Goldhofer »LINK«

This document contains both, the document for the Agreement on the Processing of Personal Data (DPA) and the Privacy Policy Agreement for the “Goldhofer LINK” DataPortal.

Please read both documents carefully.
To be able to use the Goldhofer »LINK« service, you must confirm these documents after having read them, provided that you agree with them.

1. **Agreement On the Processing of Personal Data (DPA)**
   Agreement on the Commissioned Processing in Accordance with Art. 28 GDPR

2. **Privacy Policy for the „Goldhofer Link“-DataPortal**

Agreement
On the Processing of Personal Data

- hereinafter referred to as “DPA“ -

between

The Customer

- hereinafter referred to as “**Customer**“ or “Responsible Party“-

and

Goldhofer Aktiengesellschaft
Donaustraße 95
87700 Memmingen

- hereinafter referred to as “**Contractor**“ or ”Processor“ -

Referred individually or commonly as “**Party**“ and/or „**Parties**“

1 Begriffsbestimmungen

For the purposes of this DP-Agreement, the term

(1) **"Processor"** refers to a natural or legal entity, public authority, agency, or other body that processes Personal Data on behalf of the Controller; "Processor" refers to the Contractor designated as "Processor" in the foregoing.

(2) "**Third Party**" refers to a natural or legal entity, public authority, agency or other body, excluding the Data Subject, the Controller, the Processor and the persons who are authorized to process the Personal Data under the direct responsibility of the Controller or the Processor;

(3) „**Main Agreement**": The contract for the provision of GOLDHOFER >>LINK<< Services, including the "Terms and Conditions for the Use of GOLDHOFER >>LINK<< Services".

(4) The "**Controller**" is the natural person or legal entity, public authority, agency or other body who alone or jointly with others determines the purpose and means of processing personal data; "Controller" means the Party referred to as "Controller" in the foregoing, which alone determines the purposes and means of the processing of Personal Data hereunder in this DPA.

(5) "**Processing**" means any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(6) "**Personal Data**" refers to any information relating to an identified or identifiable natural person (hereinafter referred to as "Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, an online identifier, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity of this natural entity.

(7) "**Other Processor or Subprocessor**" refers to the contractor assigned by the processor to carry out certain processing activities on behalf of the controller;

(8) "**Sub-Subprocessor**" refers to the agreement partner of the Other Processor or Subprocessor assigned by the latter to carry out certain processing activities within the scope of this DPA.

2 SUBJECT MATTER THE AGREEMENT, LEGAL BASIS

(1) **[Subject matter the Agreement]** Subject matter the Agreement is the processing of personal data by the Processor on behalf of the Controller on the latter's behalf and according to the Controller's instructions in connection with the provision of GOLDHOFER >>LINK<< Services in addition to the main contract of the parties.

(2) **[Processing Details]** The subject matter of this DPA and duration of the assignment, the nature and purpose of the processing, the type of personal data and the categories of Data Subjects are determined from the Main Agreement in conjunction with Annex 1 of this contract. The Controller grants Processor access to the personal data of the Controller as specified in **Annex 1** of this DPA.

(3) **[Maintenance, Verification]** If the Processor performs services for the Controller in the area of maintenance/remote maintenance/IT troubleshooting where access to the Controller's personal

data is not intended but cannot be ruled out, this Agreement applies accordingly. Any details relating to data processing are defined among the Parties in **Annex 1** of this DPA.

3 RIGHTS AND OBLIGATIONS OF THE CONTROLLER

(1) **[Permissibility of data processing]** The Controller is solely responsible for evaluating the permissibility of data processing and for safeguarding the rights of the Data Subjects. Within its area of responsibility, the Controller must ensure that the legally required prerequisites have been established (e.g. by obtaining declarations of consent) so that the Processor may provide the agreed services without violating the law to this extent as well.

(2) **[Instructions]** The Processor shall only process personal data on the basis of documented instructions from the Controller, also with regard to transferring personal data to a third country or an international organization, provided that it is not legally bound to do so by the law of the Union or the Member States to which the Processor is subject. In such case, the Processor will notify the Controller of such legal requirements prior to the data being processed, unless the relevant law prohibits a notification of this kind to safeguard an important public interest.

(3) **[Compensation for added services]** Insofar as a change in services has been agreed in the Main Agreement, such change in services has priority over the provisions of this paragraph. Unless an agreement on changes to services has been made in the Main Agreement, any instructions and measures representing a deviation from the services specified in this DPA or in the Main Agreement are treated as a request for a change to services. Unless expressly agreed otherwise, additional instructions and measures over and above the contractually agreed services are to be paid for separately should the Processor incur additional expense. In such case, the contracting parties will reach a separate agreement on an appropriate compensation.

Unless expressly agreed otherwise, the Processor my demand separate remuneration for support and services pursuant to Clause 3 (5), (6) and Clause 4 (4), (5) (7), (8, sentence 2 therein), (9), (10, sentence 2 therein), (11) of this DPA.

