plugilo

PLUGILO PRIVACY POLICY

Effective Date: Jun 22, 2026

Summary

We work hard to make our use of personal data transparent and to make your rights and choices easy to understand. This policy explains what information we collect, how we use it, and what choices you have.

Key Points:

• We collect information you provide and technical data about how you use our services

• We use this information to personalize your experience and show you relevant content

• You have rights to access, correct, delete, and control how we use your data

• We implement strong security measures to protect your information

1. Scope of This Privacy Policy

This is Plugilo's global Privacy Policy. We have highlighted below where a particular section applies to you based on where you live.

Data Controllers

For purposes of the General Data Protection Regulation ("GDPR"), if you are a resident in the EEA, Switzerland, and UK, Plugilo, Inc. is the data controller of your personal information. Plugilo, Inc. is a US company with its registered office at 200 Continental Drive Suite 401, Newark, Delaware 19713. Plugilo, Inc. is a Delaware corporation.

If you have any questions about our data processing activities, please contact our Data Protection Officer at: legal@plugilo.com

For residents in the EEA/Germany: Our Data Protection Officer is heydata GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, datenschutz@heydata.eu.

2. Information We Collect

We collect information in three main ways:

2.1 Information You Provide to Us

When you use Plugilo websites, apps, services, technologies, APIs, widgets, or any other products or features we offer (collectively, “Plugilo” or the “Services”), you voluntarily share certain information:

Account Information: When you create an account, we collect your name, email address, birthday, gender, country of residence, interests, and preferred language. For business accounts, you may provide additional identifying information.

Content: We collect information when you save, upload, or create photos, stacks, cards, boards, or other content, and when you interact with our services or communicate with other users.

Precise Location Information: With your permission, you can choose to share your precise location using your device settings.

Communications: If you contact us for customer support or otherwise communicate with us, we collect the content of these communications.

2.2 Technical Information We Collect Automatically

When you use our Services, certain information is created and logged automatically:

Device Information: We collect information about the device you use to access our Services, including device type, operating system, network service provider, settings, and unique device identifiers.

Log Data: Our servers automatically record information including your Internet Protocol (IP) address, browser type and settings, pages visited, and the date and time of your access.

Cookies and Similar Technologies: We use cookies and similar technologies to store preferences and track activity. For more information, please review our Cookie Policy at https://plugilo.de/policy#cookie-policy

Usage Data and Inferences: We analyze your activity—such as items you click, search terms, boards you create, and comments you add—to make inferences about your interests and preferences.

Location Information: We use your IP address to infer your approximate location. Photos and other content you share may include metadata about where they were created.

2.3 Information from Partners and Third Parties

We receive information from:

Third-Party Platforms: If you register or log in using a third-party platform (like Apple, Facebook, or Google), they provide us with certain information to facilitate your account creation or login.

Technical Service Partners: We receive information from technical service partners and marketing firms to improve our services.

Advertisers and Partners: Measurement providers share information that helps us understand how our own marketing campaigns (for example, campaigns we run on social media platforms) perform. We do not receive or use third-party data to build interest profiles or to serve you personalized advertising.

3. How We Use Your Information

We use your information to provide, improve, and personalize our Services:

3.1 Service Delivery and Personalization

• Identify you when you use our Services

• Recommend stacks, cards, boards, and content based on your activity and interests

• Respond to your questions and comments

• Build your community by suggesting users with similar interests

• Customize your experience based on your location (with your consent)

• Send you updates via email, push notification, SMS, or phone (you can unsubscribe anytime)

3.2 Safety, Security, and Legal Compliance

• Review activity and messages to detect spam or risky behavior

• Analyze log data to identify suspicious behavior or policy violations

• Conduct age verification, which may include facial age estimation

• Work with law enforcement when necessary to keep Plugilo safe

• Access user information in connection with legal claims or proceedings

3.3 Service Improvement and AI Development

Artificial Intelligence and Machine Learning: We use your information to train, develop, and improve our technology, including machine learning models and artificial intelligence systems. This helps us:

• Improve content recommendations

• Enhance search functionality

• Detect and prevent spam and abuse

• Develop new features and products

We create aggregated or de-identified information that cannot reasonably be used to identify you. We process, maintain, and use this information only in a de-identified fashion and will not attempt to re-identify it.

3.4 Advertising and Marketing

We do not currently serve personalized or interest-based advertising on Plugilo. We use information only to promote Plugilo and to measure our own marketing:

- Advertise Plugilo on other sites and apps
- Measure the performance of our own marketing campaigns

Your Choices: We do not sell or share your personal information for cross-context behavioral advertising, and we do not currently serve personalized ads. You can manage your cookie and tracking preferences at any time through our consent management tool at https://plugilo.com/policy

4. Age Requirements and Verification

Minimum Age: You must be at least 13 years old to use Plugilo. In some jurisdictions, the minimum age may be higher.

