Personnel training
As part of our onboarding process, all employees receive training on information security and privacy. We maintain competency with recurring mandatory training for all personnel on information security and privacy (GDPR) through nano-learning courses.

Encryption
We use industry-standard TLS encryption for communication between customer devices and our products and services. When data is transported between our locations or across services, we use encrypted communication channels protected by IPSec or a similar protocol. All data is stored on storage services that use encryption at rest.

Anonymization
We never store any personally identifiable information unless needed to deliver our products and services. If applicable, we pseudonymize data, and wherever possible, we utilize geohashing to minimize the possibility of address identification through our stored positioning data.

Deletion
Data is stored for the duration of the customer contract and automatically deleted after 60 days unless the customer instructs us otherwise. We log and monitor all deletion activities for compliance.

Availability & resilience
Backup
We store data in multiple technological platforms that utilize different backup technologies. We always ensure that we take regular backups at least once a day. Backups are stored separately from our production environment to ensure the safety and integrity of the backup data. Regular validation and testing of all backups are conducted, utilizing both automated methods and manual verification.

Monitoring
All our systems are proactively monitored 24 hours a day, 7 days a week to ensure availability. Our technical on-call team is available 24/7 to respond to abnormalities identified by our monitoring solutions.

Logging

All logging from our products and services is centralized, enabling our technical team to get deep insight into the operations of our products and services, as well as creating a robust audit trail. We log all impersonation sessions in which employees access customer accounts to provide support and resolve problems.

Incident handling
Documented and formal processes for detecting and responding to incidents, including data breaches, are established in our information security management system (ISMS). The Information Security Officer and Data Protection Officer (DPO) are involved in handling all security incidents and data breaches.
Formal processes for conducting post-mortem analysis of incidents have been established and followed up according to processes in our Quality Management System (QMS).

Specific Technical and Organisational Measures

Description of the technical and organizational security measures implemented by the controller(s) (including any relevant certifications) to ensure an adequate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks to the rights and freedoms of natural persons:

1. Description of technical and organizational security measures
The Processor and Sub-Processors undertake to guarantee a level of security no lower than that provided for by the technical and organizational measures described below.
2. System Administrators
The Data Processor and Sub-Processors shall comply with the Decision issued by the Italian Data Protection Authority, dated 27 November 2008 (and its subsequent amendments) entitled "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator”
2.1 Designation
The Processor and Sub-Processors shall draw up a letter of individual designation for each system administrator, following the evaluation of the experience, capacity and reliability of the subjects, containing an analytical list of the areas of operation.
2.2 Review of the work of the System Directors
The Processor and Sub-Processors shall proceed, at least once a year, with a process of reviewing the work of the system administrators through the means that they deem appropriate.
2.3 List of System Administrators
The Processor and Sub-Processors shall produce, at the request of the Data Controller, a list of the personnel designated as system administrator**.**
2.4 Logging
The Processor and Sub-Processors shall implement an operational intelligence software that produces access logs relating to the systems on which the system administrators operate, having characteristics of completeness and inalterability as well as being subject to integrity verification and to be kept for at least 6 months.
3. Authentication
3.1 Credentials
The Processor and the Sub-Processors shall create an alphanumeric password consisting of at least 8 characters in length, containing upper/lower case letters and special characters. The Data Processor and the Sub-Processors shall proceed, if necessary, at the express request of the Data Controller, with the combination of two or more authentication factors. The Processor and the Sub-Processors shall apply this password policy to all company systems and applications.
3.2 Individual Credentials

The Processor and the Sub-Processors shall not assign shared credentials but shall assign only individual credentials, in particular with regard to figures with high permissions on systems and applications.

3.3 Reporting inactivity

The Processor and the Sub-Processors shall ensure that all credentials, except those used for technical management purposes only (e.g. machine users or root credentials), are reported as inactive after 6 months.

3.6 Non-disclosures

The Processor and the Sub-Processors shall implement and document appropriate procedures for accessing the data in the event of the prolonged absence of the person in charge who holds them. These procedures should not, in any case, provide for the disclosure of the password of the person in charge.

4. Data and Device Protection

4.1 Protection of credentials

The Processor and the Sub-Processors shall draw up a policy containing clear instructions on the precautions to be taken to ensure the secrecy of the credentials and the diligent custody of the devices assigned.

4.2 Protection from damage and theft

The Processor and the Sub-Processors shall draw up a policy containing clear instructions on the precautions to be taken to ensure the protection of the devices assigned.

4.3 Session protection

The Processor and the Sub-Processors shall implement a lock screen/screensaver system with the re-entry of credentials whenever there is not physically an employee present to supervise/use the workstation. This lock screen should be set so that it activates automatically after less than 20 minutes of inactivity.

5. Authorization

5.1 Authorization profiles

The Processor and the Sub-Processors shall implement a centralized system for the management of authentication and authorization. The Processor and the Sub-Processors shall proceed to a census of the authorization profiles, before assigning them.

5.2 Minimizing permissions

The Processor and the Sub-Processors shall proceed in a residual way, not assigning more permissions than necessary and respecting the principles of least privilege and need to know, i.e. allowing the visualization only of the data necessary to carry out the work function, with the attribution of minimum permissions on systems and applications.

