

Privacy Policy for the DataPortal

Name and address of the responsible party

The responsible party, pursuant to the EU General Data Protection Regulations and other national data protection laws of the member states as well as other data protection regulations, (hereinafter also referred to as "controller"), is:

Proemion GmbH
Donaustraße 14
36043 Fulda
Germany
+49 661 9490 - 0
info@proemion.com
www.proemion.com

Name and address of the Data Protection Officer

The responsible party appoints the following data protection officer (DPO):

BerisDa GmbH
Justus-Liebig-Str. 4
36093 Künzell
Germany
+49 661 29 69 80 90
datenschutz@proemion.com
www.berisda.de

I. General information on data processing

1. Scope of personal data processing

The responsible party collects and uses personal data of its users (hereinafter also referred to as "data subject" or "visitor") only insofar as this is necessary for the provision of a functioning DataPortal and for the presentation of the contents and services. The collection and processing of personal data of users for other purposes is generally only permitted with the consent of the user. An exception applies in those cases in which it is not possible to obtain consent in advance for factual reasons, the processing is carried out on the basis of pre-contractual or contractual measures, the processing of the data is permitted by legal regulations and/or there is a legitimate interest of the controller in the processing.

2. Legal basis for the processing of personal data

Insofar as the controller obtains the consent of the data subject for processing operations involving personal data, Article 6, para. 1 point a of the EU General Data Protection Regulation (GDPR) serves as the legal basis for the processing of personal data.

When processing personal data that is necessary for the performance of a contract to which the data subject is a party, Article 6, para. 1 point (b) of the GDPR serves as the legal basis. This also

applies to processing operations that are necessary for the performance of pre-contractual measures.

If processing of personal data is necessary for compliance with a legal obligation to which the controller is subject, Article 6, para. 1 point (c) of the GDPR serves as the legal basis.

In the event that vital interests of the data subject or another natural person make processing of personal data necessary, Article 6, para. 1 point (d) of the GDPR serves as the legal basis.

If the processing is necessary to protect a legitimate interest of the controller or a third party and the interests, fundamental rights and freedoms of the data subject do not outweigh the first-mentioned interest, Article 6, para. 1 point (f) of the GDPR serves as the legal basis for the processing.

For any transfer to a third country, the processing shall be carried out in compliance with the principles pursuant to Article 44 et seq. of the GDPR.

3. Data deletion and duration of storage

The personal data of the data subject will be deleted or blocked as soon as the purpose of the storage ceases to apply or a given consent is revoked by the data subject, or the processing is objected to. In addition, storage may take place if this has been provided for by the European or national legislator in Union regulations, laws or other provisions to which the controller is subject. The data will also be blocked or deleted if a storage period prescribed by the aforementioned standards expires, unless there is a need for further storage of the data for the conclusion or performance of a contract.

4. Data transfer to non-secure third countries

The transfer and processing of personal data of data subjects in a non-secure third country, such as the USA, is carried out under the conditions of Article 44 et seq. of the GDPR. For the USA (and other non-secure third countries), there is currently no adequacy decision of the EU Commission within the meaning of Article 45, para. 1, 3 of the GDPR. This means that the EU Commission has not yet positively determined that there is a level of data protection there comparable to the requirements of the GDPR. In addition, the GDPR requires so-called "appropriate safeguards" for a data transfer to a third country or to international organizations, Article 46, para. 2, 3 of the GDPR. These can be, for example, internal company data protection regulations approved by a supervisory authority or standard data protection contracts. **In summary, in the aforementioned non-secure third countries, there is no level of data protection comparable to the requirements of the GDPR.**

Risks of a transfer to a non-secure third country

Personal data could possibly be passed on by the provider to other third parties beyond the actual purpose of fulfilling the order, who use the data for advertising purposes, for example. In addition, it is probably not possible to effectively enforce any rights to information against the subcontractor. There may be a higher probability that incorrect data processing may occur, as the subcontractor's technical and organizational measures for the protection of personal data do not fully meet the requirements of the GDPR in terms of quantity and quality. It is also possible that government agencies may access the personal data provided without the data subject being aware of this. This risk is particularly present when data is transferred to the USA. In principle, this also corresponds to the European legal regulations, e.g. for the purpose of hazard prevention. However, the permissibility threshold for such data processing in the European Union is higher than in the country of the data recipient.

If data is transferred to processors whose processing takes place in a non-secure third country, a separate notice is provided by the respective service provider.

II. Rights of the data subject

If we process personal data of you, you have the following rights as a data subject against us as a data controller:

1. Right to information, Article 15 GDPR.

Within the scope of the applicable legal provisions, you have the right to (free of charge) information about your collected and stored personal data at any time. This includes, among other things, information about their processing purposes, their origin and recipients, the storage period and the existence of various rights.

2. Right to rectification, Article 16 GDPR

You have the right to rectification (also in the sense of completion) of your data vis-à-vis the controller, insofar as the processed personal data concerning you are inaccurate or incomplete for the purpose of the processing. The controller shall carry out the rectification without undue delay.