Age Verification and Biometric Data

We may use facial age estimation technology to verify your age. When we do:

- We obtain your explicit consent before collecting biometric data
- Biometric data is encrypted and stored securely
- We retain biometric data only as long as necessary to verify your age, typically no more than 30 days
- You can request deletion of your biometric data at any time
- We never sell or share biometric data with third parties

If you have trouble with age verification or believe there's been a mistake, contact us at legal@plugilo.com

Children's Privacy (COPPA Compliance)

We do not knowingly collect personal information from children under 13. If we discover that we have collected information from a child under 13 without parental consent, we will delete that information immediately. If you believe we have collected information from a child under 13, please contact us at legal@plugilo.com

5. Data Security and Protection

We implement comprehensive security measures to protect your information:

Technical Security Measures

• **Encryption:** Data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 encryption

• **Access Controls:** Strict authentication and authorization protocols limit access to your data

• **Security Monitoring:** 24/7 monitoring for suspicious activity and potential security threats

• **Regular Audits:** Third-party security audits and penetration testing

• **Secure Development:** Security reviews and testing throughout our development process

Data Breach Notification

In the event of a data breach that affects your personal information:

• We will notify you within 72 hours of discovering the breach (or sooner if required by law)

• Notification will include the nature of the breach, types of data affected, and steps we're taking

• We will provide recommendations on how to protect yourself

• We will notify relevant regulatory authorities as required by law

6. How and When We Share Information

Anyone can see the public content you post, such as stacks, cards, and boards you create. We also share information in the following circumstances:

Categories of Third Parties

Service Providers: We share data with vendors who process information on our behalf, including:

- Cloud hosting providers
- Analytics services
- Customer support platforms
- Email and communication services
- Payment processors
- Security consultants

Advertising Partners: We share data with marketing and measurement providers that help us run and analyze our own campaigns, including:

- Social media advertising platforms (Facebook Ads, etc.)
- Google Marketing Platform
- Ad verification services

At Your Direction: When you choose to link your account to third-party services or publish content to other platforms

Legal and Safety: With law enforcement, government agencies, or other parties when required by law or necessary to protect safety, rights, or property

Business Transfers: If we engage in a merger, acquisition, or sale of assets, your information may be transferred to the acquiring entity

7. International Data Transfers

Plugilo is a worldwide service. By using our Services, you authorize us to transfer and store your information outside your home country, including in the United States.

Transfer Mechanisms (EEA, UK, Switzerland)

For users in the European Economic Area, UK, and Switzerland, we use the following safeguards:

• **Standard Contractual Clauses:** We use European Commission-approved Standard Contractual Clauses for transfers to countries without adequacy decisions

• **Adequacy Decisions:** We rely on European Commission adequacy decisions where available

• **Additional Safeguards:** We implement supplementary security measures to protect data transferred internationally

8. Data Retention

We retain your information only as long as necessary for the purposes described in this policy or as required by law.

Retention Periods

Data Type	Retention Period
Account Information	Duration of account plus 30 days after deletion
Content (stacks, cards, boards)	Duration of account or until deleted by user
Biometric Data	30 days maximum after age verification
Log Data	90 days
Marketing Communications	Until you unsubscribe or account deletion
Legal/Compliance Records	As required by law (typically 3-7 years)

When information is no longer needed, we either delete it or de-identify it so it cannot be linked to you.

9. Your Rights and Choices

You have significant control over your personal information. The specific rights available to you depend on where you live.

Rights Available to All Users

Access: Request a copy of the personal information we hold about you in a portable format. Send an email to legal@plugilo.com and request for your data.

Correction: Update or correct your information through your profile settings.

Deletion: Delete your account and associated data. Send an email to legal@plugilo.com and request for us to delete your data and account." Note that some information may be retained for legal compliance.

Cookie and Tracking Preferences: We do not currently use your data for personalized or targeted advertising. You can manage cookies and tracking technologies at any time through our consent management tool. If we introduce targeted advertising in the future, we will provide a clear opt-out and update this policy beforehand.

Marketing Communications: Unsubscribe from promotional emails by clicking the unsubscribe link or adjusting your notification settings.