5.3 Profile review

The Processor and the Sub-Processors shall verify the consistency of the authorization profiles at least annually and proceed with the reporting of such activity.

6. Defense

6.1 Updates

The Processor and the Sub-Processors shall monitor and manage the updates in a centralized and/or automated manner, or to adopt suitable organizational means in such a way as to make the machines and applications constantly updated, taking particular account of security updates.

6.2 Isolation of systems no longer supported

The Processor and the Sub-Processors shall segregate the machines that for operational reasons are still in use even though they are no longer supported by updates.

6.3 Data protection by design

The Processor and the Sub-Processors shall formalize or adopt data protection by design guidelines, ensuring that the company systems developed internally are consistent with them.

6.4 State of the art protection programs

The Processor and the Sub-Processors shall implement and maintain updated protection software such as antivirus, which should be managed preferably centrally, firewall, preferably containing IDS and IPS modules, antispam.

7. Data availability

7.1 Backups

The Processor and the Sub-Processors shall implement a backup system, formalizing a backup plan, documenting the technologies in place within a policy that also contains a procedure for correctly carrying out this activity.

8. Data protection

8.1 Encryption and confinement

The Processor and the Sub-Processors shall are committed to implementing encryption techniques at all levels: full disk encryption on mass drives, transparent data encryption on databases, file-level encryption for files containing credentials, through the use of non-deprecated cryptographic standards.

8.2 Pseudonymization

The Processor and the Sub-Processors shall pseudonymize any personal data contained in the databases.

8.3 Encryption in transit

The Processor and the Sub-Processors shall implement and document the encryption technologies in transit

9. Removable devices

9.1 Removable devices

The Processor and the Sub-Processors shall regulate the use of removable media and their protection.

9.2 Sanitization of removable devices

The Processor and the Sub-Processors shall formalize appropriate procedures for the destruction, encryption and/or formatting of removable devices and company devices in use.

10. Security roles

The Processor and the Sub-Processors shall define the corporate function who is responsible for cybersecurity, i.e. who can cover it in the company with the relative responsibilities. This may involve appointing a CISO (Chief Information Security Officer) or, more generally, a CSO (Chief Security Officer) or, generally, a person who has the authority, in the company, to perimeter, under the security, information technology and information, the processes of the organization. This figure should be available to detect security incidents and should be known to all employees.

11. Third parties

11.1 Contracts

The Processor and the Sub-Processors shall draw up all relevant contracts with outsourcers and suppliers in such a way that they also include the security requirements relevant to the service provided or product supplied.

11.2 Second level audits

The Processor and the Sub-Processors shall periodically verify the consistency with the contractual security requirements by means of second-level audits, suitably being contracted and scheduled.

12. Asset Management

The Processor and the Sub-Processors shall remove assets and credentials of employees who are no longer in force within the infrastructure of the Processor and the Sub-Processors, or who have changed the task and assets necessary to carry out the task.

The Processor and the Sub-Processors shall carry out a periodic verification of the effective removal of assets and credentials.

13. Physical security of the Data Center

13.1 Physical security measures
The Manager and any Sub-Managers agree to cooperate with the Controller in implementing formal access procedures to allow physical access to the Data Center. The servers and machines on which the Controller's data are stored, within the Data Center, are housed in facilities that require access with keys equipped with electronic cards, with alarms linked to any SOCs or physical security monitoring centers. Requests for key card access must go through a formalized approval process. Unauthorized activities and unsuccessful access attempts are logged by the access control system and, where appropriate, reviewed. Fire doors in the Data Center are equipped with alarms. CCTV cameras are in operation both inside and outside the Data Center. The placement of the cameras is designed to cover strategic areas including, but not limited to, the perimeter, the doors of the CED building, and the entrance areas. On-site security operations personnel operate the CCTV monitoring, recording, and control equipment. The CCTV equipment records 24 hours a day, 7 days a week. Recordings are kept for at least 7 days, depending on activity.
13.2 Visitors
The Processor and the Sub-Processors undertake to authenticate visitors before accessing the Data Center. The Processor and the Sub-Processors shall accompany visitors within the structure of the Data Center and to prepare an access register for them. In order to gain access to the Data Center facility, visitors must (i) obtain approval in advance from the Data Center Managers for the internal areas they wish to visit; (ii) gain access through on-site identification.
13.3 Conditions of the Data Center
The Processor and the Sub-Processors shall constantly monitor the conditions of the Data Center, taking into account the variables relating, among others, to temperature, condition of the cooling system, dust, humidity and to periodically check the functioning of the sensors.
14. Access control
14.1 Individual credentials
The Processor and the Sub-Processors shall commit themselves to set individual credentials for each person in charge and forbid them in sharing such credentials.
14.2 Authorisation profiles
The Processor and the Sub-Processors shall undertake, within the limits of what is permitted by the systems, to create authorization profiles to which the users created are assigned.
14.3 Competing sessions
The Processor and the Sub-Processors shall set a maximum number of competing sessions on a given system for the same user.
14.4 Rate limiting
The Processor and the Sub-Processors shall set a maximum number of failed login attempts before blocking the account on all company systems and applications.
15. System Integrity
15.1 Password management and encryption keys
The Processor and the Sub-Processors shall commit to implementing solutions for the management of passwords and encryption keys.
15.2 Absence of possible deactivation
The Processor and the Sub-Processors shall undertake not to allow the persons who are not in charge of security functions, to be able to deactivate the protective measures on their machines.
16. Vulnerability assessment and penetration testing
16.1 Scheduling
The Processor and the Sub-Processors shall conduct sessions of vulnerability assessment and penetration testing on the company's systems on a regular basis.
16.2 Automated scan
The Processor and the Sub-Processors shall use tools for automated Vulnerability Assessment, which must not, however, replace the traditional one.

