PRIVACY POLICY

As of: 11/01/2025

1. General

The protection of your personal data is very important to us. We process your data exclusively in compliance with the legal provisions (GDPR, Data Protection Act (DSG), Telecommunication Act (TKG)). In this privacy policy, we inform you about the most important aspects of data processing within the scope of our services.

In order to provide our services, we process information about you, known as personal data – or "*data*" for short. The term "processing" refers to any handling of data, such as the collection, storage, use, and deletion of personal data.

We are happy to inform you in this privacy policy about the processing of your personal data and the claims and rights to which you are entitled under data protection regulations.

The entity responsible for processing your personal data is:

Graystack IT GmbH
Am Pilgerweg 25
3131 Inzersdorf ob der Traisen
Austria
Email: dsgvo@graystack.cloud

If you have any questions about how your data is processed or would like to exercise your rights (see below), please contact us at this address.

1.1. Cookies

Our website uses cookies. These are small text files that are stored on your device and can be retrieved again. Information about the cookies used when you visit the website can be found in the cookie banner that appears when you visit the website. You can use this banner to set your cookie preferences. To change these settings later, please click here.

These cookies are either cookies that are technically necessary for the operation of our website or cookies that enable us to personalize your user experience and display content and advertising tailored to your interests.

You can refuse some or all cookies or delete cookies that have already been set via your browser settings. Please note that certain functions of the

website may not be available if you deactivate cookies.

2. Data processing when using our website

2.1. General information

As part of our website, we process data that you provide to us (e.g., when contacting us, registering for an account, and purchasing a service package) and that is generated when you use our website, logs (for security reasons, our servers log who makes requests) and cookies (these are small text files that are stored on your device and contain information to recognize you).

The web server providing our website is technically operated by Laravel Holdings Inc. (New York). The servers are operated in Europe.

2.2. Data processing for running and securing our platform (server logs and service monitoring by Nightwatch):

Server logs: When you access our platform and use our software, the web server collects usage data (so-called server logs). The collection of this data is necessary to enable the connection to our server and the use of the website from a technical perspective. This data is also used to defend our platform against online attacks. The following data is collected: the host name and IP address of the accessing device, date and time of the request, identification data of the browser and operating system, and the referrer URL.

Service monitoring by Nightwatch: We monitor the correct and stable operation of our software with the Nightwatch application, which is part of the services provided by our web hosting provider Laravel Holdings Inc. (https://nightwatch.laravel.com). Nightwatch logs the username, session ID, and IP addresses of users of our software. This enables us to locate errors and fix them for our customers.

Legal basis for processing: Your data is processed on the basis of our legitimate interest in ensuring the operation of the service and system security and in locating errors.

Recipients of the data: The web server for the operation of our website is technically operated by Laravel Holdings Inc. (New York). In the event of a hacker attack, the data from the **server logs** will be passed on to the law enforcement authorities. No further disclosure to third parties will take place. The data logged by **Nightwatch** is only visible to us and is not transmitted to third parties.

Further information: Personal data is stored in **server logs** for a maximum of 3 months. The IP address is stored in the logs so that, in the event of security incidents (hacking, data breaches, etc.), we can assist the relevant authorities in investigating and prosecuting the incident. We store **Nightwatch logs** until the end of the customer contract and for a further three years beyond that in order to be able to prove the quality of our services in the event of complaints.

2.3. Data processing when contacting us:

Purpose of processing: When you contact us by email, phone, or via the online form for product inquiries (not: support, see point 2.6 for that), we collect and store all data that you provide to us.

Legal basis for processing: Your data is processed for the purpose of implementing pre-contractual measures (such as inquiries prior to the purchase of a service package) or for the fulfillment of a contractual relationship (Art. 6 (1) (b) GDPR) or is based on our legitimate interest in processing the inquiry response (Art. 6 (1) (f) GDPR).

Recipients of the data: We only transmit the data to third parties if this is necessary to respond to the inquiry.

Further information: We store the data for the duration of responding to the inquiry and for any follow-up questions. In addition, we retain your inquiries for up to six months so that you can refer to an older inquiry at a later date.

2.4. Data processing in connection with our newsletter

Purpose of processing: When you subscribe to our newsletter, you will receive regular information from us by email about us, our offers, and our services. If you no longer wish to be contacted by us, simply unsubscribe using the unsubscribe link in the newsletter. We evaluate your use of our mailings anonymously in order to determine how many users read our emails so that we can better tailor the newsletter to the interests of our subscribers.

Legal basis for processing: Your data is processed for mailing purposes on the basis of your consent (Art. 6 (1) (a) GDPR). You can revoke your consent to receive the newsletter at any time. A link to do so is included in all mailings. You can also revoke your consent using the contact options provided.

Declaring your revocation does not affect the legality of the processing that has taken place up to that point.