Additional Rights for EEA, UK, and Switzerland Residents

Under the GDPR, you have additional rights:

- **Right to Object:** Object to processing based on legitimate interests
- **Right to Restriction:** Request we restrict processing in certain circumstances
- **Right to Data Portability:** Receive your data in a structured, machine-readable format
- **Right to Withdraw Consent:** Withdraw consent at any time where we rely on consent
- **Right to Lodge a Complaint:** File a complaint with your local data protection authority

Rights Under US State Privacy Laws

If you reside in California, Virginia, Colorado, Connecticut, Utah, Iowa, Texas, Oregon, Montana, Delaware, New Hampshire, New Jersey, Nebraska, Tennessee, or Minnesota, you have specific rights under state privacy laws:

California (CCPA/CPRA)

- Right to know what personal information we collect and how we use it
- Right to delete personal information
- Right to opt out of the sale or sharing of personal information
- Right to limit use of sensitive personal information
- Right to correct inaccurate information

• Right to non-discrimination for exercising your rights

California "Shine the Light" Law: Once per year, California residents can request information about personal information disclosed to third parties for direct marketing purposes. Contact legal@plugilo.com to make this request.

Other US States

Residents of Virginia, Colorado, Connecticut, Utah, Iowa, Texas, Oregon, Montana, Delaware, New Hampshire, New Jersey, Nebraska, Tennessee, and Minnesota have similar rights including:

• Right to confirm whether we process your personal information

• Right to access your personal information

• Right to delete personal information

• Right to opt out of targeted advertising

• Right to opt out of sale of personal information

• Right to opt out of profiling in furtherance of decisions with legal or similarly significant effects

• Right to correct inaccuracies

Canada

Canadian residents can withdraw consent for processing at any time. We may process information without consent in specific circumstances permitted by law, such as fraud detection, legal compliance, or when collection is in your interest and consent cannot be obtained timely.

Other locations

Residents of other countries may have additional rights regarding their data and its processing. Plugilo and its affiliates will honor the binding local regulations as required.

To exercise any of these rights, please contact us via: 1. Email: legal@plugilo.com 2. Postal Mail: Plugilo, Inc., 200 Continental Drive Suite 401, Newark, DE 19713

How to Exercise Your Rights

To exercise any of these rights:

1. Visit https://www.plugilo.com/Privacy for most requests

2. Contact our Help Center at https://corporate.plugilo.com/knowledge-hub/

3. Email us at legal@plugilo.com

Response Time: We will respond to your request within 45 days (or as required by applicable law). If we need more time, we'll explain why.

Verification: To protect your privacy, we must verify your identity before processing requests. We will not respond if we cannot verify your identity.

Appeals: If we deny your request, you may appeal by contacting legal@plugilo.com. We will respond to appeals within 45 days.

Authorized Agents: You may designate an authorized agent to make requests on your behalf. The agent must provide proof of authorization.

No Fee: We do not charge a fee to process requests unless the request is manifestly unfounded or excessive.

Global Privacy Control (GPC)

We recognize and honor Global Privacy Control (GPC) signals. If your browser sends a GPC signal, we will treat it as a valid opt-out request for the sale or sharing of your personal information for targeted advertising purposes.

10. Legal Bases for Processing (EEA, UK, Switzerland)

This section applies to residents of the European Economic Area, UK, and Switzerland. Under GDPR, we must have a legal basis to process your information.

Legitimate Interests

We process your information based on our legitimate interests or those of third parties where not outweighed by your rights:

- Personalizing content and recommendations
- Building your community and suggesting connections
- Maintaining safety and security
- Improving and developing our Services
- Providing measurement and analytics
- Communicating with you about our Services
- Measuring the performance of marketing campaigns

Legal Obligations

We process information to comply with legal and regulatory obligations, including:

- Responding to court orders, warrants, and legal requests
- Complying with GDPR, Digital Services Act, and other regulations
- Meeting tax and corporate reporting requirements
- Investigating misuse and protecting safety

Consent

We rely on your consent for:

• Precise location data collection
• Biometric data for age verification
• Certain cookies and tracking technologies
• Marketing communications (where required by law)

You can withdraw consent at any time through your settings or by contacting us.

11. Changes to This Privacy Policy

We may update this policy from time to time. When we do:

• We will post changes on this page and update the “Effective Date”
• For significant changes, we will provide prominent notice (such as email notification)
• Continued use of Plugilo after changes take effect means you accept the updated policy

12. Contact Us

If you have questions about this Privacy Policy or want to exercise your rights:

Plugilo, Inc.
200 Continental Drive Suite 401
Newark, Delaware 19713
United States

Email: legal@plugilo.com

Help Center: https://corporate.plugilo.com/knowledge-hub/

Cookie & Consent Settings: https://plugilo.com/policy

Data Protection Officer: legal@plugilo.com

Additional information for EEA & Deutschland

1. Introduction

In the following, we provide information about the collection of personal data when using

● our website plugilo.de, plugilo.com, plugiloinc.com

● our profiles in social media.