17. Management of incidents and violations

17.1 Incident handling procedures

The Processor and the Sub-Processors shall introduce practices, protocols and procedures relating to incident handling and manage all security events and/or security incidents through a formalised procedure with pre-established roles.

17.2 Staff training

The Processor and the Sub-Processors shall inform the personnel regarding the incident handling procedures.

17.3 Alerts

The Processor and the Sub-Processors shall consider, if deemed functional and appropriate to the risk, to adopt a SIEM, or alternative solutions that achieve the purpose of reporting anomalies and/or attacks in progress.

17.4 Record of incidents

The Processor and the Sub-Processors shall draw up and maintain a record of incidents, containing at least information on discovery, analysis, containment, mitigation and recovery from the various security incidents.

17.5 Communication to the Data Controller

The Processor and the Sub-Processors shall notify the Data Controller, without undue delay after having become aware, of any security incident that has occurred on their infrastructure.

18. Business continuity and Disaster Recovery

18.1 Business continuity

The Processor and the Sub-Processors shall guarantee the operational continuity for all the services offered to the Data Controller, though, if necessary, the formalization of a Business Continuity Plan.

18.2 Disaster recovery

The Processor and the Sub-Processors undertake to make it possible to restore all of the Processor's data following disasters, by formalizing, if necessary, a Disaster Recovery strategy, including detailed policies for the safe storage of backup copies and their recovery.

18.3 Encryption and storage

The Processor and the Sub-Processors shall provide for the encryption of the backup and to provide for secure procedures for their custody.

19. Training

The Processor and the Sub-Processors shall formalize periodic security awareness training for all office staff, in order to reduce the possibility of intrusions, successful phishing or malware infection.

20. Recording of operations

The Processor and the Sub-Processors shall implement an operational intelligence software that produces unalterable logs, complete and subject to integrity verification that operates on the systems on which the personal data referring to the Data Controller are processed.

21. Software development and environment management

21.1 Development guidelines

The Processor and the Sub-Processors shall implement and adopt guidelines for writing secure code.

21.2 Testing

The Processor and the Sub-Processors shall test software and systems after they have been put into production.

21.3 Patches

The Processor and the Sub-Processors shall install and uninstall the patches using known practices.

21.4 Protection of test data

The Processor and the Sub-Processors shall protect the test data by obfuscation or encryption and to make them usable by authorized personnel.

22. Change management

22.1 Formalization of change management

The Processor and the Sub-Processors shall make changes to critical systems through known practices or formalized procedures.

22.2 Notification to the Data Controller

The Processor and the Sub-Processors shall notify the Data Controller of any significant changes to the User Experience.

23. Employment relationships

23.1 Before the start of the employment

The Processor and the Sub-Processors shall take into consideration the responsibilities of information security when hiring employees, collaborators and temporary staff (e.g. through adequate job descriptions, pre-employment controls) and to include them in the contracts (e.g. with terms and conditions of the employment relationship and signing of further agreements aimed at defining roles and responsibilities in terms of security, compliance obligations, etc.).

23.2 During the employment

The Processor and Sub-Processors are committed to ensuring that Processors ensure that employees and contractors are aware of and motivated to comply with their obligations to ensure information security. The Processor and the Sub-Processors shall also undertake to formalise a disciplinary procedure to manage information security incidents allegedly caused by workers.

23.3 Termination or modification of the employment

The Processor and the Sub-Processors shall manage security aspects when a person leaves the organization, or in the event of significant changes to the role held, such as the return of company information and equipment held by the outgoing person, the updating of access permits, as well as compliance with the continuing obligations relating to confidential information and intellectual property rights, contractual terms, etc. and also to ethical duties.

24. Compliance

24.1 Compliance with legal and contractual requirements

The Processor and the Sub-Processors shall ensure that the organization identifies and documents its obligations to external authorities and other third parties in relation to the security of information, including intellectual property, accounting documentation, privacy information/conditions for personal identification and encryption.

24.2 Information security review

The Processor and the Sub-Processors shall ensure that the organization’s information security projects are reviewed (audited) in such a way as to guarantee the independence of the assessment and reported to the Management. The Processor and Sub-Processors also undertake to ensure that Processors periodically review the compliance of employees and systems with security policies, procedures, etc., and promote corrective action where necessary.