3. Right to deletion, Article 17 GDPR

You may request the deletion of your personal data at any time under the conditions of Art. 17 of the GDPR, unless circumstances still apply that entitle or oblige the controller to continue to process your personal data (such as statutory retention obligations).

4. Right to restriction of processing, Article 18 GDPR

If the legal requirements are met, you may request restriction of the processing of your personal data within the scope of Article of the 18 GDPR.

5. Right to information, Article 19 GDPR

If your personal data has been processed by a recipient to whom the controller has disclosed the data, the controller is obliged to inform them of your requests for rectification, deletion, or restriction of processing, unless this proves impossible or involves a disproportionate effort. You may request that the controller inform you about this recipient.

6. Right to data portability, Article 20 GDPR

If you have provided us with personal data, and automated processing is carried out on the basis of your consent or on the basis of a contract, you have a right to transfer the data you have provided within the scope of Article 20 of the GDPR, provided that this does not affect the rights and freedoms of other persons. The data will be provided in a common, machine-readable format. If you request the direct transfer of the data to another controller, this will only be done insofar as it is technically possible.

7. Right of objection, Article 21 GDPR

You have the right to object to the processing of your data at any time, provided that the processing is carried out on the basis of a balance of interests. This is the case if the controller

relies on the public interest or its legitimate interest for processing (see Article 6, para. 1 point (e) and (f) of the GDPR). The prerequisite is that you assert reasons arising from your particular situation that outweigh the interest of the controller. The controller will no longer process the personal data concerning you, unless he can demonstrate compelling legitimate reasons for the processing which override your interests, rights and freedoms, or the processing serves the purpose of asserting, exercising or defending of legal claims.

Article 21, para. 2 of the GDPR contains a special deviating regulation if the personal data concerning you is used for direct marketing. Here, you have the right to object to the processing of the personal data concerning you at any time without further requirements. The personal data concerning you will no longer be processed for the purpose of direct marketing. Insofar as profiling is associated with direct advertising, you can also object to this.

In connection with the use of information society services, you may exercise your right to object by means of automated procedures involving the use of technical specifications.

8. Automated individual decision-making, including profiling, Article 22 GDPR

Pursuant to Article 22 of the GDPR, you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you. This does not apply if the decision (a) is necessary for the conclusion or performance of a contract between you and the controller, (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, and (c) is based on your explicit consent.

9. Right to withdraw the consent, Article 7 GDPR

Pursuant to Article 7, para. 3 of the GDPR, you have the right to withdraw your consent at any time. The lawfulness of the data processing carried out until the withdrawal remains unaffected by the revocation. You can send the revocation by e-mail or by post to the person responsible.

10. Right to complain to a supervisory authority

Without prejudice to any other administrative or judicial remedy, you have the right to complain to a data protection supervisory authority, in particular in the Member State of your residence, place of work or the place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

III. SSL/TLS Encryption

This website uses SSL/TLS encryption for reasons of security and to protect the transmission of confidential content, such as the inquiries that you as the data subject send to us as the site operator. An encrypted connection can be recognized by the fact that the address line of the browser changes from "http://" to "https://" and by the lock symbol in the browser line. If SSL/TLS encryption is activated, the data you transmit to us cannot be read by third parties.

IV. Proemion (Operation of the DataPortal)

1. Description and scope of data processing

The DataPortal is provided as software as a service (SaaS). The provider is Proemion GmbH, Donaustraße 14, 36043 Fulda, Germany.

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

- (1) Company data
- (2) Vehicle or machine information
- (3) GPS data
- (4) User data
- (5) CU data
- (6) Device identification data and traffic data (IP addresses, MAC addresses, user IDs, web logs, browser agents)
- (7) Utilization of DataPortal functions.

2. Legal basis for data processing

The legal basis for data processing is Article 6, para. 1 point (f) of the GDPR for the provision of the data portal.

If you, as the data subject, are a contractual partner of the controller, the legal basis for processing is Article 6, para. 1 point (b) of the GDPR.

3. Purpose of data processing

The purpose of the processing operations is to provide a telematics platform.

4. Duration of storage, possibility of objection and elimination

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In the case of the collection of data for the provision of the website, this is the case when the respective session has ended.

The collection of data for the provision of the website and the storage of the data in log files is absolutely necessary for the operation of the website. Consequently, there is no possibility for the user to object.

V. Provision of the website and creation of log files

1. Description and scope of data processing

Each time our DataPortal login page, as well as the sub-pages of the DataPortal, is called up, our system automatically collects data and information from the computer system of the calling computer.

The following data is collected:

- (1) Information about the browser type and version used.
- (2) The operating system of the user
- (3) The user's Internet service provider
- (4) The IP address of the user
- (5) Date and time of access
- (6) Websites from which the user's system accesses our website
- (7) Websites that are accessed by the user's system via our website
- (8) User name
- (9) Information about the operations performed by the user (and their parameters).