Personal data is any data that can be related to a specific natural person, such as their name or IP address.

2. Contact details

The controller within the meaning of Art. 4 para. 7 EU General Data Protection Regulation (GDPR) is plugilo Inc., Continental Drive 200 , Newark, United States, email: info@plugilo.de. We are legally represented by Michael Mohr.

Our data protection officer can be reached via heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu , E-Mail: datenschutz@heydata.eu.

3. Scope of data processing, processing purposes and legal bases

We detail the scope of data processing, processing purposes and legal bases below. In

principle, the following come into consideration as the legal basis for data processing:

● Art. 6 para. 1 s. 1 lit. a GDPR serves as our legal basis for processing operations for which we obtain consent.

● Art. 6 para. 1 s. 1 lit. b GDPR is the legal basis insofar as the processing of

personal data is necessary for the performance of a contract, e.g. if a site visitor purchases a product from us or we perform a service for him. This legal basis also applies to processing that is necessary for pre-contractual measures, such as in the case of inquiries about our products or services.

● Art. 6 para. 1 s. 1 lit. c GDPR applies if we fulfill a legal obligation by processing personal data, as may be the case, for example, in tax law.

● Art. 6 para. 1 s. 1 lit. f GDPR serves as the legal basis when we can rely on legitimate interests to process personal data, e.g. for cookies that are necessary for the technical operation of our website.

4. Data processing outside the EEA

Insofar as we transfer data to service providers or other third parties outside the EEA,the security of the data during the transfer is guaranteed by adequacy decisions of theEU Commission, insofar as they exist (e.g. for Great Britain, Canada and Israel) (Art. 45 para. 3 GDPR).

In the case of data transfer to service providers in the USA, the legal basis for the data transfer is an adequacy decision of the EU Commission if the service provider has also certified itself under the EU US Data Privacy Framework.

In other cases (e.g. if no adequacy decision exists), the legal basis for the data transfer are usually, i.e. unless we indicate otherwise, standard contractual clauses. These are a set of rules adopted by the EU Commission and are part of the contract with the respective third party. According to Art. 46 para. 2 lit. b GDPR, they ensure the security of the data transfer. Many of the providers have given contractual guarantees that go beyond the standard contractual clauses to protect the data. These include, for example, guarantees regarding the encryption of data or regarding an obligation on the part of the third party to notify data subjects if law enforcement agencies wish to access the respective data.

5. Storage duration

Unless expressly stated in this privacy policy, the data stored by us will be deleted as soon as they are no longer required for their intended purpose and no legal obligations to retain data conflict with the deletion. If the data are not deleted because they are required for other and legally permissible purposes, their processing is restricted, i.e. the data are blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax law reasons.

6. Rights of data subjects

Data subjects have the following rights against us with regard to their personal data:

● Right of access,

● Right to correction or deletion,

● Right to limit processing,

● Right to object to the processing,

- Right to data transferability,
- Right to revoke a given consent at any time.

Data subjects also have the right to complain to a data protection supervisory authority about the processing of their personal data. Contact details of the data protection supervisory authorities are available at https://www.bfdi.bund.de/EN/Service/Anschriften/Laender/Laender-node.html.

7. Obligation to provide data

Within the scope of the business or other relationship, customers, prospective customers or third parties need to provide us with personal data that is necessary for the establishment, execution and termination of a business or other relationship or that we are legally obliged to collect. Without this data, we will generally have to refuse to conclude the contract or to provide a service or will no longer be able to perform an existing contract or other relationship.

Mandatory data are marked as such.

8. No automatic decision making in individual cases

As a matter of principle, we do not use a fully automated decision-making process in accordance with article 22 GDPR to establish and implement the business or other relationship. Should we use these procedures in individual cases, we will inform of this separately if this is required by law.

9. Making contact

When contacting us, e.g. by e-mail or telephone, the data provided to us (e.g. names and e-mail addresses) will be stored by us in order to answer questions. The legal basis for the processing is our legitimate interest (Art. 6 para. 1 s. 1 lit. f GDPR) to answer inquiries directed to us. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if there are legal retention obligations.

10. Competitions

Occasionally, we offer competitions via our website or in other ways. We process the data requested in these competitions in order to determine and notify the winners. Afterwards, we delete the data. It may also be that we only offer competitions for existing customers. In this case, we only process the name to determine the winners and the contact data to notify the winners. It is our legitimate interest to offer competitions to attract customers or to interact with our existing customers. The legal basis for data processing is Art. 6 para. 1 s. 1 lit. f GDPR.