Recipients of the data: We use the email delivery service Mailgun from Mailgun Technologies, Inc., San Antonio, TX, USA ("Mailgun") to send our messages. We have concluded a data processing agreement with Mailgun. This contractor has committed to complying with the requirements of the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list), so that adequate protection is provided for the transfer and processing of your data, even in countries outside the EU. Further information on data processing can be found in Mailgun's privacy policy and here: https://www.mailgun.com/glossary/gdpr/

Further information: Your personal data will be processed until you unsubscribe from the newsletter.

2.5. Data processing when registering for a user account:

Purpose of processing: When you register for a user account, we store all the data you provide us with in this context, namely master data (such as company, first and last name of the representative), contact details (such as postal address, telephone number, email address), login credentials (username and password), service data (service packages booked, order, supplier, and product database), and billing data.

Some information is mandatory and marked accordingly. If you do not provide us with this data, you will not be able to use our services. We use this data to provide your account and enable you to use our services.

Legal basis for processing: The legal basis for processing your data is the fulfillment of the contractual relationship entered into with you (Art. 6 (1) (b) GDPR) or a legal obligation (Art. 6 (1) (c) GDPR).

Recipients of the data: The data will be transferred to third parties if and to the extent necessary to fulfill this contractual relationship. If the transfer of your data relevant in the respective individual case is necessary for the fulfillment of the contractual relationship or on the basis of a legal basis, it will be transferred to the following categories of recipients:

- Contractual and business partners
- Legal representatives
- Chartered accountants, auditors, and tax advisors
- Courts

- Competent administrative authorities
- Debt collection agencies

Further information: We store all this data until the order is completed and the period for asserting warranty and damage claims arising from the contract has expired (usually three years). Statutory retention obligations (e.g. under accounting regulations) remain unaffected.

2.6. Data processing when using our software:

Purpose of processing: When you use our software, we process all personal data disclosed in the process and otherwise incurred. This includes the master and contact data of the logged-in user, the master and contact data of suppliers and customers, data on business transactions (if applicable, contact persons for orders and deliveries), and communication data (texts, documents, if applicable also voicemails, support requests, messages regarding the service package) when we handle communication between you, suppliers, and customers.

Legal basis for processing: The legal basis is the fulfillment of our contractual obligations to you or the implementation of pre-contractual measures – Art. 6 (1) (b) GDPR.

Recipients of the data: The data will be transferred to third parties if and to the extent necessary to fulfill this contractual relationship. If the transfer of your data relevant in the respective individual case is necessary for the fulfillment of the contractual relationship or on the basis of a legal basis, this will be done to the following categories of recipients:

- Contractual and business partners
- Legal representatives
- Chartered accountants, auditors, and tax advisors
- Courts
- Competent administrative authorities
- Debt collection agencies

Further information: We store all this data until the order is completed and the period for asserting warranty and damage claims arising from the contract has expired (usually three years). Statutory retention obligations (e.g. under accounting regulations) remain unaffected.

3. Transfer of data, data processing

Your personal data will be used exclusively by us and will not be disclosed to third parties without your consent, a legal obligation, or a court or administrative decision.

When using our software, personal data of your suppliers, your customers, and other people who have a relationship with you will be processed. In this context, we act as a data processor for you within the meaning of Article 28 GDPR. The terms and conditions of the data processing agreement concluded with you apply.

If we ourselves use third parties ("processors") to carry out orders, we ensure that they use your data exclusively within the scope of the agreement concluded with them, our orders, and in compliance with data protection regulations.

Our **internet provider** Laravel Holding operates the servers on which our service is operated within Europe.

For the processing of payments, we transfer personal data to the respective **payment service providers** (e.g., Stripe). The legal basis for this is Art. 6 (1) lit. b GDPR. Further information can be found in the privacy policies of the respective payment providers.

Some of the services we use (e.g., Google, Meta, Microsoft) process data in the United States. When transferring personal data to these service providers, an adequate level of data protection is ensured by the respective EU standard contractual clauses and/or by the service provider's certification in accordance with the requirements of the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list).

4. Your rights

4.1 Right of access to processed data in accordance with Art. 15 GDPR

You have the right to request **information** about whether we process your personal data. If this is the case, you have the right to information about this personal data and other information related to the processing.

4.2 Right to rectification of inaccurate data in accordance with Art. 16 GDPR

In the event that personal data that we process about you is no longer accurate or is incomplete, you may request that this data **be corrected** and, if necessary, **completed**.

4.3 Right to erasure of data in accordance with Art. 17 GDPR

If the legal requirements are met, you may request the **erasure of** your personal data.

4.4 Right to restriction of data processing pursuant to Art. 18 GDPR

If the legal requirements are met, you can request the **restriction of processing** of data concerning you.

