

Data License Agreement

(as of February 2026)

PREAMBLE

idem telematics GmbH (the "**Contractor**") is a provider of telematics solutions in the field of transport and logistics. Sensors are used to collect, transmit, process, and send data on freight and vehicles to customers.

In accordance with Regulation (EU) 2023/2854 of 13 December 2023 (the "**Data Act**"), connected products must be designed and manufactured in such a way that customers can easily and securely access, use, and share the generated data. This is intended to ensure fair access to and use of data. Customers of connected products may choose to share this data with third parties to create new or improved services. .

This This data license agreement (the "**Data License Agreement**") forms part of the service contract or other written agreement between the Contractor and the Customer that governs the Contractor's and third parties' use of the data (the "**Service Agreement**").

1. SUBJECT MATTER, SCOPE OF APPLICATION

- 1.1 The object of usage processing is all data (Article 2 No. 1 Data Act) that is obtained, generated or collected during the use of the Contractor's *connected products* (Article 2 No. 5 Data Act) (together "**Data**"). This includes *product data* (Article 2 No. 15 Data Act), *related service data* (Article 2 No. 16 Data Act) and relevant *metadata* required for the interpretation and use of this data (Article 2 No. 2 Data Act).
- 1.2 This Data License Agreement regulates the rights and obligations of the Customer as the *user* (Article 2 No. 12 Data Act) of the connected products and the Contractor as the *data holder* (Article 2 No. 13 Data Act) of the data.
- 1.3 The transfer of the connected products and the content and scope of data processing are set out in the Service Agreement between the Parties.
- 1.4 Insofar as the data pursuant to Section 1.1 has a personal reference and constitutes *personal data* within the meaning of Article 4 No. 1 of Regulation (EU) 2016/679 ("**GDPR**"), the agreement concluded between the Parties on data processing pursuant to Article 28 GDPR shall also apply to this data, which shall take precedence over the provisions of this Data License Agreement in the event of a conflict or an objection regarding the processing of personal data.
- 1.5 If terms are not defined in this Data License Agreement, they shall have the meaning given in the Data Act and the GDPR.

2. USAGE OF DATA BY THE CONTRACTOR

- 2.1 The Contractor shall be entitled to use data that is not personal data for the following purpose:
 - a) Fulfillment of contracts with the Customer or activities in connection with such contracts (e.g., issuing invoices, preparing and providing reports or analyses, forecasts, impact assessments);
 - b) Provision of assistance, support, warranty, or similar services, or for the evaluation of claims by the Customer, Contractor, or third parties in connection with the product or related services;
 - c) Monitoring and maintaining the functionality, security, and protection of the product or related services and ensuring quality control;
 - d) Improving products or related services offered by the Contractor;
 - e) Developing new products or services, including Artificial Intelligence (AI) solutions, by the Contractor, by third parties on behalf of the Contractor, or by companies affiliated with the Contractor;
 - f) Aggregating this data with other data or creating derived data for any lawful purpose, including the purpose of selling or otherwise making such aggregated or derived data available to third parties, subject to contractual confidentiality obligations.

- 2.2 The Contractor undertakes
- a) not to use the data to derive insights into the economic situation, assets, and production methods of the Customer; and
 - b) to ensure this with appropriate organizational and technical means.

3. ACCESS AND PROVISION OF DATA FOR THE CUSTOMER

- 3.1 Data Accessibility by Design & by Default: The Contractor shall design and manufacture the connected products and connected services in accordance with Article 3 (1), 50 sentence 3 Data Act in such a way that the data is accessible to the Customer.
- 3.2 Data Access Entitlement: The Contractor shall make the data available to the Customer in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, directly (Data Access Entitlement).
- 3.3 Obligation to provide: If the Customer cannot access the data directly from the connected product or connected service in accordance with Section 3.2, the Contractor shall provide the Customer with *readily available data* (Article 2 No. 17 Data Act) including *metadata* that were generated after the Data Protection Act came into force immediately, simply, securely, free of charge, in a comprehensive, common and machine-readable format and - if relevant and technically feasible - in the same quality as for the Contractor continuously and in real time. This shall be done electronically upon simple request, insofar as this is technically feasible.
- 3.4 Derived data: The right of access does not include inferred or derived data that is the result of additional investment in attributing value or insight from the data (*Derived Data*). The Contractor is not obliged to provide this data.