11. Newsletter

We reserve the right to inform customers who have already used services from us or purchased goods from time to time by e-mail or other means about our offers, if they have not objected to this. The legal basis for this data processing is Art. 6 para. 1 s. 1 lit. f GDPR. Our legitimate interest is to conduct direct advertising (recital 47 GDPR). Customers can object to the use of their e-mail address for advertising purposes at any time without incurring additional costs, for example via the link at the end of each e-mail or by sending an e-mail to our above-mentioned e-mail address.

Interested parties have the option to subscribe to a free newsletter. We process the data provided during registration exclusively for sending the newsletter. Subscription takes place by selecting the corresponding field on our website, by ticking the corresponding field in a paper document or by another clear action, whereby interested parties declare their consent to the processing of their data, so that the legal basis is Art. 6 para. p. 1 lit. a GDPR. Consent can be revoked at any time, e.g. by clicking the corresponding link in the newsletter or notifying our e-mail address given above. The processing of the data until revocation remains lawful even in the event of revocation.

Based on the consent of the recipients (Art. 6 para. 1 s. 1 lit. a GDPR), we also measure the opening and click-through rate of our newsletters to understand what is relevant for our audience.

● We send newsletters with the tool Brevo of the provider Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin . The provider processes content, usage, meta/communication data and contact data in the process in the EU. Further information is available in the provider's privacy policy at https://www.sendinblue.com/legal/privacypolicy/ .

12. Data processing on our website

Notice for website visitors from Germany Our website stores information in the terminal equipment of website visitors (e.g. cookies) or accesses information that is already stored in the terminal equipment (e.g. IP addresses). What information this is in detail can be found in the following sections.

This storage and access is based on the following provisions:

● Insofar as this storage or access is absolutely necessary for us to provide the service of our website expressly requested by website visitors (e.g., to carry out a chatbot used by the website visitor or to ensure the IT security of our website), it is carried out on the basis of Section 25 para. 2 no. 2 of the German Telecommunications Digital Services Data Protection Act (Telekommunikation-Digitale-Dienste-Datenschutzgesetz, "TDDDG").

● Otherwise, this storage or access takes place on the basis of the website visitor's consent (Section 25 para. 1 TDDDG).

The subsequent data processing is carried out in accordance with the following sections and on the basis of the provisions of the GDPR.

13. Informative use of our website

During the informative use of the website, i.e. when site visitors do not separately transmit information to us, we collect the personal data that the browser transmits to our server in order to ensure the stability and security of our website. This is our legitimate interest, so that the legal basis is Art. 6 para. 1 s. 1 lit. f GDPR.

These data are:

● IP address

● Date and time of the request

● Time zone difference to Greenwich Mean Time (GMT)

● Content of the request (specific page)

● Access status/HTTP status code

● Amount of data transferred in each case

● Website from which the request comes

● Browser

● Operating system and its interface

● Language and version of the browser software.

This data is also stored in log files. They are deleted when their storage is no longer necessary, at the latest after 14 days.

14. Web hosting and provision of the website

Our website is hosted by Microsoft Azure. The provider is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland. In doing so, the provider processes the personal data transmitted via the website, e.g. content, usage, meta/communication data or contact data, in the EU. Further information can be found in the provider's privacy policy at https://privacy.microsoft.com/en-gb/privacystatement.

It is our legitimate interest to provide a website, so the legal basis of the described data processing is Art. 6 para. 1 s. 1 lit. f GDPR.

We use the content delivery network Azure CDN for our website. The provider is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA. The provider thereby processes the personal data transmitted via the website, e.g. content, usage, meta/communication data or contact data in the EU. Further information can be found in the provider's privacy policy at https://privacy.microsoft.com/de-de/privacystatement?culture=de-de&country=DE.

We have a legitimate interest in using sufficient storage and delivery capacity to ensure optimal data throughput even during large peak loads. Therefore, the legal basis of the described data processing is Art. 6 para. 1 s. 1 lit. f GDPR.

We use the content delivery network Azure CDN for our website. The provider is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA . The provider thereby processes the personal data transmitted via the website, e.g. content, usage, meta/communication data or contact data in the EU. Further information can be found in the provider's privacy policy at https://privacy.microsoft.com/de-de/privacystatement?culture=de-de&country=DE .

We have a legitimate interest in using sufficient storage and delivery capacity to ensure optimal data throughput even during large peak loads. Therefore, the legal basis of the described data processing is Art. 6 para. 1 s. 1 lit. f GDPR.

Legal basis of the transfer to a country outside the EEA are .

15. Vacant positions

We publish vacant positions on our website, on pages linked to the website or on third-party websites.