(4) **[Verification by the Processor]** It is at the Processor´s discretion to demonstrate the obligations under this DPA, in particular the technical-organizational measures (Clause 5) and measures not solely related to the specific contract, have been adequately implemented by providing the following documented verficiation:

- Compliance with approved rules;
- Certification in accordance with an approved certification procedure;
- Up-to-date attestations, reports or excerpts from reports by independent bodies (e.g. auditors, auditing);
- Adequate certification by IT security or data protection audit;
- Processor´s self-declaration.

(5) **[Audits, inspections]** The Controller may, at its own expense, monitor the Processor's compliance with the provisions on data protection and the obligations set forth in this DPA by obtaining information and requesting the documents listed in Clause 3 (4) from the Processor in relation to the processing that concerns it. The Controller will primarily verify whether the verification option allowed in sentence 1 of this paragraph is adequate. Moreover, the Controller may, at its own expense, monitor compliance with the provisions on data protection on site. The Controller may either itself conduct the audits or have them conducted by a commissioned third party at its own expense. Any person or third party entrusted by the Controller with an audit must be demonstrably obligated to maintain confidentiality at the time of commission. The Processor will be given appropriate advance notice of the persons or third parties entrusted by the Controller

with the audit and will be provided with the opportunity to verify their qualification to conduct such audits. A third party within the meaning of this paragraph may not represent competitors of the Processor. The Controller will provide reasonable notice of audits and will respect business operations and operational procedures when conducting such audits.

(6) **[Support by the Controller]** The Controller undertakes, with regard to the processing concerning it, to promptly and fully inform the Processor of any suspected data breaches and/or other irregularities in the processing of the personal data. As regards the data processing by the Controller, the Controller will promptly and extensively support the Processor in the review of potential violations and in the defense against claims by Data Subjects or a third party and against any sanctions by supervisory authorities.

4 RIGHTS AND OBLIGATIONS OF THE PROCESSOR

(1) **[Data processing]** The Processor is to process the Personal Data within the scope of the Agreement entered into and as instructed by the Controller in accordance with the provisions of Clause 3 (2). The Processor assures that the employees involved in the processing of Controller's personal data and other persons working for the Processor process such data only on the basis of the Controller's instructions, unless they are required to process such data under Union or Member State law.

(2) **[Data Protection Officer]** The Processor undertakes to appoint an independent, competent and reliable data protection officer if required by the applicable legislation of the European Union or the Member State to which the Processor is subject.

(3) **[Place of performance]** The Processor will provide the contractual services within the European Union (EU) or the European Economic Area (EEA) or in a third country. This similarly applies to any Subprocessors and Sub-subprocessors. The service locations agreed upon at the time the agreement was awarded are shown in **Annex 1, 3 and 4** of this DPA.

(4) **[Reporting of incidents]** The Processor must inform the Controller without undue delay of any severe operational disruptions, suspected data protection breaches and/or other irregularities in the processing of personal data.

(5) **[Exercise of Data Subject Rights**] Depending on the type of processing, the Processor undertakes to support the Controller in its obligation to respond to requests to exercise Data Subject rights using appropriate technical and organizational measures where possible. If needed, the contracting parties will coordinate the content and scope of any support services provided by the Processor.
Should a Data Subject contact the Processor directly for the purpose of asserting a Data Subject right, the Processor will promptly forward the inquiries made by the Data Subject to the Controller.

5 TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

(1) **[Technical organizational measures]** Both, the Controller and the Processor will implement appropriate technical and organizational measures to ensure a level of protection commensurate with the risk. Measures by the Processor and its Subprocessors that are deemed appropriate at this time are described in Annex 2 of this DPA. The Controller has assessed the technical and organizational measures in connection with any other measures to ensure an adequate level of protection. Such measures have been determined to be appropriate, as described in Annex 2.

(2) **[Verification and demonstration]** Clause 3 (4) and Clause 3 (5) apply to the verification and demonstration options.

6 CONFIDENTIALITY

The Processor undertakes to maintain confidentiality with respect to the processing of personal data as agreed herein.

7 SUBPROCESSOR

(1) **[Authority]** The Processor may use other Processors (Subprocessors and Sub-Subprocessors) to perform the duties outlined in this Agreement. Not deemed subprocessor relationships as understood by this provision are contracts that the Processor utilizes from third parties as an ancillary service to support the execution of the contract.

(2) **[Separate approval]** For the subprocessors listed in **Annex 3** of this DPA and the sub-subprocessors listed in **Annex 4** along with the areas of responsibility specified therein, the approval of the Controller is deemed to have been granted.

(3) **[General written authorization]** The Controller hereby grants the Processor general authorization for future use of other Processors (Subprocessor and Sub-subprocessors).