4. CUSTOMER'S RIGHT TO TRANSFER DATA TO THIRD PARTIES

- 4.1 Data transfer claim: At the request of the Customer or a party acting on its behalf, the Contractor shall provide a designated third party with readily available data (Article 2 No. 2 Data Act) and the metadata without undue delay, free of charge to the Customer, in the same quality as is available to the Contractor, simply, securely, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real time.
- 4.2 Exclusion of gatekeepers: The data transfer claim does not exist with regard to gatekeepers within the meaning of Article 3 of Regulation (EU) 2022/1925 September 14, 2022 ("**Digital Markets Act**").
- 4.3 Verification of the parties involved: The Contractor is entitled to demand suitable proof of identification from the Customer in order to verify the Customer's authorization to access the data and transfer it to a third party.
- 4.4 Protection of personal data: If the data to be transferred contains *personal data* and the Customer is not the *data subject* (Article 4 No. 1 GDPR) whose personal data is requested (fourth-

person reference), the Contractor may only provide this data to the third party if the legal requirements, in particular Article 6 and Article 9 GDPR and Section 25 of the German Law on Data Protection and Privacy in Telecommunications and Digital Services (*Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten – “TDDDG”*) are met. This also applies to mixed data sets that contain both personal and non-personal data. In this case, the third party must ensure that the data subject is adequately informed in accordance with Article 13 and Article 14 GDPR about the specific, clear and lawful purposes of the data processing as well as of the data subject's rights. The right to data transfer applies without prejudice to the right to data portability pursuant to Article 20 GDPR.

4.5 Protection of trade secrets: The protection of the Contractor's trade secrets in accordance with the Trade Secrets Protection Act (*Geschäftsgeheimnisgesetz – “GeschGehG”*) and Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure shall remain unaffected.

- a) The Contractor shall only disclose data to the extent that such disclosure is absolutely necessary for the purpose agreed between the Customer and the third party.
- b) The Contractor or the holder of the trade secret is entitled to take all reasonable technical and organizational measures necessary to protect the confidentiality of the data disclosed, in particular to conclude a confidentiality agreement with the third party and to implement access logs, before disclosing the data.
- c) The data holder is entitled to refuse or suspend the transfer of data if (i) the third party is not prepared to enter into a confidentiality agreement, (ii) does not implement the measures referred to in lit. b) or (iii) breaches the confidentiality of the trade secrets. The Contractor must duly justify the decision and notify the third party in writing without delay. In this case, the Contractor must notify the competent authority designated in accordance with Article 37 Data Act that it has refused or suspended the transfer of data and indicate which measures have not been agreed or implemented and in which trade secrets confidentiality has been breached.
- d) The data holder is entitled to refuse to disclose data in individual cases if despite the measures taken in accordance with lit. b), the Contractor is highly likely to suffer serious economic damage as a result of the disclosure of data containing trade secrets. The contractor must demonstrate the impending damage on the basis of objective facts, in particular the enforceability of the protection of trade secrets in third countries, the nature and degree of confidentiality of the requested data, and the uniqueness and novelty of the connected product and submit the justification to the third party in writing without delay. In this case, the contractor must inform the competent authority designated in accordance with Article 37 Data Act.

4.6 Agreement with third parties: If there is a right to transfer data, the Contractor must conclude an agreement with the third party as the data recipient prior to transferring the data, in which the arrangement of the data provision is regulated in accordance with Article 6 Data Act and taking into account the restrictions in Article 6 (2) Data Act. The Contractor is entitled to implement technical protective measures in accordance with Article 11 Data Act in order to prevent unauthorized access to data and to ensure compliance with the agreement with the third party. The

Contractor is entitled to demand reasonable and non-discriminatory consideration from the third party for the provision of the data.

5. SHARING OF DATA BETWEEN COMPANIES

If the Contractor is legally obliged (including under the Data Act) to share data with other companies, it must ensure that the conditions set out in Chapter III Data Act are complied with.