The processing of the data provided as part of the application is carried out for the purpose of implementing the application process. Insofar as this is necessary for our decision to establish an employment relationship, the legal basis is Art. 88 para. GDPR in conjunction with Sec. 26

para. 1 of the German Data Protection Act (Bundesdatenschutzgesetz). We have marked the data required to carry out the application process accordingly or refer to them. If applicants do not provide this data, we cannot process the application.Further data is voluntary and not required for an application. If applicants provide further information, the basis is their consent (Art. 6para. 1 s. 1 lit. a GDPR).

We ask applicants to refrain from providing information on political opinions, religious beliefs and similarly sensitive data in their CV and cover letter. They are not required for an application. If applicants nevertheless provide such information, we cannot prevent their processing as part of the processing of the resume or cover letter. Their processing is then also based on the consent of the applicants (Art. 9 para. 2 lit. aGDPR).

Finally, we process the applicants' data for further application procedures if they have given us their consent to do so. In this case, the legal basis is Art. 6 para. 1 s. 1 lit. a GDPR.

We pass on the applicants' data to the responsible employees in the HR department, to our data processors in the area of recruiting and to the employees otherwise involved in the application process.

If we enter into an employment relationship with the applicant following the application process, we delete the data only after the employment relationship has ended.

Otherwise, we delete the data no later than six months after rejecting an applicant.

If applicants have given us their consent to use their data for further application procedures as well, we will not delete their data until one year after receiving the application.

16. Customer account

Site visitors can open a customer account on our website. We process the data requested in this context based on the consent of the site visitor. We process the data requested in this context to fulfill the respective user contract concluded for the account, so that the legal basis for the processing is Art. 6 para. 1 p. 1 lit. b GDPR.

17. Single-sign on

Users can log in to our website using one or more single sign-on methods. In doing so, they use the login data already created for a provider. The prerequisite is that the user is already registered with the respective provider. When a user logs in using a single sign-on procedure, we receive information from the provider that the user is logged in to the provider and the provider receives information that the user is using the single sign-on procedure on our website. Depending on the user's settings in his account on the provider's site, additional information may be provided to us by the provider. The legal basis for this processing is Art. 6 para. 1

sentence 1 lit. f GDPR. We have a legitimate interest in providing users with a simple log-in option. At the same time, the interests of the users are safeguarded, as use is only voluntary.

Providers of the offered method(s) are:

● Apple Inc, Infinite Loop, Cupertino, CA 95014, USA (privacy policy:

https://www.apple.com/legal/privacy/de-ww/)

● Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (privacy

policy: https://policies.google.com/privacy)

● own single sign on

18. Technically necessary cookies

Our website sets cookies. Cookies are small text files that are stored in the web browser on the end device of a site visitor. Cookies help to make the offer more user-friendly, effective and secure. Insofar as these cookies are necessary for the operation of our website or its functions (hereinafter "Technically Necessary Cookies"), the legal basis for the associated data processing is Art. 6 para. 1 s. 1 lit. f GDPR. We have a legitimate interest in providing customers and other site visitors with a functional website. Specifically, we set technically necessary cookies for the following purpose or purposes:

• Cookies, to save login data

• Cookies, to apply language settings

19. Use of the Plugilo platform and Plugilo Dock

Users can register on the plugilo platform and follow companies, products, topics or people that interest them. On the platform, these are referred to as stacks and cards. The purpose of the plugilo platform is to connect all players within a supply chain, from the manufacturer to the end customer, in both the B2B and B2C sectors. The company behind the respective stack or card has the opportunity to view information about its own followers. The first name, surname and shortened email address of the user are displayed. Users can configure on the platform how often they want to be notified about the companies, stacks and cards they follow. Users can also object to the visibility of stacks and cards they follow or hide their name. Companies have the option of sending targeted information to their own followers via the platform or communicating with them directly via chat.

Users can also use the Plugilo Dock on external websites. In this case, the user can use the bookmarking function, which enables them to save products or articles from the website as cards and store them in their Plugilo Dock. Registered users can access their saved cards

across all devices and in the app. Unregistered users can still retrieve them via fingerprinting within the respective browser (see below).

20. Fingerprinting

Plugilo uses device fingerprinting technology to enhance the user experience by enabling the bookmarking of content (such as articles, products and others) across multiple devices and domains. This technology allows us to recognise the device when the user returns and ensures that the bookmarked content is always accessible, even without logging in.

Device fingerprinting collects technical information about the device, including your browser type, operating system, screen resolution, time zone, installed fonts and other unique characteristics. This information is combined to create a unique identifier for the device, which Plugilo uses to save your bookmarks and improve the usability of the widget.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. a GDPR. The processing is based on consent. Data subjects may revoke their consent at any time by contacting us, for example, using the contact details provided in our privacy policy. The revocation does not affect the lawfulness of the processing until the revocation.

