ABAX Data Processing Agreement

These documents are valid from April 12th 2022.

Data Processing Agreement

Between:

THE SUPPLIER,

by the legal entity as specified in order confirmation or the signed customer agreement (the "**Customer Contract**"), acting as data processor

and

THE CUSTOMER,

by the person or legal entity as specified the Customer Contract, acting as data controller

the following agreement on the processing of personal data has been entered into ("**Data Processor Agreement**"):

1. Background and purpose

1.1. The Supplier and the Customer have entered into a Customer Contract. The Supplier's provision of some or all services under the Customer Contract requires that the Supplier process personal data on behalf of the Customer. The Supplier is therefore regarded as a data processor and the Customer as a data controller in connection with processing of personal data.

1.2. This Data Processor Contract sets out the rights and obligations of the Supplier's processing of personal data on behalf of the Customer pursuant to the Customer Contract, and applies to all processing of personal data the Supplier undertakes for the Customer upon performing the services. This Data Processor Agreement constitutes an integral part of the Customer Contract, including other contract documents. In case of any inconsistencies between the terms of this Data Processor Agreement and the General Terms and Conditions,

the terms of this Data Processor Agreement shall prevail with regards to the processing of personal data.

1.3. The Data Processor Agreement shall ensure that personal data is processed in accordance with applicable national laws and EU or EU member state law for processing of personal data, including the General Data Protection Regulation (2016/679) of the European Parliament and of the Council ("**GDPR**"), hereinafter jointly referred to as the "**Data Protection Legislation**".

1.4. Concepts and definitions used in this Data Processor Agreement shall be understood in the same way as in the Data Protection Legislation.

2. The Supplier's obligations

2.1. The Supplier shall only process personal data on behalf of the Customer in accordance with documented instructions of the Customer.

2.2. The Supplier shall process personal data in the manner as described in this Data Processor Agreement, or as otherwise agreed in writing (including electronically) between the Supplier and the Customer.

2.3. Any supplementary instructions on the processing shall be submitted to the Supplier's stated contact information.

2.4. Regardless of what is stated in clause 2.1 to 2.3, the Supplier shall process personal data as required by law. The Supplier shall notify the Customer if the Supplier is required by mandatory law to process personal data contrary to the Customer's instructions, unless providing such notification is prohibited by law.

2.5. If the Supplier considers that an instruction from the Customer is in violation of the Data Protection Legislation, the Supplier shall immediately inform the Customer of its opinion. The Supplier undertakes to exercise its obligations under the Customer Contract and Data Processor Agreement despite its opinion.

2.6. The Supplier shall ensure that employees and subcontractors or other third parties authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This provision also applies after the termination of the Data Processor Agreement.

2.7. The Supplier shall implement appropriate technical and organisational measures required pursuant to Article 32 of the GDPR, including measures to ensure that data is available to the Customer, to prevent the loss or destruction of data, and prevent unauthorised access to data.

2.8. The Supplier shall keep an updated list of all sub-processors and ensure that any sub-processors processing personal data on behalf of the Customer have entered into a binding agreement with the Supplier pursuant to Article 28 (2) and (4) of the GDPR.

2.9. The Supplier shall, by means of appropriate technical and organisational measures, bearing in mind the nature of processing and to the extent possible, assist the Customer in responding to requests submitted by data subjects seeking to exercise their rights pursuant to Chapter III of the GDPR.

2.10. The Supplier shall assist the Customer in fulfilling the duties pursuant to Articles 32 to 36 of the GDPR.

2.11. The Supplier shall keep a record of processing activities performed on behalf of the Customer, which shall contain at least the information provided pursuant to the GDPR Article 30 (2).

3. The Customer's obligations

3.1. The Customer is responsible for ensuring that the processing of personal data complies with the requirements set out in the Data Protection Legislation, hereunder ensuring that the processing of personal data, which the Supplier is instructed to perform, has a legal basis.

3.2. The Customer has the right and obligation to determine the purpose and means of the processing.

3.3. The Customer might provide the Supplier with documented instructions on how the personal data should be processed, and hereby instructs the Supplier to process personal data to the extent and in the manner in which such processing is required to provide the services under the Customer Contract and as described in section 8.

3.4. The Customer may give other additional instructions as long as such additional instructions are, taking into account the nature of and the Supplier's obligations under the Customer Contract, relevant for the provision of the services under the Customer Contract.

4. Use of sub-processors and transfer of data outside the EEA

4.1. The Supplier has the right to use the current sub-processors which appears on the list found here: https://www.abax.com/terms-and-conditions. The Supplier use few sub-processors outside the European Economic Area (EEA) where European Standard Contract Clauses (SCCs) are used as a basis for transfer.