(4) **[Information in the event of changes]** The Processor undertakes to notify the Controller, in writing or by email, of any intended change in relation to the use or replacement of other Processors (Subprocessors and Sub-subprocessors) at least four (4) weeks before the intended change. That gives the Controller the opportunity to object to such changes within 14 days of having received such information from the Controller. The Controller will not refuse permission to include further Subprocessors and Sub-subprocessors without just cause.

(5) **[Processor's right of termination]** The Processor is entitled to an extraordinary right of termination of the main Agreement pursuant to the Main Agreement, or, in the event that such a right of termination has not been granted in the Main Agreement, an extraordinary right of termination of 4 weeks to the end of the month, if, in the opinion of the Processor, the Controller refuses to integrate the Subprocessor and/or Sub-subprocessor without just cause, or if it is not possible for the Processor to provide the service without the rejected Subprocessor and/or Sub-subprocessor.

(6) **[Selection, back-to-back agreement]** The Processor will choose subprocessors that provide sufficient guarantees that the appropriate technical and organizational measures agreed upon are implemented in a way that Data Processing is conducted pursuant to the requirements of the relevant applicable legal provisions. The Processor will conclude contractual agreements with Subprocessors that essentially conform to the contractual provisions of this Agreement. The Processor will establish the technical and organizational measures with the Subprocessor and monitor compliance with the agreed technical and organizational measures, prior to the start of the Data Processing and subsequently on a regular basis.

(7) **[Sub-subprocessors]** The commissioning of sub-subprocessors by the Processors is permitted in accordance with Clause 7 (1) to (6).

8 TERM OF THE AGREEMENT, TERMINATION

This Agreement is valid for the duration of the Main Agreement.

9 CONTACTING GOLDHOFER

Concerns regarding this DPA are to be addressed on the part of the processor to

GOLDHOFER Aktiengesellschaft
Donaustraße 95
87700 Memmingen
link@goldhofer.com or datenschutz@goldhofer.com

10 LIABILITY

Liability for damages caused by processing that does not comply with the GDPR and applicable data protection regulations shall be governed by the statutory provisions.

11 OTHER

(1) **[Effectiveness of the Agreement]** If any provision of this DPA is found to be ineffective, this will not affect the effectiveness of the remaining provisions.

(2) **[Amendments to the Agreement]** Amendments to the DPA and ancillary agreements must be made in writing (including in electronic form). This also applies to any change to the written form clause itself. Processor reserves the right to amend this DPA at any time if there is sufficient reason to do so. Factual reasons shall be deemed to exist in particular in the event of a change In the legal situation, supreme court rulings or market conditions. The Processor shall inform the Controller of the change in text form, stating the reasons, at least 4 weeks before it is scheduled to take effect. The Controller may object to the new terms and conditions no later than 2 (two) weeks before they are scheduled to take effect. If he does not object, his consent shall be deemed to have been granted. In the event of an objection by the person responsible, Goldhofer has the right to choose whether to continue the contract under the old conditions or to terminate the contract with effect from the date on which the new regulations come into force. Item 7 (Changes in the use of subcontracted processors) shall remain unaffected.

(3) **[Competent court]** The exclusive legal venue for all disputes arising from and in connection with this DPA is Memmingen, Germany. This is subject to any exclusive legal venue.

(4) **[Applicable law]** As regards applicable law and legal venue, the provisions of the Main Agreement apply.

(5) **[Precedence provision]** In the event of contradictions between the provisions of this Agreement and provisions of any other agreements, in particular the Main Agreement, the provisions of this DPA take precedence. In all other respects, the provisions of the Main Agreement remain unaffected and apply to this DPA accordingly.

Annexes:

The following annexes are an integral part of this Agreement:

Annex 1: Details of Data Processing

Annex 2: Technical and Organizational Security Measures

Annex 3: Approved Subprocessors

Annex 4: Approved Sub-subprocessors

Annex 1

Details of Data Processing

1. Subject Matter of Processing

The contract awarded by Client to Contractor includes the following work and/or services:

Provision of Goldhofer Telematic Services via the Goldhofer LINK data platform

2. Subject Matter of Processing

When accessing the data platform via the data portal, the following **personal data** is requested and stored from the user:

- First and last name
- E-Mail-Address
- Organizational unit
- Login times and source IP address
- User activity, such as selected time zone, language

Note: Goldhofer **does not** collect and process any special categories of personal data pursuant to Art. 9 GDPR or personal data about criminal convictions and criminal offenses pursuant to Art. 10 GDPR.

The data listed is collected:

- To facilitate and implement our services within the scope of Goldhofer Services, including support.

Data is processed for the purpose listed and is necessary for the provision, use and invoicing of our services.

If access to the Goldhofer LINK data portal has been activated and a subscription contract has been concluded and activated for the machine, the requested machines will be transferred, stored and made available. This may involve the following **machine data**:

- Machine parameters, such as oil pressure, tank level, battery level, speeds, diagnostic messages, threshold violations, maintenance requirements, next maintenance
- GPS data to determine the location and movement profile of a machine.