21. Third parties

Hotjar

We use Hotjar for analytics. The provider is Hotjar Ltd., Dragonara Business Centre, 5th Floor, Dragonara Road, Paceville St Julian's, STJ 3141, Malta. The provider processes usage data (e.g. web pages visited, interest in content, access times), meta/communication data (e.g. device information, IP addresses) in the EU. The legal basis for the processing is Art. 6 para. 1 s. 1 lit. a GDPR . The processing is based on consent. Data subjects may revoke their consent at any time by contacting us, for example, using the contact details provided in our privacy policy. The revocation does not affect the lawfulness of the processing until the revocation.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://www.hotjar.com/legal/policies/privacy/.

Iubenda

We use Iubenda to manage consents. The provider is iubenda s.r.l, Via San Raffaele, 1 - 20121 Milan, Italy. The provider processes meta/communication data (e.g. device information, IP addresses) in the EU.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. c DSGVO . The processing is necessary for the fulfillment of a legal obligation to which we are subject.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://www.iubenda.com/privacy-policy/94654098.

Google Analytics

We use Google Analytics for analytics. The provider is Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA. The provider processes usage data (e.g. web pages visited, interest in content, access times), meta/communication data (e.g. device

information, IP addresses) in the USA in the USA.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. a GDPR . The processing is based on consent. Data subjects may revoke their consent at any time by contacting us, for example, using the contact details provided in our privacy policy. The revocation does not affect the lawfulness of the processing until the revocation.

The transfer of personal data to a country outside the EEA takes place on the legal basis adequacy decision. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed because the EU Commission has decided as part of an adequacy decision in accordance with Art. 45 para. 3 GDPR that the third country ensures an adequate level of protection.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://business.safety.google/privacy/.

Google Tag Manager

We use Google Tag Manager for advertising, for analytics. The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. The provider processes usage data (e.g. web pages visited, interest in content, access times) in the USA in the USA.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. a GDPR . The processing is based on consent. Data subjects may revoke their consent at any time by contacting us, for example, using the contact details provided in our privacy policy. The revocation does not affect the lawfulness of the processing until the revocation.

The transfer of personal data to a country outside the EEA takes place on the legal basis adequacy decision. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed because the EU Commission has decided as part of an adequacy decision in accordance with Art. 45 para. 3 GDPR that the third country ensures an adequate level of protection.

We delete the data when the purpose for which it was collected no longer applies. Further information is available in the provider's privacy policy at https://business.safety.google/privacy/.

Meta Pixel

We use Meta Pixel for analytics. The provider is Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. The provider processes usage data (e.g. web pages visited, interest in content, access times) in the USA in the USA. The legal basis for the processing is Art. 6 para. 1 s. 1 lit. a GDPR . The processing is based on consent. Data subjects may revoke their consent at any time by contacting us, for example, using the contact details provided in our privacy policy. The revocation does not affect the lawfulness of the processing until the revocation.

The transfer of personal data to a country outside the EEA takes place on the legal basis adequacy decision. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed because the EU Commission has decided as part of an adequacy decision in accordance with Art. 45 para. 3 GDPR that the third country ensures an adequate level of protection.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's privacy policy at https://www.facebook.com/policy.php.

Kochava

We use Kochava for affiliate marketing. The provider is Kochava Inc., 201 Church St, Sandpoint, ID 83864, USA. The provider processes usage data (e.g. web pages visited, interest in content, access times), meta/communication data (e.g. device information, IP addresses), contact data (e.g. e-mail addresses, telephone numbers) in the USA in the USA.

The legal basis for the processing is Art. 6 para. 1 s. 1 lit. a GDPR . The processing is based on consent. Data subjects may revoke their consent at any time by contacting us, for example, using the contact details provided in our privacy policy. The revocation does not affect the lawfulness of the processing until the revocation.

The transfer of personal data to a country outside the EEA takes place on the legal basis adequacy decision. The security of the data transferred to the third country (i.e. a country outside the EEA) is guaranteed because the EU Commission has decided as part of an adequacy decision in accordance with Art. 45 para. 3 GDPR that the third country ensures an adequate level of protection.

The data will be deleted when the purpose for which it was collected no longer applies and there is no obligation to retain it. Further information is available in the provider's

privacy policy at https://www.kochava.com/legal/website-visitor-privacy-policy/?int-

link=menu-website-privacy.

heyData

We have integrated a data protection seal on our website. The provider is heyData GmbH, Schützenstraße 5, 10117 Berlin, Germany. The provider processes meta/communication data (e.g. IP addresses) in the EU.

