



Privacy Policy

Status as of 02/2024 – ddp: Deutsche Digital & Performance, Owner: Arne Ahlreip, Gottfried-August Bürger-Str. 7, D-06343 Molmerswende

PREAMBLE

With the following privacy policy, we would like to inform you about the types of your personal data (hereinafter also referred to as “data”) that we process, for what purposes, and to what extent. The privacy policy applies to all processing of personal data carried out by us, both in the provision of our services and especially on our websites, in mobile applications, and within external online presences, such as our social media profiles (hereinafter collectively referred to as the “online offering”).

The terms used are not gender-specific.

1. CONTROLLER

Arne Ahlreip
Gottfried-August-Bürger-Str. 7
D-06343 Mansfeld (Sachsen-Anhalt)
Email: office – at – ddp-harz.de

2. OVERVIEW OF PROCESSING

The following overview summarizes the types of processed data and the purposes of their processing, referring to the data subjects.

TYPES OF PROCESSED DATA

- Inventory data
- Payment data
- Contact data
- Content data
- Contract data
- Usage data
- Meta, communication, and procedural data

CATEGORIES OF DATA SUBJECTS

- Customers
- Interested parties
- Communication partners
- Users
- Business and contractual partners
- Participants

PURPOSES OF PROCESSING

- Provision of contractual services and fulfillment of contractual obligations
- Contact inquiries and communication
- Security measures
- Direct marketing
- Range measurement
- Office and organizational procedures
- Administration and response to inquiries
- Feedback
- Marketing
- Profiles with user-related information
- Provision of our online offering and user-friendliness
- Information technology infrastructure

3. APPLICABLE LEGAL BASES

Relevant legal bases under the GDPR: Here is an overview of the legal bases of the GDPR on which we process personal data. Please note that, in addition to the provisions of the GDPR, national data protection regulations may apply in your or our country of residence or business. If more specific legal bases are relevant in individual cases, we will inform you of these in the privacy policy.

Consent (Art. 6(1)(a) GDPR) – The data subject has given consent to the processing of personal data concerning him or her for one or more specific purposes.

Performance of a contract and pre-contractual inquiries (Art. 6(1)(b) GDPR) – Processing is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures requested by the data subject.

Legal obligation (Art. 6(1)(c) GDPR) – Processing is necessary for compliance with a legal obligation to which the controller is subject.

Legitimate interests (Art. 6(1)(f) GDPR) – Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

National data protection regulations in Germany: In addition to the data protection regulations of the GDPR, national regulations on data protection in Germany apply. This includes, in particular, the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG). The BDSG contains special regulations on the right to information, the right to deletion, the right to object, the processing of special categories of personal data, processing for other purposes, and transmission as well as automated decision-making, including profiling. In addition, data protection laws of the individual federal states may apply.

National data protection regulations in Austria: In addition to the data protection regulations of the GDPR, national regulations on data protection in Austria apply. This includes, in particular, the Austrian Data Protection Act (Datenschutzgesetz – DSG). The Data Protection Act contains special regulations on the right to information, the right to rectification or deletion, the processing of special categories of personal data, processing for other purposes, and transmission, as well as automated decision-making in individual cases.

Note on the applicability of the GDPR and Swiss DPA: These data protection notices serve as information in accordance with the Swiss

Federal Data Protection Act (Schweizer DSG) as well as the General Data Protection Regulation (GDPR). For this reason, please note that due to broader spatial application and understanding, the terms of the GDPR are used. In particular, instead of the terms “processing” of “personal data,” “overriding interest,” and “particularly sensitive personal data” used in the Swiss DSG, the terms “processing” of “personal data,” “legitimate interest,” and “special categories of data” used in the GDPR are used. However, the legal meaning of the terms continues to be determined within the scope of the Swiss DSG.

4. SECURITY MEASURES

We take appropriate technical and organizational measures in accordance with legal requirements, taking into account the state of the art, implementation costs, and the nature, scope, circumstances, and purposes of processing, as well as the different probabilities of occurrence and the extent of the threat to the rights and freedoms of natural persons, to ensure a level of protection appropriate to the risk.