Note: Machine data only contains personal data if it includes information that can be used to identify persons (including but not limited to name, address, etc.). For such persons, the data relates to personal data.

Goldhofer explicitly emphasizes that the recorded machine data are purely technical in nature and that Goldhofer and the Subprocessors cannot trace them back to or associate them with a specific natural individual.

This also applies to **GPS data**: Without any additional information, this data cannot be assigned to a specific natural individual. Although Goldhofer tracks the position of a machine or vehicle with a high degree of accuracy, it does **not** store, process or manage information about the driver.

3. Service, Processing Purpose:

See above (Clause 1 and 2), Main Agreement and Annex 1 thereto.

4. Processing Location:

see Annex 2, 3 and 4

Annex 2

Technical and Organizational Security Measures

The Processor uses the technical infrastructure provided by the Subprocessor Proemion to offer the services to the Controller (see Annex 3). The Processor and Subprocessor have agreed on the following technical and organizational measures for the provision of the services.

1. Confidentiality Pursuant to Art. 32 (1b) GDPR

1.1. Access authorization

Measures suitable for preventing unauthorized persons from gaining access to data processing systems used to process or use personal data.

Technical measures	Organizational measures
☒ Alarm system	☒ Key rules/list
☒ Biometric access locks	☒ Reception
☒ Chip card/transponder systems	☒ Visitor monitoring/logging
☒ Security locks	☒ Care when selecting security staff
	☒ Care in the selection of cleaning services

1.2. Access control

Measures suitable to prevent data processing systems (computers) from being used by unauthorized persons.

Technical measures	Organizational measures
☒ Login with user name and password	☒ Manage user authorizations
☒ Firewall	☒ Creating user profiles
☒ Anti-virus software server	☒ Central password assignment
☒ Anti-virus software clients	☒ “Secure password” guidelines
☒ Intrusion detection systems	☒ General data protection and/or security guidelines
☒ Mobile device management	
☒ Use of VPN for remote access	
☒ BIOS protection (separate password)	
☒ Automatic desktop lock	
☒ Notebook/tablet encryption	

1.3. Access authorization

Measures ensuring that those authorized to use a data processing system can only access the data they are authorized to access, and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical measures	Organizational measures
☒ File shredder (at least level 3, cross cut)	☒ Use of authorization concepts
☒ Third-party file shredder (esp. DIN 66399)	☒ Minimum number of administrators

☒ Physical deletion of data carriers	☒ Data protection safe

1.4. Separation control

Measures ensuring that data collected for different purposes can only be processed separately. For example, this may ensured be using logical and physical spearation of the data.

Technical measures	Organizational measures
☒ Separation of production and test environment	☒ Controlled via authorization concept
☒ Physical separation (systems/databases/data carriers	☒ Definition of database rights

2. Integrity Pursuant to Art. 32 Abs. (1b) GDPR

2.1. Transmission check

Measures ensuring that personal data cannot be read, copied, changed or removed unauthorized during electronic transfer or during the transport thereof or the storage thereof on data carriers, and that it can be checked and determined at which areas a transfer of personal data is provided for by a data transfer installation.

Technical measures	Organizational measures
☒ Use of VPN	
☒ Logging of accesses and data retrievals	

2.2. Input control

Measures ensuring that it can be verified and determined retroactively whether and by whom personal data was entered, changed or removed in data processing systems.

Technical measures	Organizational measures
☒ Manual or automated check of the logs	☒ Ability to track the input, change and deletion of data by individual user names (not user groups)

3. Availability and Resilience Pursuant to Art. 32 (1b) GDPR

3.1. Availability control

Measures ensuring that personal data are protected against random destruction or loss.

Technical measures	Organizational measures
☒ Fire and smoke alarm systems	☒ Backup & recovery concept
☒ Server room monitoring temperature and humidity	☒ Regular tests for data recovery and results logging
☒ Air conditioned server room	☒ Storing the backup media at a safe location outside of the server room
☒ Server extinguishing system	☒ Backup process control
☒ UPS	
☒ Safety power strip server room	
☒ RAID system/hard disk mirroring	

4. Process for Regular Review, Assessment and Evaluation Pursuant to Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

4.1. Data protection management

Technical measures	Organizational measures
☒ The effectiveness of the technical protection measures is reviewed at least once a year	☒ Staff trained and obligated to confidentiality/data protection
	☒ Regular awareness training for staff, at least once a year

4.2. Incident and response

Support in responding to security violations

Technical measures	Organizational measures
☒ Use of firewalls and regular updates	
☒ Use of spam filters and regular updates	
☒ Use of virus scanners and regular updates	
☒ Intrusion detection system (IDS)	
☒ Intrusion prevention system (IPS)	