6. INFORMATION ON DATA HANDLING

Information from the Contractor on the handling of data in accordance with this Data License Agreement can be found in [Appendix 1](#).

7. TECHNICAL PROTECTION MEASURES

- 7.1 The Contractor has taken appropriate technical and organizational measures in accordance with Article 11 Data Act to prevent unauthorized access to data, including metadata.
- 7.2 The technical and organizational measures are subject to technical progress and further development. The Contractor is entitled to implement alternative adequate measures, provided that the security level of the specified measures is not compromised.
- 7.3 The Contractor shall only employ persons to process the data who have committed to themselves to confidentiality or who are subject to an appropriate legal duty of confidentiality.
- 7.4 The Contractor has appointed a Chief Information Security Officer (CISO). The current CISO can be reached at:

idem telematics GmbH
Standort Ulm
Riedweg 5
89081 Ulm
Bundesrepublik Deutschland
E-Mail: ciso@idemtelematics.com

- 7.5 The Contractor regularly checks its data processing procedures and systems for compliance with legal requirements and documents checks. Upon request, the Contractor shall provide the Customer with the documentation as proof of adequate safeguards.
- 7.6 The Contractor shall inform the Customer of any suspected data breaches and of any control actions and measures taken by the supervisory authority.

8. SUBCONTRACTORS

- 8.1 The Contractor is entitled to use subcontractors. Upon request, the Contractor shall inform the client about the subcontractors used.
- 8.2 The Contractor must structure orders to subcontractors in such a way that they comply with the requirements Data Act.

9. TERM OF THE DATA LICENSE AGREEMENT, TERMINATION

- 9.1 This Data License Agreement comes into force upon the conclusion of the Service Agreement and is concluded for an indefinite period.
- 9.2 Upon termination of the Service Agreement, this Data License Agreement shall end at the same time.
- 9.3 The Contractor's right to use the data generated during the term of the Data License Agreement shall remain unaffected.
- 9.4 The right of both parties to terminate the Data License Agreement at any time for good cause without notice remains unaffected. Good cause shall be deemed to exist in particular if one party culpably violates an essential obligation under this Data License Agreement and it is therefore no longer reasonable for the terminating party to adhere to its Data License Agreement.

10. CONFIDENTIALITY

The obligation to maintain confidentiality is governed by the Service Agreement or separate confidentiality agreement concluded separately between the parties, with the provision that the Contractor's right of use with regard to the data remains unaffected.

11. FINAL PROVISION, WRITTEN FORM REQUIREMENT, CHOICE OF LAW, PLACE OF JURISDICTION

- 11.1 This Data License Agreement contains all agreements between the parties with regard to the subject matter of the Data License Agreement. There are no verbal or written agreements outside of this Data License Agreement. This Data License Agreement replaces and supersedes all previous verbal and written agreements between the parties with regard to the subject matter of the Data License Agreement upon commencement of the Data License Agreement.
- 11.2 Any side agreements or amendments to this Data License Agreement - including this written form clause - must be made in writing, which may also be in electronic format.
- 11.3 References to laws, regulations, documents and annexes apply, unless expressly stated otherwise, to the laws, regulations, documents and annexes in their current valid version, i.e. including any amendments made after the date of the Data License Agreement.

- 11.4 The annex is an integral part of this Data License Agreement. In the event of a conflict between the provisions of the actual Data License Agreement text and its annex, the provisions of the Data License Agreement text shall prevail. However, mandatory statutory provisions shall remain unaffected by this.
- 11.5 This Data License Agreement is governed by the law of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods (CISG). The international place of jurisdiction is the Federal Republic of Germany. The local place of jurisdiction is Munich.
- 11.6 Should individual provisions of this Data License Agreement be or become invalid or unenforceable, this shall not affect the validity of the remaining provision. In such a case, the parties undertake to replace the invalid or unenforceable provision with one that comes as close as possible to the intended purpose in a legally permissible manner. The same applies to loopholes in the provisions.