The measures include, in particular, ensuring the confidentiality, integrity, and availability of data by controlling physical and electronic access to the data, as well as the access, input, transfer, securing of availability, and its separation. Furthermore, we have established procedures to ensure the exercise of data subjects’ rights, the deletion of data, and responses to the threat to data. We also consider data protection when developing or selecting hardware, software, and procedures, in accordance with the principle of data protection, through technology design and data protection-friendly default settings.

TLS/SSL encryption (https): To protect the data of users transmitted through our online services, we use TLS/SSL encryption. Secure Sockets Layer (SSL) is the standard technology for securing Internet connections by encrypting data transmitted between a website or app and a browser (or between two servers). Transport Layer Security (TLS) is an updated and more secure version of SSL. Hyper Text Transfer Protocol Secure (HTTPS) is displayed in the URL when a website is secured by an SSL/TLS certificate.

5. TRANSMISSION OF PERSONAL DATA

In the context of our processing of personal data, it may happen that the data is transferred to other locations, companies, legally independent organizational units, or individuals or disclosed to them. Recipients of this data may include, for example, service providers commissioned with IT tasks or providers of services and content embedded in a website. In such cases, we comply with legal requirements and, in particular, conclude appropriate contracts or

agreements that serve to protect your data with the recipients of your data.

6. INTERNATIONAL DATA TRANSFERS

Data processing in third countries: If we process data in a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)) or if the processing is part of the use of third-party services or the disclosure or transfer of data to other persons, bodies, or companies, this only takes place in accordance with legal requirements. If the level of data protection in the third country has been recognized by means of an adequacy decision (Art. 45 GDPR), this serves as the basis for data transfer. Otherwise, data transfers only take place if the level of data protection is otherwise guaranteed, in particular by means of standard contractual clauses (Art. 46(2)(c) GDPR), explicit consent, or in the case of contractual or legally required transfer (Art. 49(1) GDPR). In addition, we will inform you about the bases of third-country transmission for each provider from the third country, with adequacy decisions taking precedence as a basis. Information on third-country transfers and existing adequacy decisions can be found in the information provided by the EU Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en?prefLang=de.

EU-US Trans-Atlantic Data Privacy Framework: As part of the so-called "Data Privacy Framework" (DPF), the EU Commission has also recognized the level of data protection for certain companies from the USA as safe within the framework of the adequacy decision of 10.07.2023. The list of certified companies as well as further information on the DPF can be found on the website of the US Department of Commerce at <https://www.dataprivacyframework.gov/> (in English). We will inform you as part of the data protection notices which service providers certified under the Data Privacy Framework are used by us.

7. DELETION OF DATA

The data processed by us will be deleted or restricted in processing in accordance with legal requirements, as soon as the purposes for which they were processed cease to apply or the data subjects revoke their consent or other permissions expire (e.g., if the purpose of processing this data has ceased to apply or they are not necessary for the purpose). If the data is not deleted because it is required for other and legally permissible purposes, its processing will be limited to these purposes. This means that the data will be blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax reasons or whose storage is necessary for the assertion, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person. Our data protection notices may also contain further information on the storage and deletion of data that is primarily applicable to the respective processing.

8. RIGHTS OF DATA SUBJECTS

Rights of data subjects under the GDPR: You have various rights as data subjects under the GDPR, which result in particular from Art. 15 to 21 GDPR:

Right to object: You have the right, for reasons that arise from your particular situation, to object at any time to the processing of personal data concerning you, which is based on Art. 6(1)(e) or (f) GDPR, including profiling based on these provisions. If the personal data concerning you is processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for the purpose of such advertising, including profiling, insofar as it is related to such direct marketing.

Right to revoke consent: You have the right to revoke your consent at any time.

Right to information: You have the right to request confirmation as to whether the data in question is being processed and to obtain information about this data and further information and a copy of the data in accordance with legal requirements.

Right to rectification: In accordance with legal requirements, you have the right to request the completion of data concerning you or the correction of inaccurate data concerning you.

Right to erasure and restriction of processing: You have the right, in accordance with legal requirements, to request that data concerning you be deleted immediately or, alternatively, to request that the processing of the data be restricted in accordance with legal requirements.

Right to data portability: You have the right to receive data concerning you that you have provided to us in a structured, common, and machine-readable format in accordance with legal requirements, or to request its transmission to another controller.