4.3. Privacy-friendly Default Setting (Art. 25 (2) GDPR)

Technical measures	Organizational measures
☒ No more personal data is collected than is necessary for the respective purpose	
☒ Technical measures ensuring easy exercise of data subject rights	

4.4. Order control (outsourcing to a third party)

Technical measures	Organizational measures
	☒ Obligation of the contractor's staff to maintain data secrecy
	☒ Selecting the contractor based on due diligence criteria
	☒ Rules on the use of additional subprocessors

Annex 3

Approved Subprocessors

Information on Subprocessors/Services/Processing Locations

Special Authorization

The Processor can utilize the following subprocessor for the following services/at the following processing locations:

Subprocessor: *(Proemion GmbH, Donaustrasse 14, 36041 Fulda, Germany, +49 661 9490 - 0)*
Services: Data portal operator

Annex 4

Approved Sub-subprocessors

Information on Sub-subprocessors/Services/Processing Locations

Special Authorization
The following sub-subprocessors may be utilized for the following services/at the following processing locations:

Company	Services	Contact	Purpose	Personal data categories
Amazon Web Services	Provision of cloud computing/data routes	Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109 USA	Data platform operation	Device identification data and traffic data (IP addresses, MAC addresses, web protocols, browser agents)
Amplitude	Web User Tracking	Amplitude, Inc. 631 Howard Street, Floor 5 San Francisco, CA 94105 USA	Data platform operation	Device identification data and traffic data (user ID, web protocols, browser agents) utilization of functions
Atlassian.com	Jira Confluence Statuspage Opsgenie	Atlassian.com Singel 236 1016 AB Amsterdam The Netherlands	Support services	Device identification data and traffic data (IP addresses, MAC addresses, web protocols, browser agents) User/login data Names and contact data (company-related), data from customer/user requests
Box.com	Cloud storage	Box Deutschland GmbH Neuturmstrasse 5 80331 Munich Germany	Support services	Device identification data and traffic data (e.g. IP addresses, MAC addresses, web protocols, browser agents), user/login data
Sentry	Error tracking and performance monitoring	Functional Software, Inc. dba Sentry 45 Fremont Street, 8th Floor San Francisco, CA 94105 USA	Data platform operation	Device identification data and traffic data (e.g. IP addresses, MAC addresses, web protocols, browser agents), utilization of data platform functions

GitHub	Software development platform	GitHub BV Vijzelstraat 68-72 1017 HL Amsterdam The Netherlands	Support in the development of the data platform	Names and contact data (company-related), data from customer/user inquiries
Google Ireland Ltd.	Google Maps Google Cloud Services	Gordon House Barow Street Dublin 4 Ireland	Data platform operation	Device identification data and traffic data (e.g. IP addresses, MAC addresses, web protocols, browser agents), location data
Mapbox	Maps	Mappbox, Inc. 740 15th Street NW, 5th Floor, Washington DC 20005 USA	Data platform operation	Device identification data and traffic data (e.g. IP addresses, MAC addresses, web protocols, browser agents), location data
Microsoft Azure EU	Office 365 Cloud Computing SharePoint OneDrive	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Data platform operation	Device identification data and traffic data (IP addresses, MAC addresses, web protocols, browser agent) Names and contact data (company-related), data from customer/user requests
Mixpanel	Web User Tracking	Mixpanel Inc. One Front Street, 28th Floor, San Francisco, CA 94111 USA	Data platform operation	Device identification data and traffic data (user ID, web protocols, browser agents) utilization of data portal functions
Salesforce.com	CRM (sales, support)	Salesforce Germany GmbH Erika-Mann-Str. 31 80636 Munich Germany	Support services	Names and contact data (company-related), payment data from project and contract processing
Segment	Service analysis	Segment.io Inc. 100 California Street, Suite 700 San Francisco, CA 94111 USA	Data platform operation	Device identification data and traffic data (e.g. IP addresses, MAC addresses, web protocols, browser agents), utilization of data portal functions,

ProductBoard	Surveytools (Productboard and Sentry)	ProductBoard, Inc. 612 Howard St, 4th Floor, San Francisco, CA 94105 USA	Data platform operation	Device identification data and traffic data (user ID, web protocols, browser agents) utilization of data portal functions, user feedback
Notion.so	Platform for notes and tasks	Notion Labs, Inc. 548 Market St # 74567, San Francisco, CA USA	Support services	Names and contact data (company-related), data from customer/user inquiries
SupportLogic	Support platform	SupportLogic, Inc. 356 Santana Row, Suite 1000, Santa Clara, CA 95128 USA	Support services	Names and contact data (company-related), data from customer/user inquiries
Outreach	Sales platform	Outreach Corporation 333 Elliot Ave W, Suite 500 Seattle, WA 98119 USA	Support services	Names and contact data (company-related), payment data from project and contract processing

Privacy Policy for the “Goldhofer Link”-Data Portal

Introduction and Scope of this Privacy Policy

Goldhofer (hereinafter referred to as **Goldhofer**) grants its customers access to the GOLDHOFER Link Services, a portal on which customers can view and manage data of their vehicle fleet (hereinafter **data portal**). Customers (hereinafter referred to as **customer**) and their employees (hereinafter referred to as **user** and / or **you** and / or **data subject**) can log into this data portal. During this process and during the period of use, personal data of the user is processed. In the following, we will inform you about how your personal data is processed in connection with the use of the data portal.