4.2. The Customer hereby grants a general authorisation for the Supplier to use sub-processors to process personal data to fulfil the contractual obligations under the Customer Contract.

4.3. The same data protection obligations as set out in this Data Processor Agreement shall be imposed on the sub-processor, in particular concerning guarantees to implement appropriate technical and organisational measures. If a sub-processor does not fulfil its data protection obligations, the Supplier shall remain fully liable to the Customer as regards the fulfilment of

the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR.

4.4. The Supplier shall inform the Customer in writing before replacing or adding new sub-processors, no less than 30 days prior to the intended change, thereby giving the Customer the opportunity to object to such changes.

4.5. The Customer may not reject a new sub-processor without a legitimate reason. Any rejection based on well-founded suspicion that the level of data protection may be degraded as a result of the change of sub-processor shall be regarded as a legitimate reason.

4.6. If the Customer wishes to object to the engagement of the new sub-processor and has legitimate reasons based on privacy to do so, the Customer may, within 14 days of receiving the Supplier's written notification, serve the Supplier a written objection detailing such legitimate reasons. If the Customer does not serve such objection notice within the stipulated timeframe, the Customer is deemed to have accepted the use of the new sub-contractor.

4.7. If the Supplier insists on using the new sub-processor even though the Customer has provided an objection with legitimate reasons based on privacy as described above, the Customer shall, as its sole remedy, have the right to terminate the part of the Customer Contract affected by the change. To terminate part of the Customer Contract, the Customer shall serve the Supplier a written termination notice stating the date the termination shall take effect, which shall be no later than the last day of the 30-day period as set out in clause 4.4. If the Supplier has not received such termination notice two days before the end of the 30-day period, the Customer's right to termination under this section 4.7 expires.

4.8. If it is critical to replace or add a new sub-processor in order to fulfil the services under the Customer Contract, the Supplier may, notwithstanding the above, implement the change immediately after the Customer has been notified.

4.9. The Supplier is entitled to process personal data outside the EEA to the extent the processing is carried out by sub-processors at any time included on the list of sub-processors outside the EEA. Any additional transfers of personal data to a country outside the EEA will not be carried out without documented instructions from the Customer.

5. Security Measures

5.1. The Supplier shall fulfil the requirements for security measures imposed under the Data Protection Legislation and shall be able to document procedures and other measures to meet these requirements.

5.2.

- The Supplier complies with information security management system standard ISO 27001:2017.

- All Customer data is encrypted both in transit and "at rest".
- The Supplier utilise network segmentation in all our production environments.
- All Supplier infrastructure is kept up to date with the latest security patches released by our vendors.
- The Supplier uses the principle of least privilege (PoLP) to control access to systems and data to ensure proper access control.

5.3. The Supplier has 24/7 on-call staff to handle unplanned events and incidents. The Supplier ensures redundancy in all infrastructure and systems by using vendors that deliverers industry-standard solutions with a high degree of availability.

6. Audits

6.1. The Supplier shall make available to the Customer all information necessary to demonstrate compliance with Article 28 of the GDPR and fulfilment of the obligations outllined in this Data Processor Agreement, as well as facilitate and contribute to audits, including onsite inspections, conducted by the Customer or another auditor mandated by the Customer. The other auditor shall not be a competitor of the Supplier.

6.2. The Customer may require audits once per year. In case of special circumstances that motivate an additional audit, such as a personal data breach or the Customer having reasons to believe that the Supplier is in breach of this Data Processor Agreement, the Customer may carry out an additional audit.

6.3. The Customer shall provide no less than two weeks written notice of the proposed audit, and the audit shall be carried out in a manner that minimises interference with the Supplier's day-to-day business activities. The findings of the audit shall be treated as confidential and shall be discussed and evaluated by both parties.

6.4. The Customer shall bear all costs and fees related to such audit. If the Supplier is rendering any support or services related to the audit, then the Supplier is entitled to issue an invoice for hourly time 200 EUR for all actual costs and fees.

6.5. Notwithstanding the above mentioned, the Customer or inspector will not be allowed access to server rooms and other information and location to the extent this could potentially pose a risk to the Supplier's security level or confidential information. The Supplier alone assesses this risk.

7. Notification routines

7.1. If the Supplier becomes aware of a personal data breach, the Supplier shall notify the Customer without undue delay.

7.2. The notification shall at least describe:

1. The nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned,
2. The name and contact details of the data protection officer or another contact point where more information can be obtained,
3. The likely consequences of the personal data breach,
4. The measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.3. If the Supplier is unable to provide all the information above at the first notice, the information may be provided gradually without undue delay.