4.5 Right to data portability pursuant to Art. 20 GDPR

If the legal requirements are met, you may request the transfer of your data in a structured, commonly used, and machine-readable format.

4.6 Right to object to unreasonable data processing pursuant to Art. 21 GDPR

On grounds relating to your particular situation, you may object at any time to the processing of data concerning you that we process on the basis of a legitimate interest pursuant to Art. 6 (1) (f) GDPR.

4.7 Right to withdraw consent

If data processing is based on your consent, you have the option of withdrawing this consent at any time without affecting the lawfulness of the processing carried out on the basis of the consent until withdrawal.

4.8 Right to lodge a complaint with the data protection authority

If you believe that our processing of your personal data violates applicable data protection law or that your data protection rights have been violated in any other way, you have the option of lodging a complaint with the competent supervisory authority (Austrian Data Protection Authority). The address is:

Österreichische Datenschutzbehörde (Austrian Data Protection Authority)
Barichgasse 40-42
1030 Vienna
Phone: +43 1 52 152-0
Email: dsb@dsb.gv.at

5. Further information:

We require the data we ask you to provide in order to perform our services within the scope of the contractual relationship or to provide you with the information you have requested. If you do not provide the data, we will not be able to perform our services.

We do not use automated decision-making, including profiling. However, profiling may take place in the context of advertising measures (e.g., personalized ads) if you have consented to this.

If we process your personal data for a purpose other than that for which we collected it, we will notify you of this fact and inform you of this other purpose.

We reserve the right to amend or supplement this statement as necessary to reflect changes in our offerings and customer feedback. The date of the last change can be found at the top of this document. Please visit this website regularly to stay informed about the current status of the privacy policy.

Technical and Organizational Measures (TOM)

1. General

These technical and organizational measures (TOM) serve to ensure an adequate level of protection within the meaning of Art. 32 GDPR for the processing of personal data in the context of the web application under https://www.graystack.one.

Processing is carried out using modern cloud infrastructure (Laravel Cloud based on AWS).

2. Confidentiality

2.1 Access control

- The servers used are operated in highly secure data centers of the cloud provider (AWS).
- Physical access is only available to authorized personnel of the provider.

2.2 Access control

- Access to the systems is exclusively via personalized user accounts.
- Administrative access is limited to a minimum.
- Two-factor authentication (2FA) can be enabled for user accounts.
- Regular review and revocation of access rights that are no longer needed.

2.3 Access Control

- Access to personal data is only granted to authorized persons.
- Implementation of a role and authorization concept (need-to-know principle).
- Administrative access is restricted.

2.4 Separation control

- Data from different users is logically separated from each other (multi-client capability of the application).
- Separation of development, test and production environments.

3. Integrity

3.1 Passing control

- All data transfers are encrypted (TLS/HTTPS).
- Internal communication interfaces (APIs) are secured and authenticated.
- Protection against unauthorized access through network and infrastructure measures (e.g. security groups, firewalls).

3.2 Input control

- Entries, changes and deletions of data are logged in a traceable manner.
- Use of audit logs, as far as technically implemented.

4. Availability and resilience

4.1 Availability control

- Use of highly available cloud infrastructure (Laravel Cloud together with AWS).
- Automated backups through the platform or database systems.
- Monitoring and logging for early detection of faults.

4.2 Recoverability

- Ability to restore data from backups.
- Periodic review of recoverability as part of the platform's capabilities.

4.3 Protection against loss and attacks

- Use of current security mechanisms (firewalls, network isolation) by the cloud provider.
- Protection against common web attacks (e.g., through Laravel framework security mechanisms).
- Regular updates and security patches of the software used.

5. Periodic review and evaluation procedures

- Regular review of technical and organizational measures.
- Continuous updating of software and dependencies.
- Monitoring of system and security logs.
- Assessment of new risks and adaptation of measures.

6. Order processing

- Selection of service providers (e.g. Laravel Cloud, AWS) according to recognized security standards.
- Conclusion of order processing agreements (DPA), if necessary.
- Processing of personal data exclusively within the framework of documented instructions.

7. Data protection through technology design and privacy-friendly default settings

- Implementation of "Privacy by Design" and "Privacy by Default".
- Collection of only the personal data necessary for the respective purpose.
- Restrictive access settings by default.
- Ability to enable additional security measures (e.g., 2FA for user accounts).

- Minimization of data processing and storage.

8. Incident response and reporting procedure

- Implement processes to detect and deal with security incidents.
- Documentation of incidents and measures.
- Notification of data breaches in accordance with Art. 33 GDPR within 72 hours, if required.

9. Employees and authorized access

- Access to personal data is limited to authorized persons.
- Commitment to confidentiality.

10. Up-to-dateness and adaptation

- These TOMs are reviewed regularly and updated as needed.
- Adjustments are made in particular for:
    - Changes to the technical infrastructure
    - Changes in legal requirements