Please note that Goldhofer is not the so-called data controller in this respect. The data controller is the customer and thus, if you are an employee of the customer, your employer. Goldhofer is the processor on behalf of the customer and only processes your personal data on customer’s instruction. For the provision of the data portal, Goldhofer uses the services of Proemion GmbH as a subcontractor (cf. clause III.). This Privacy Policy is only in addition to the Privacy Policy that customer may provide to you.

If you have any questions regarding data protection and any supplementary questions regarding this data protection declaration, please contact your employer. Alternatively, we are happy to pass on your questions on data protection in connection with the use of the data portal to your employer. For this purpose, please use the contact address given in clause I.

I. Data controller; contact details

The controller, pursuant to the EU General Data Protection Regulations and various national data protection provisions of the member states of the European Union and other legal data privacy policies, is the customer / your employer (hereinafter jointly referred to as **controller**). For your issues and questions regarding data protection laws as well as for the assertion of your rights as the data subject please contact controller, alternatively please contact Goldhofer under the following contact details:

Company: Goldhofer AG
Street: Donaustrasse 95
City: Memmingen
Country: Germany
Email: info@goldhofer.com
Website: www.goldhofer.com

II. Data processing in general

1. Scope of personal data processing

Goldhofer processes your personal information (data) solely to the extent necessary to operate the Data portal.

2. Legal basis for the processing of personal data

The legal basis of the processing by the customer (and subsequently by Goldhofer as processor and Proemion as sub-processor) is, depending on the individual situation at the customer and the categories of data that are processed:

- Art. 6 para. 1 lit. b), 88 DSGVO in conjunction with § 26 para. 1 BDSG (German Federal Data Protection Act) and / or
- Art. 88 DSGVO in conjunction with § 26 para. 4 BDSG in conjunction with a company agreement and / or
- Art. 6 para. 1 lit. f) DSGVO and / or
- § 25 para. 2 TTDSG (German Telecommunications Telemedia Data Protection Act).

3. Deleting data and data retention

Personal information regarding the data subject will be deleted or blocked once the purpose for storing no longer applies. Furthermore, data may be stored if such storage has been stipulated by the European or national legislature in EU regulations, laws or other provisions under which the controller is bound. Data shall also be blocked or deleted in the event a storage period, as stipulated in the aforementioned provisions, expires, unless a need for extended storage of data arises, i.e., in order to conclude a contract or meet contractual obligations.

4. Proemion as technical operator of the Data Portal

The Data portalis provided as Software as a Service (SaaS) by Proemion GmbH, Donaustraße 14, 36043 Fulda. In this respect, Proemion acts as a subcontracted processor on the basis of a DPA concluded between Goldhofer (processor) and Proemion (sub-processor).

The Data portal is a service that can be used to process telematics data. The data entered / transmitted by customer / you for the purpose of processing will be stored on Proemion's servers. Possible data categories are:

(1) Company data
(2) vehicle or machine information
(3) GPS data
(4) user profile data (First and last name, log-in data, e-mail address, IP address)
(5) CU data.

III. Provision of the data portal and creating log-files

1. Description and scope of data processing

Whenever the Data portal Login page is accessed, the system automatically collects data and information from the computer system of the visiting party. The following data is collected:

(1) Information regarding the browser type and current browser version
(2) The user's operating system
(3) The user's internet service provider
(4) The user's IP address
(5) Access date and time
(6) Websites from which the user's computer system accesses our website

(7) Websites which are accessed by the user's computer system via our website
(8) User profile data (cf. Clause IV)
(9) Information about the operations (and their parameters) performed by the user

The data is also stored in the log files of our computer system. This data is not stored together with other personal user data.

2. Purpose of data processing

The temporary storage of the IP address by the computer system is necessary to enable the Data portal to be transmitted to the user's computer. For this purpose, the user's IP address must remain stored for the duration of the session. The storage in log files is necessary to ensure Data portal operation. We also use the data to optimize the Data portal and to ensure the security of our information technology systems

3. Data Retention

The data shall be deleted once these are no longer required for their intended purpose. When a collection of data occurs for the purpose of providing the Data Portal, ending the respective session results in such data being deleted. In case of storage of data in application logs, we delete it after 40 days at the latest. In case of storage of data in access logs, we delete it after 60 days at the latest. Additional data backup is available, if it is necessary, in particular, for error analyses or product improvements. In this event, the personal information of the users will be deleted or altered, making it impossible to identify the contacting client.