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

9. USE OF COOKIES

Cookies are small text files or other storage technologies that store information on end devices and retrieve information from end devices. For example, to store login status in a user account, shopping cart contents in an e-shop, accessed content, or functions used in an online offering. Cookies can also be used for different purposes, such as functionality, security, and convenience of online offerings, as well as for analyzing visitor flows.

Notes on consent: We use cookies in accordance with legal regulations. Therefore, we obtain prior consent from users, unless this is not required by law. Consent is not necessary, in particular, if storing and retrieving information, including cookies, is absolutely necessary to

provide users with a telemedia service (i.e., our online offering) expressly requested by them. Cookies that are absolutely necessary usually include cookies with functions that serve the display and operability of the online offering, load balancing, security, and the storage of user preferences and choices, or similar purposes related to the provision of the main and secondary functions of the online offering requested by users. Revocable consent is clearly communicated to users and includes information about the respective cookie usage.

Notes on the legal basis of data protection: The legal basis on which we process users' personal data using cookies depends on whether we ask users for consent. If users consent, the legal basis for processing their data is the declared consent. Otherwise, the data processed using cookies is based on our legitimate interests (e.g., in the operational management of our online offering and the improvement of its usability) or, if cookies are necessary for the fulfillment of our contractual obligations, because the use of cookies is necessary to fulfill our contractual obligations. We will inform users about the purposes for which cookies are processed as part of these data protection notices or within the scope of our consent and processing processes.

Storage duration: With regard to the storage period, the following types of cookies are distinguished:

Temporary cookies (also: session or session cookies): Temporary cookies are deleted at the latest after a user has left an online offering and closed their end device (e.g., browser or mobile application).

Permanent cookies: Permanent cookies remain stored even after the end device has been closed. For example, the login status can be stored or preferred content can be displayed directly when the user visits a website again. The data collected using cookies can also be used for audience measurement. If we do not provide users with explicit information about the type and duration of cookies used (e.g., as part of obtaining consent), users should assume that cookies are permanent and can be stored for up to two years.

General information on revocation and objection (so-called "opt-out"): Users can revoke their consent and object to the processing in accordance with legal requirements at any time. For this purpose, users can, among other things, restrict the use of cookies in their browser settings (which may also limit the functionality of our online offering). An objection to the use of cookies for online marketing purposes can also be declared on the websites <https://optout.aboutads.info> and <https://www.youronlinechoices.com/>.

10. BUSINESS SERVICES

We process data from our contractual and business partners, e.g., customers and interested parties (collectively referred to as "contractual partners"), within the framework of contractual and comparable legal relationships as well as related measures and in the context of communication with contractual partners (or pre-contractually), e.g., to answer inquiries.

We process this data to fulfill our contractual obligations. This includes, in particular, the obligations to provide the agreed-upon services,

any update obligations, and remedies for warranty and other service disruptions. In addition, we process the data to safeguard our rights and for the purposes of the administrative tasks associated with these obligations and the organization of our business. We also process the data based on our legitimate interests in proper and business management and security measures to protect our contractual partners and our business operations from misuse, safeguarding their data, secrets, information, and rights (e.g., involvement of telecommunications, transport, and other auxiliary services as well as subcontractors, banks, tax and legal advisors, payment service providers, or financial authorities). In the context of legal requirements, we only pass on the data of contractual partners to third parties to the extent that this is necessary for the aforementioned purposes or to fulfill legal obligations. Contractual partners will be informed about further forms of processing, e.g., for marketing purposes, within the scope of this data protection declaration.

We delete the data after the expiry of legal warranty and comparable obligations, i.e., in principle after 4 years, unless the data is stored in a customer account, e.g., as long as it must be kept for legal reasons of archiving. The statutory retention period is ten years for tax-relevant documents and business letters, inventories, opening balances, annual financial statements, the documents required for understanding these documents, and the relevant instructions and organizational documents, and six years for received commercial and business letters and copies of sent commercial and business letters. The period begins at the end of the calendar year in which the last entry was made in the book, the inventory, the opening balance sheet, the annual financial statement, or the management report was prepared, the commercial or business letter was received or sent, or the booking document was created, and the recording was made or the other documents were created.

If we use third-party providers or platforms to provide our services, the terms and conditions and data protection notices of the respective third-party providers or platforms apply in relation to users.