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

2. Legal basis for the data processing

The legal basis for the temporary storage of the data and the log files is Article 6, para. 1 point (f) of the GDPR

3. Purpose of data processing

The temporary storage of the IP address by the system is necessary to enable delivery of the DataPortal to the user's computer. For this purpose, the user's IP address must remain stored for the duration of the session.

Log files are stored to ensure the functionality of the DataPortal. In addition, we use the data to optimize the DataPortal and to ensure the security of our information technology systems. An evaluation of the data for marketing purposes does not take place in this context.

These purposes are also our legitimate interest in data processing according to Article 6, para. 1 point (f) of the GDPR.

4. Duration of storage, possibility of objection and elimination

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In the case of the collection of data for the provision of the DataPortal, this is the case when the respective session has ended.

In the case of storage of data in application log files, this is the case after 40 days at the latest. In the case of storage of data in access log files, this is the case after 60 days at the latest. Storage

beyond this period is possible if it is required in particular for error analyses or product improvements. In this case, the user's personal data is deleted or alienated, so that it is no longer possible to assign the calling client.

VI. Use of Cookies

1. Description and scope of data processing

Our DataPortal uses cookies. Cookies are text files that are stored in the Internet browser or by the Internet browser on the user's computer system. If a user calls up the DataPortal, a cookie may be stored on the user's operating system. This cookie contains a characteristic character string that enables the browser to be uniquely identified when the DataPortal is called up again.

We use cookies to make our DataPortal more user-friendly. Some elements of our DataPortal require that the calling browser can be identified even after a page change. We also use cookies that allow us to analyze how users use the DataPortal.

We use cookies and local browser storage for the following applications:

- (1) Log-in information
- (2) Adoption of language settings
- (3) Remembering search terms
- (4) User settings
- (5) Theming
- (6) Time zone
- (7) Last visited page in DataPortal
- (8) Use of functions

Transfer to a third country: The data collected via the aforementioned cookies for analysis purposes may be transferred to a service provider located in a third country. Further information can be found in this data protection information with the respective service provider. **Processing of personal data thus also takes place in a non-secure third country. In the USA, there is no level of data protection comparable to the requirements of the GDPR. You can find more information on the transfer to a non-secure third country in this data protection information under "I. General information on data processing - 4. Data transfer to non-secure third countries".**

2. Legal basis for data processing

The legal basis for the processing of personal data using technically necessary cookies is Article 6, para. 1 point (f) of the GDPR; the storage of cookies in your terminal device is based on § 25 para. 2 no. 2 TTDSG (= German Telecommunications-Telemedia Data Protection Act).

3. Purpose of data processing

The purpose of using technically necessary cookies is to simplify the use of our DataPortal for users. Some functions of our DataPortal cannot be offered without the use of cookies. For these, it is necessary that the browser is recognized even after a page change.

We use the data from analysis cookies to improve and troubleshoot the provision of the DataPortal. The user data collected by cookies is not used to create user profiles.

In these purposes also lies our legitimate interest in the processing of personal data according to Article 6, para. 1 point (f) of the GDPR.

4. Duration of storage, possibility of objection and elimination

Cookies are stored on the user's computer and transmitted by the latter to our website. Therefore, you as a user also have full control over the use of cookies. By changing the settings in your Internet browser, you can disable or restrict the transmission of cookies. Cookies that have already been stored can be deleted at any time. This can also be done automatically. If cookies are deactivated for our DataPortal, it may no longer be possible to fully use all functions of the DataPortal.

The cookies we use are generally stored for a maximum of 2 years.

VII. Registration / Login

1. Description and scope of data processing

On the DataPortal, it is possible to log in by entering a user name and password. Registration and creation of user data are carried out centrally by an admin.

The following data is generally stored by you during registration:

- (1) Name
- (2) First name
- (3) E-mail address
- (4) Organization
- (5) Language
- (6) DataPortal permissions.

An activity log is created for logged-in users.

2. Legal basis for the data processing

The legal basis for the processing of personal data is Article.6, para. 1 point (f) of the GDPR. If you as the data subject are a contractual partner of the responsible party, the legal basis is Article 6, para.1 point (b) of the GDPR.

3. Purpose of the data processing

The processing through registration and login is necessary for the fulfillment of a contract with the user or for the implementation of pre-contractual measures.

The registration and login are necessary to ensure secure access to the data in the DataPortal. Furthermore, the user-specific login assigns the user rights within the DataPortal and allows user settings to be saved. The purpose of activity logging is to ensure the integrity of the DataPortal.

4. Duration of storage, possibility of objection and elimination

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected.

This is the case for data collected during the registration process for the fulfillment of a contract or for the implementation of pre-contractual measures when the data is no longer required for the implementation of the contract. Even after the conclusion of the contract, it may be necessary to store personal data of the contractual partner in order to fulfill contractual or legal obligations. If the data is required for the performance 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.

VIII. Subcontracting relationships - Information on subcontractors used by the DataPortal operator

The DataPortal uses services of several subcontractors, which are carefully selected and used by the DataPortal operator.

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 subcontractors used under the following link <https://dataportal.proemion.com/#!/subprocessors>. This will be updated regularly if the use of the services changes.