The legal basis of the processing is Art. 6 para. 1 s. 1 lit. f GDPR. We have a legitimate interest in providing website visitors with confirmation of our data privacy compliance. At the same time, the provider has a legitimate interest in ensuring that only customers with existing contracts use its seals, which is why a mere image copy of the certificate is not a viable alternative as confirmation.

As the data is masked after collection, there is no possibility to identify website visitors. Further information is available in the privacy policy of the provider at https://heydata.eu/en/privacy-policy .

Cloudflare

For certain technical endpoints, we use Cloudflare, provided by Cloudflare, Inc., 101Townsend Street, San Francisco, CA 94107, USA, to make our services more secureand reliable. Cloudflare is used as an upstream reverse proxy and helps us, inparticular, to protect against unauthorized access, automated requests, andattacks on our systems, as well as to ensure the availability of our services.

As part of this security function, Cloudflare may process the following technicaldata in particular: IP address, user agent, accessed URL or request path, HTTPheaders, referrer, technical TLS/connection information, and security andchallenge data required to detect and defend against automated or unauthorizedaccess.

This processing is carried out for the purpose of ensuring the security, integrity,and availability of our technical systems. The legal basis is our legitimate interest inthe secure and uninterrupted operation of our services pursuant to Article 6(1)(f) ofthe GDPR.

Cloudflare may process data in data centers both within and outside the EuropeanUnion. To the extent that personal data is transferred to third countries, inparticular the United States, this is done on the basis of appropriate safeguards, inparticular the EU-U.S. Data Privacy Framework and/or the Standard ContractualClauses. We have a data processing agreement in place with Cloudflare.

We do not use Cloudflare for marketing or advertising purposes. There is nofurther use of the data for analysis or tracking purposes.

22. Data processing on social media platforms

We are represented in social media networks in order to present our organization and our services there. The operators of these networks regularly process their users' data for advertising purposes. Among other things, they create user profiles from their online behavior,

which are used, for example, to show advertising on the pages of the networks and elsewhere on the Internet that corresponds to the interests of the users.

To this end, the operators of the networks store information on user behavior in cookies on the users' computers. Furthermore, it cannot be ruled out that the operators merge this information with other data. Users can obtain further information and instructions on how to object to processing by the site operators in the data protection declarations of the respective operators listed below. It is also possible that the operators or their servers are located in non-EU countries, so that they process data there. This may result in risks for users, e.g. because it is more difficult to enforce their rights or because government agencies access the data.

If users of the networks contact us via our profiles, we process the data provided to us in order to respond to the inquiries. This is our legitimate interest, so that the legal basis is Art. 6 para. 1 s. 1 lit. f GDPR.

Facebook

We maintain a profile on Facebook. The operator is Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. The privacy policy is available here: https://www.facebook.com/policy.php. A possibility to object to data processing arises via settings for advertisements: https://www.facebook.com/settings?tab=ads.We are joint controllers for processing the data of visitors to our profile on the basis of an agreement within the meaning of Art. 26 GDPR with Facebook. Facebook explains exactly what data is processed at https://www.facebook.com/legal/terms/information_about_page_insights_data. Data subjects can exercise their rights both against us and against Facebook. However, according to our agreement with Facebook, we are obliged to forward requests to Facebook. Data subjects will therefore receive a faster response if they contact Facebook directly.

Tiktok

We maintain a profile on Tiktok. The operator is TikTok Technology Limited, whose registered office is at 10 Earlsfort Terrace, Dublin, D02 T380, Ireland. The privacy policy is available here: https://www.tiktok.com/de/privacy-policy.

YouTube

We maintain a profile on YouTube. The operator is Google Ireland Limited Gordon House, Barrow Street Dublin 4. Ireland. The privacy policy is available here:

https://policies.google.com/privacy?hl=de.

X (formerly Twitter)

We maintain a profile on X. The operator is Twitter Inc, 1355 Market Street, Suite 900, San Francisco, CA 94103, USA. The privacy policy is available here:

https://twitter.com/de/privacy. One way to object to data processing is via the settings

for advertisements: https://twitter.com/personalization.

LinkedIn

We maintain a profile on LinkedIn. The operator is LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland. The privacy policy is available here:

https://www.linkedin.com/legal/privacy-policy?_l=de_DE. One way to object to data processing is via the settings for advertisements:

https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out.

23. Changes to this privacy policy

We reserve the right to change this privacy policy with effect for the future. A current version is always available here.

24. Questions and comments

If you have any questions or comments regarding this privacy policy, please feel free to contact us using the contact information provided above.

* * *

Effective Date: Jun 22, 2026

This policy applies worldwide.

Last Updated: Jun 22, 2026