7.4. The Customer shall ensure that an incident report is sent to the relevant Data Protection Authority in accordance with Article 33 of the GDPR, whereas the Supplier may not send such notice or contact the supervisory authority without the Customer's instructions.

8. Scope of the processing

8.1. The scope of the processing will depend on which services are included in the Customer Contract, and of the instructions given by the Customer and the adjustments made by the Customer in the user interface.

8.2. Hereby follows a description of the scope of the processing, describing inter alia the type of personal data that may be processed upon providing the services:

The purpose of the processing

The Supplier shall process personal data to provide the services specified in the Customer Contract.

The duration of the processing

The processing shall last for as long as the Supplier provides services to the Customer under the Customer Contract.

The nature of the processing

The Supplier shall collect, store and make data available for the Customer and users via a graphical user interface to provide the services specified in the Customer Contract. The Supplier may also transfer data to third parties at the Customer's request.

The Supplier shall make data available for its affiliated company's technical and support personnel to provide support under the Customer Contract, and collect data on how the Suppliers services are used and collected.

The type of personal data to be processed

Depending on services included in the Customer Contract and the instructions and amendments made by the Customer, the Supplier might process the following data that can be considered personal:

Information about users, optionally provided by the Customer, such as Name, Address, Mobile, E-mail, Job title, Employee number, Tax zone, Bank account number, Department.

Information about vehicles, optionally provided by the Customer, such as Registration number, Make, Model, First-time registered date, Emissions data, Vehicle group, Colour, Vehicle name, Vehicle type, Fuel type, Vehicle category, Assigned driver, Initial and corrected mileage readings, Leasing details (Leasing company, Contract number, Contract start date, Mileage limit, Leasing agreement duration, Mileage reading at the start of the leasing period), Insurance details (Insurance company, Contract number, Contract start date, Mileage limit, Insurance agreement duration, Mileage reading at the start of the insurance), Servicing details (Date of last service, Mileage at last service, Service interval by distance driven, Service interval by time, E-mail address on who to notify and who has been notified).

Information about equipment, optionally provided by the Customer, such as Make, Model, Name, Serial nr, Registration number, Department, Tags, Operating hours at last service, Service intervals, Inspection details (Last inspection date, Inspection interval, Inspection notes), E-mail address on who to notify and who has been notified).

Data provided by hardware or created from hardware data, such as Location, Engine on and off, Trip start and stop location, Trip start and stop address, Trip start and stop date and time, Current speed, Current direction, Raw Accelerometer data to build driving behaviour score and detect driving events (Rapid acceleration, Hard breaking, Harsh turning, Idling), data per 1 HZ to build risk profile for improved and reduced ownership costs including for insurance, leasing and vehicle maintenance costs, hardware diagnostic such as GPS satellites in view, installation angle, Operating hours.

User profile information such as Username, Password, E-mail, Mobile number, and language preference.

Logging of software usage such as what the user clicks on, sequence of clicks, statistics, traffic sources and analysis data including masked IP address.

The categories of data subjects

Customers, Customers' employees, or others using the vehicle or equipment.

8.3. The Customer may however instruct the Supplier on the processing, which may cause the processing to deviate from what is described above. The Customer may also add information

and make a change in the user interface, including changes of settings, which may cause the processing to deviate from the description above.

8.4. Unless otherwise is agreed, the Supplier has the right to receive a reasonable payment if the Customer gives instructions that do not lie within the service and requires changes or adjustments, with remuneration based on the Supplier's hourly rate of 200 EUR. The Supplier may also refuse the instruction if it exceeds the service and cannot be met by simple means.

9. Liability

9.1. Each party is responsible for covering administrative fines and other sanctions imposed as a result of breaches of the Data Protection Legislation. If a party has been held liable for damages under Article 82 of the GDPR for a matter for which the other party is responsible, the party responsible shall cover the cost of damages. The limitation of liability set out in the General Terms and Conditions shall apply to liability according to Article 82 of the GDPR.

10. Term and termination

10.1. This Data Processor Agreement enters into force by the Customers electronical signature and remains in force for as long as the Supplier processes personal information on behalf of the Customer according to the Customer Contract.

10.2. If the Customer Contract is terminated, this Data Processor Agreement will automatically be terminated when the processing has ended after deletion (including backup).

10.3. In the event of a breach of this Data Processor Agreement or the Data Protection Legislation, the Customer may instruct the Supplier to stop further processing of the data with immediate effect.

11. Duties upon termination and cancellation

11.1. Upon termination of the Customer Contract, the Supplier shall at the choice of the Customer either permanently delete or return all personal data received on behalf of the Customer.