IDEM TELEMATICS GMBH

Contractor in Print: idem telematics GmbH

Place: Munich

Date: 05 February 2026

Signature:


(Thomas Piller, Managing Director)

Appendix User information

A. Connected products

1. Type, format and estimated scope of the product data (Article 3 (2) (a) Data Act)

- Data structures: Attribute-value pairs of sensor data in accordance with Section B.1, as well as relational schemas for storing master data (vehicles, users, user groups, etc.)
- Data formats:
 - Master data in SQL database
 - Movement data as JSON structures in a column-organized ADX database
- Vocabularies: A mixture of industry-specific and generally accepted terms that enable precise communication and data interpretation
- Classification systems:
 - Master data
 - Movement data
- Taxonomies and code lists:
 - Master data: Relational schemas
 - Transaction data: Technically organized data groups such as FMS data, EBS data, etc.

2. Is the connected product capable of generating data continuously and in real-time (Article 3 (2) (b) Data Act)?

yes
 no

3. Is the connected product capable of storing data on-device or remote server, including the intended storage period (Article 3 (2) (c) Data Act)?

yes; *Intended storage period depending on customer contract: 18 months or longer, up to 10 years*
 no

4. Information on how the user can access, retrieve or, where applicable, delete the data, including the technical means for doing so, as well as the relevant terms of use and quality of service (Article 3 (2) (d) Data Act)

Access is via a portal or a technically structured AP. Direct access to the database by the user is not possible.

B. Provision of a related service

1. The type, estimated scope and frequency of collection of the product data that the potential data holder is likely to receive and, where applicable, the modalities by which the user can access or retrieve such data, including the modalities of the future data holder with regard to the storage and retention period of data (Article 3 (3) (a) Data Act).

1. Types of data:

- Position data
- Sensor data
- Vehicle data
- User interaction data (via an app)

2. Scope and transmission interval:

- Data vectors vectors with 1 to 200 data points
- Event-related
- Regularly with a maximum frequency of 1/min

3. Access options:

- Via a portal
- Via an app
- Via an API

4. Storage and retention period

- Storage in database
- Retention in accordance with end customer contract for 18 months or longer, up to 10 years

2. Type and estimated volume of the connected service data to be generated, as well as the methods by which the user can access or retrieve this data, including the methods of the future data holder with regard to the storage and retention period of data (Article 3 (3) (b) Data Act).

1. Types of data:

- Location data
- Sensor data
- Vehicle data
- User interaction data (via an app)

2. Scope and transmission interval:

- Data vectors vectors with 1 to 200 data points
- Event-related
- Regularly with a maximum frequency of 1/min

3. Access options:

- Via a portal
- Via an app
- Via an API

4. Storage and retention period:

- Storage in database

- Retention in accordance with end customer agreement for 18 months or longer, up to 10 years
3. Indication of whether the potential data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user (Article 3 (3) (c) Data Act).

In accordance with Art. 3 (3) (c) Data Act, the potential data holder expects to use readily available data themselves. The purposes for which this data is to be used include product improvement and the generation of new offers and services. The data holder also intends to allow one or more third parties to use the data for the purposes agreed with the user.

4. Identity of the potential data controller, e.g. its trading name and the address of the place where it is established, as well as, where applicable, other data processing parties (Article 3 (3) (d) Data Act).

idem telematics GmbH
Lazarettstraße 4
80636 Munich
Munich District Court HRB 154698

5. Means of communication through which the potential data holder can be contacted and communicated quickly and efficiently (Article 3 (3) (e) Data Act).

e-mail to: support@idemtelematics.com

6. Information on how the user can request the data to be transferred to a third party and how they can terminate the data transfer if necessary (Article 3 (3) (f) Data Act).

e-mail to: support@idemtelematics.com

7. The user's right to lodge a complaint with the competent authority referred to Article 37 Data Act regarding a breach of any of the provisions of this chapter (Art. 3 (3) (g) Data Act).

8. Indication of whether a potential data holder is the holder of trade secrets contained in the data that is accessible from the connected product or generated during the provision of a related service, and, if the potential data holder is not the holder of trade secrets, the identity of the trade secret holder (Article 3 (3) (h) Data Act).

The generated data is the trade secret of the data holder.

9. Duration of the contract between the user and the potential data holder as well as the terms for the early termination of such a contract (Article 3 (3) (i) Data Act).

In accordance with individual agreement entered into with the data holder.