IV. Data processing in connection with the registration / log-in

1. Description and scope of data processing

On the DataPortal it is possible to log in by entering a user name and a password. The registration and creation of the user data is carried out centrally by an administrator. The following data is usually stored by you during registration:

(1) Name
(2) First name
(3) Email
(4) Organization
(5) Language
(6) DataPortal permissions

An activity log is created for logged-in users.

2. Purpose of data processing

Registration of the user is necessary for the fulfilment of a contract with the user or for the implementation of pre-contractual measures. The login is necessary to ensure secure access to the data in the Data Portal. Furthermore, the user-specific login assigns the user rights within the Data portal and allows user settings to be saved.

3. Data Retention

The data shall be deleted once these are no longer required for their intended purpose. This is the case for the data stored during the registration process for the fulfilment of a contract or for the implementation of pre-contractual measures if the data is no longer required for the implementation of the contract. Even after the conclusion of the contract, there may be a need to store personal data of the contractual partner in order to fulfil contractual or legal obligations.

4. Options regarding deletion

You can have the data stored about you changed at any time. As a user, you have the option to cancel your registration at any time. However, please note that in this case, the telematics services may no longer be fully usable. The end user must send a request to delete the account or change data to the controller. The controller will forward the requests for deletion or data modification to Proemion Technical Support, by phone or via the support form posted on Proemion's homepage. If the data is required for the fulfilment of a contract or for the implementation of pre-contractual measures, early deletion of the data is only possible insofar as contractual or legal obligations do not prevent deletion.

V. Cookies

1. Description and scope of data processing

The Data portal uses cookies. Cookies are small data files that are stored on your computer or other device when you visit a website. Once a user visits the Data Portal, a cookie may be stored on the user's operating system. This cookie contains a characteristic string of characters which uniquely identifies the browser on subsequent visits to the Data Portal. Cookies are used to improve the Data portal and enhance the user experience. Several of the Data portal features require visitor browser identification with each new page to navigate around the Data Portal. Cookies and local browser storage are required for the following applications:

(1) Log-in information
(2) Language settings
(3) Track your searches
(4) User preferences
(5) Theming
(6) Timezone
(7) Last visited page on Data Portal

2. Purpose of processing data

The purpose of using technically essential cookies is to simplify your visit to our Data Portal. Several features of our Data portalrequire the use of cookies. It is essential that the browser is recognized even in the event of navigating to a new page. User data collected for technically essential cookies are not used to create user profiles.

3. Data Retention, restricting and deleting cookies

Cookies are stored on the user's computer and transmitted to our Data Portal. Therefore, you as a user have full control regarding the use of cookies. By changing the settings in your internet browser, you can deactivate or limit the placement of cookies. Previously stored cookies can be deleted at

any time. This can also be performed automatically. In the event cookies are deactivated for our Data Portal, this may result that not all features of our Data portalcan be used to their full extent.

VI. Use of sub-contractors by Proemion

Proemion will use the following subcontractors for the provision of the services and the data portal and insofar transfer personal data to these subcontractors.

In order to ensure a continuously updated overview of the services and subcontractors used, the operator of the DataPortal provides an up-to-date overview with the required information on the subprocessors used available at the following link https://dataportal.proemion.com/#!/subprocessors. This overview will be updated regularly if the use of the services changes.

Some of the subcontractors process the data in so-called third countries where there is no level of data protection equivalent to that of the EU according to the provisions of the GDPR. Proemion has concluded standard contractual clauses with the subcontractors to legitimise the transfer of data.

VII. Your Rights

You have the following rights towards the customer / your employer as the data controller. Goldhofer as a processor will support the customer in responding to and fulfilling the rights asserted by you to the best of its ability and within applicable laws.

1. The right to access of information

You may request confirmation from the controller regarding whether personal data on your behalf is being processed by him. In the event of such processing, you may request the following information from the controller:

(1) the purpose for which the personal data are being processed;
(2) the categories of personally identifying information being processed;
(3) the recipients or categories of recipients to whom the personal data regarding oneself has been or will be disclosed;
(4) the intended duration of personal data storage regarding oneself or, in the event specific details are not possible, criteria for determining the retention period;
(5) the right to exercise the rectification or erasure of personal data regarding oneself, a right to limit processing by the controller and a right to object to such processing;
(6) the right of appeal with a supervisory authority;
(7) all available information regarding origin of the data, in the event the personally identifiable data was not collected from the data subject;
(8) the existence of an automated data processor, including profiling, in accordance with Article 22, Section 1 and 4 of the GDPR and, at least in these events, conclusive information regarding the logic involved as well as the scope and intended consequences of such processing for the data subject.