11.2. The Customer may require that the Supplier delete all personal data processed under this agreement. The deletion shall be carried out no later than 60 days after the agreement is terminated.

11.3. Should the Customer not request return or deletion in accordance with the previous paragraph, the Supplier shall nevertheless delete personal data received on behalf of the Customer no later than 60 days after the Customer Contract is terminated, unless the Supplier has another legal basis for storing the data, such as having a legal obligation to do so or a separate agreement with Customer on further data storage.

11.4. The Supplier's obligation to delete personal data does not apply if the information is anonymized (and thus no longer constitutes personal data) or the Supplier has a legal basis for refraining from deleting, e.g. to defend a legal claim.

11.5. Backup copies that contain personal data will be deleted in accordance with the Supplier's routines for deletion of backups. If the Customer requires the backup copies to be deleted outside the regular routines, the Supplier will do this as a paid service, with remuneration based on the Supplier's hourly rates.

12. Miscellaneous

12.1. This Data Processor Agreement forms an integral part of the Customer Contract, including other contract documents, such as the General Terms and Conditions. Provisions laid down in the above-mentioned documents apply, including but not limited to the contact information, limitation of liability and law and legal venue.

12.2. Upon transfer of the Customer Contract to other parties, the Data Processor Agreement shall be transferred accordingly.

12.3. The Supplier is entitled to do necessary changes in this Data Processor Agreement. The Supplier shall send a written notice (also electronically) to the Customer. The Customer has the right to oppose major changes in writing within 30 days provided that the Customer has a just and factual objection.

Sub Data Processors

Name	Country	Description	Link
Amazon Web Services EMEA SARL (AWS Europe)	Luxembourg	We use AWS public cloud services to deliver services to our customers	https://aws.amazon.com/
AS Skan-Kontroll	Norway	In your request and only after signing a legal contract we share certain data with Skan-Kontroll in order to enable our after-theft recovery solution.	http://www.skan-kontroll.no
Telenor ASA	Norway	Telenor delivers connectivity to our sensors.	https://www.telenor.no
Twoday AS	Norway	Twoday helps us operate our business intelligence platform	https://www.twoday.no
Saga Regnskap og Rådgivning AS	Norway	Saga helps us operate our ERP platform	https://sagarr.no/
ITX Norge AS	Norway	ITX delivers our unified communication platform used to	https://itx.no

		communicate with our customers	
Ferde AS	Norway	On your request and only after signing legal contract we cooperate with Ferde to deliver Toll Road service including ferry.	https://ferde.no
Skyttel AS	Norway	On your request and only after signing legal contract we cooperate with Skyttel to deliver out Toll Road service.	https://skyttel.no/
Caruso GmbH	Germany	On your request and only after signing legal contract we can share certain data in order to offer new and better services.	https://www.caruso-dataplace.com/
Ruptela UAB	Lithuania	Supplier of our Fleet Management Solution.	https://www.ruptela.com
HubSpot Ireland Ltd	Ireland	We use HubSpot to communication with our customers and prospects as well as building additional webpages on abax.com	https://hubspot.com
Google Ireland	Ireland	We use GCP public cloud services to deliver services to our customers	https://cloud.google.com/
Tryg Forsikring (Tryg Adferdsforsikring)	Norway	Tryg will receive data from ABAX to calculate user based insurance premium offers. The supplier will be used in correlation with contractual agreements based on enabled features.	https://www.tryg.no/
GetAccept	Sweden	We use GetAccept to send out Contract Documents for signing.	https://www.getaccept.com/
Piwik Pro	Poland	Piwik Pro provides web analytics services, allowing us to track website traffic, user behavior, and improve user experience through the use of cookies. Piwik Pro emphasizes data privacy and security, offering tools that ensure compliance	https://piwik.pro

		with GDPR, CCPA, and other data protection regulations. Piwik Pro may collect IP addresses, user interactions, browser information, and cookie data for analytics purposes.	
MobyLinq	Norway	MobyLinq enables the secure use of analysed vehicle data to support tailored data based services.	https://www.mobylinq.com/

Sub Data Processors – Third countries

As a result of the recent Court of Justice of the European Union ruling on data transfers, invalidating the Privacy Shield, ABAX will be moving to Standard Contractual Clauses (SCCs) for transfers of online advertising and measurement personal data out of the EU/EEA.

Any questions regarding this? Please get in touch with our Data Protection Officer, on dpo@abax.no

Business Partners

Name	Country	Description	Link
Tryg Forsikring (Tryg Adferdsforsikring)	Norway	Tryg will receive data from ABAX to calculate user based insurance premium offers. The supplier will be used in correlation with contractual agreements based on enabled features.	https://www.tryg.no/