11. WEB ANALYSIS, MONITORING, AND OPTIMIZATION

Web analysis (also known as “reach measurement”) is used to evaluate the visitor flows of our online offering and can include behavior, interests, or demographic information about visitors, such as age or gender, as pseudonymous values. With the help of reach analysis, we can, for example, recognize at what time our online offering or its functions or content is most frequently used or invites reuse. We can also determine which areas need optimization.

In addition to web analysis, we may also use test procedures to test and optimize different versions of our online offering or its components, for example.

Unless otherwise stated below, profiles, i.e., data summarized for a usage process, can be created for these purposes, and information can be stored and retrieved from a browser or end device. The information collected includes, in

particular, visited websites and elements used there, as well as technical information, such as the browser used, the computer system used, and information on usage times. If users have consented to the collection of their location data towards us or the providers of the services we use, location data can also be processed.

The IP addresses of users are also stored. However, we use an IP masking procedure (i.e., pseudonymization by shortening the IP address) to protect users. In general, no clear data of users (such as e-mail addresses or names) are stored in the context of web analysis, A/B testing, and optimization, but pseudonyms. This means that we and the providers of the software used do not know the actual identity of users, but only the information stored in their profiles for the purposes of the respective procedures.

Processed data types: Usage data (e.g., visited websites, interest in content, access times); Meta, communication, and process data (e.g., IP addresses, time data, identification numbers, consent status).

Data subjects: Users (e.g., website visitors, users of online services).

Purposes of processing: Reach measurement (e.g., access statistics, recognition of recurring visitors). Profiles with user-related information (creating user profiles).

Security measures: IP masking (pseudonymization of the IP address).

Legal bases: Consent (Art. 6 para. 1 p. 1 lit. a) GDPR). Legitimate interests (Art. 6 para. 1 p. 1 lit. f) GDPR).

Other information on processing processes, procedures, and services:

Matomo (without cookies): Matomo is a privacy-friendly web analysis software that is used without cookies and uses a so-called “digital fingerprint” for the recognition of recurring users, which is stored anonymously and changed every 24 hours; the “digital fingerprint” captures user movements within our online offering using pseudonymized IP addresses in combination with user-side browser settings, so that conclusions about the identity of individual users are not possible. The data collected from users during the use of Matomo is processed only by us and not shared with third parties; Legal basis: Legitimate interests (Art. 6 para. 1 p. 1 lit. f) GDPR). Website: <https://matomo.org/>.

Matomo: Matomo is software used for web analysis and reach measurement purposes. Cookies are generated and stored on users’ end devices as part of the use of Matomo. The data collected from users during the use of Matomo is processed only by us and not shared with third parties. The cookies are stored for a maximum period of 13 months: https://matomo.org/faq/general/faq_146/; Legal basis: Consent (Art. 6 para. 1 p. 1 lit. a) GDPR). Deletion of data: The cookies have a storage period of a maximum of 13 months.

Google Analytics: Reach measurement and web analysis; Service provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, Parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; Website: <https://marketingplatform.google.com/intl/de/about/analytics/>; Pri-

vacypolicy: <https://policies.google.com/privacy>; Types of processing and processed data: <https://privacy.google.com/businesses/adsservices>; Data processing conditions for Google advertising products and standard contractual clauses for third-country transfers of data: <https://business.safety.google/adsprocessor/terms>.

12. SOCIAL MEDIA PRESENCES

We maintain online presences within social networks and process user data in this context to communicate with active users or provide information about us.

We would like to point out that user data may be processed outside the European Union in this context. This may pose risks for users, as, for example, the enforcement of users’ rights could be more difficult.

Furthermore, user data within social networks is typically processed for market research and advertising purposes. For example, user profiles can be created based on user behavior and resulting interests. These user profiles can then be used to display advertisements within and outside the networks that presumably match the users’ interests. For these purposes, cookies are usually stored on users’ computers, storing information about users’ behavior and interests. Additionally, data can be stored in user profiles independently of the devices used by users (especially if users are members of the respective platforms and logged in).

For a detailed presentation of the respective processing methods and the possibility of objection (opt-out), we refer to the privacy policies and information provided by the operators of the respective networks.