2. The right to rectification

You have a right to rectification and/or completion by the controller in the event of inaccurate or incomplete processing of your personal data. The party responsible is required to correct the data without delay.

3. The right to restrict processing

You may request the restriction of personal data processing regarding yourself, under the following circumstances:

(1) when you deny the accuracy of your personally identifying data for a time period in which the controller is able to verify the accuracy of the personal data;
(2) processing proves to be unlawful and you object to the removal of the personal data and request instead the restriction of personal data processing;
(3) the controller no longer requires the personal data for the purpose of processing, but you need them for the establishment, exercise or defence of legal claims, or
(4) in the event you have objected to the processing pursuant to Article 21, Section 1 of the GDPR and it has not yet been determined whether the legitimate grounds of the controller override your interests.

In the event the processing of your personal data has been restricted, such data may, with the exception of being stored, be processed only with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal individual or for reasons of substantial public interest of the European Union or a member state.
In the event a limitation of the processing restriction has been imposed in accordance with the above circumstances, you will be informed by the controller before the restriction is lifted.

4. The right to request deletion

a) Obligation to delete

You may request the controller to delete your personal data without unreasonable delay, and the controller is obligated to delete such data without unreasonable delay in the event one of the following reasons apply:

(1) Your personal data is no longer necessary for the purpose for which they were collected or otherwise processed.
(2) You revoke your consent for which the processing was based pursuant to Article 6, Section 1(a) or Article 9, Section 2(a) of the GDPR and there remains no other legal basis for the processing of data.
(3) You object to the processing pursuant to Article 21, Section 1 of the GDPR and there remain no overriding legitimate grounds for the processing, or you object to the processing pursuant to Article 21, Section 2 of the GDPR.
(4) The personal data regarding your information have been processed unlawfully.
(5) The removal of the personal data concerning you is required for compliance with a legal obligation under European Union or member state law to which the controller is subject.
(6) Your personal data has been collected in connection with a Society Information Services offer pursuant to Article 8, Section 1 of the GDPR.

b) Exceptions

The right to deletion does not exist insofar as the processing is required

(1) to exercise the right to freedom of expression and information;

(2) to comply with a legal obligation which requires processing under European Union or Member State law to which the controller is subject, or for the performance of a task carried out in the interest of the public or in the exercise of official authority vested in the controller;
(3) for reasons of public interest in the scope of public health in accordance with Article 9, Section 2(h) and (i) and Article 9, Section 3 of the GDPR;
(4) For archival purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to Article 89, Section 1 of the GDPR, insofar as the right referred to in Part (a) is likely to render impossible or seriously prejudice the achievement of the purposes of such processing, or
(5) for the enforcement, exercise or defence of legal claims.

5. The right to be informed

In the event you have exercised the right to rectification, deletion or restriction of processing towards the controller, the controller is obligated to communicate this rectification or deletion of data to all recipients to whom the personal data in your regards have been disclosed, unless this proves impossible or involves a disproportionate effort.
You have the right to be informed in regards to these recipients by the controller.

6. The right to transferable data

You have the right to receive the personal data which you have provided to the controller in a structured, common and machine-readable format. In addition, you have the right to transmit this data to another controller without hindrance from the controller to whom the personal data was supplied, provided that

(1) the processing is based on consent pursuant to Article 6, Section 1(a) of the GDPR or Article 9, Section (a) of the GDPR or on a contract drawn pursuant to Article 6, Section 1(b) of the GDPR and
(2) the processing is carried out with the help of automated procedures.

In exercising this right, you also have the right to obtain those personal data concerning you, which get transferred directly from one controller to another controller, insofar as this is technically feasible. The right to data portability does not apply to processing of personal data required for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

7. Right to object

You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data relating to you which is carried out on the basis of Article 6, Section 1(e) or (f) of the GDPR. The controller shall no longer process the personal data concerning you unless it can demonstrate compelling legitimate grounds regarding the processing which override your interests, rights and freedom, or for the establishment, exercise or defence of legal claims.

8. Right to revoke ones' consent to the privacy policy

You have the right to revoke your consent under data protection law at any time. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of the consent until it is revoked.

9. Right to file a complaint with a regulatory authority

Without affecting any other administrative or judicial remedy, you have the right to file a complaint with a supervisory authority, in particular in the Member State of your residence, place of work or the place of the alleged infringement, in the event you consider the processing of personal data relating to you infringes the GDPR. The supervisory authority to which the complaint has been submitted shall inform the plaintiff of the status and outcome of the filed complaint, including the option of a judicial appeal pursuant to Article 78 of the GDPR.

VIII. SSL encryption

This site uses SSL encryption for security purposes and to protect the disclosure of confidential content, such as the inquiries you send to us as site operator. You will recognize an encrypted connection by the fact that the browser address bar changes from "http://" to "https://" and by the lock symbol in your browser tool bar. In the event SSL encryption is activated, the data you disclose to us cannot be read by third parties.