E-Mail: global@cosmeterie.com

# Data Protection Policy

Overview
Welcome to www.cosmeterie.com! In accordance with Art 13, Art 14 GDPR and § 165 para 3 TKG, we hereby provide you with comprehensive information regarding all data processing activities. Please familiarise yourself with which personal data (hereinafter referred to as "data") is processed, as well as how and why, when you:

1. Visit our website
2. Subscribe to our online marketing channels
3. Contact us
4. Use our webshop
5. Order our products via Amazon Marketplace
6. Rate your shopping experience
7. Or otherwise enter into a business relationship with us.
   As well as:
8. How long your data is stored
9. Which data we collect from other sources (Art. 14 GDPR)
10. Whether automated decision-making takes place
11. Your rights regarding data processing, as well as
12. The identity of the controller, the contact details of our Data Protection Officer, and how you can contact us.

For residents of Switzerland: The declarations in this Data Protection Policy also apply mutatis mutandis to persons resident in Switzerland and also fulfil all the data requirements stipulated in Art. 19 of the Swiss Data Protection Act. The terms "personal data", "processing" and "processor" in the Swiss Data Protection Act correspond to the terms "personal data", "processing" and "processor" in the GDPR.

For residents of the United Kingdom: The declarations in this Data Protection Policy also apply mutatis mutandis to persons resident in the United Kingdom and also fulfil the data requirements stipulated in the UK-GDPR.

We may make changes to this Privacy Policy from time to time to reflect changes in our practices or for other operational, legal or regulatory reasons.

1) What data do we process when you visit our website?
When you visit our website, the following categories of your data may be processed:

- Selected language
- Browser type
- Type of end device used to access the site
- Operating system
- Country
- Date, time and duration of access
- IP address
- Pages visited on our website, including entry and exit pages
- Data that you enter via a contact form

These categories of data are processed only to the extent necessary in each case. Unless a different legal basis is specified below, the processing is justified by our overriding legitimate interest in ensuring the secure and proper operation of our website (Article 6(1)(f) GDPR).

For the operation of our website, it may be necessary for us to transmit your data to the following recipients:

| Service provider and data protection information of the provider | Description | Place of processing | Legal bases for data transmission |
|---|---|---|---|
| Hetzner Online GmbH | Website hosting including backup storage | EU/EEA | Order processing pursuant to Art. 28 GDPR |
| Fastly, Inc. | Content-Delivery-Network | EU/EEA, USA | Processing pursuant to Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) |

Services contingent on your consent when you visit our website
You can manage your consents or revocations of the options described in this section at any time through our "Privacy settings" banner. This is the pop-up window that appears when you visit our website for the first time, which you can also call up at any time later by clicking on the ‘Privacy settings’ link in the footer section at the bottom of our website. In all cases, however, the data processing carried out up to the time of cancellation remains justified.

Your consent to the processing of your data by services that process your data within the EU or the EEA, or in other countries for which there is a valid EU adequacy decision according to Art. 45 GDPR, are based on Art 6 Para 1 lit a GDPR. Such an adequacy decision ensures an adequate level of data protection based on the European Commission's standards.

On July 10, 2023, the European Commission published a decision regarding adequacy for the USA. According to the EU-US Data Privacy Framework (EU-US DPF), data transfers to service providers in the USA are deemed adequate if they are certified as per the Data Privacy Framework (DPF) Program.

Your consent to data processing via services that process your data in countries outside of the EU or EEA that do not have an adequacy decision, or, by services in the United States that have not yet been "Data Privacy Framework Program (DPF)" certified, is based on Art 6 para 1 lit. a in connection with Art 49(1)(a) of the GDPR (exceptions for specific cases). Your rights concerning the processing of your data in such cases cannot be guaranteed, which we hereby expressly point out before you give your consent.

"Cookies" and similar "third-party services"

The above categories of data, which are processed when you visit our website, may also be processed by so-called "cookies" or other "third-party services". Cookies are small text files that are stored on your device and may include, for example, personal settings, preferences, or browsing history, which can then quickly be retrieved by the web server at a later time.

Cookies required for technical purposes are used solely to ensure the functionality of our website and do not require your consent. They enable features such as adding items to the shopping basket or saving them for later, navigating the website, and logging into customer accounts. These cookies are used only to the extent absolutely required. The use of these cookies required for technical purposes is essential for pre-contractual measures (Art 6 Para 1 lit b GDPR) or is justified by our overriding legitimate interest in the functionality of our website (Art 6 Para 1 lit f GDPR).

In addition to these cookies required for technical purposes, we may also use "third-party services" (e.g. "marketing cookies", "analytics cookies", "non-essential cookies", "pixel", "fingerprinting", "local/session storage" or similar technologies) if we have your prior, voluntary approval to do so. These services enable us to better understand and evaluate your interests. With the help of these services, we can merge your surfing behaviour beyond the boundaries of our website with data from other websites. This data allows us to better understand the interests of visitors to our websites and to address them in a more targeted manner. To this end, the categories of your data required for the purpose will also be transmitted to the respective service provider. We respect that not every visitor to our website wants this. Therefore, we only process your data through these third-party services if you give us your prior consent to do so.

Subject to your prior consent, the following third-party services may be activated on our websites with their respective cookies which are not required for technical purposes. You can find out which of these third-party services are available for selection at www.cosmeterie.com directly in our "privacy settings" banner.

| Service | Description | Duration of storage (maximum) | Place of processing | Legal basis for data transfer to the service provider | Service provider and data protection information of the provider |
|---|---|---|---|---|---|
| A/B Testing | Enables the implementation and accurate evaluation of A/B tests | 6 months | EU/EEA | Server-side hosting, no data is transmitted to external service providers. | - |
| AWIN | Targeted display of online advertising | 30 days | EU/EEA | Joint responsibility per Art. 26 GDPR under the conclusion of a joint responsibility agreement. Both parties are contact points for the exercise of rights according to Art.15-20 GDPR | AWIN AG |
| Brevo | Analysis and statistical evaluation of the website | 24 months | EU/EEA | Data processing according to Art. 28 GDPR | SendinBlue GmbH |
| Clarity | Analysis and statistical evaluation of the website | 12 months | EU/EEA, USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Microsoft Corporation |
| creativecdn.com | Creating personalised advertising offers | 12 months | EU/EEA | Joint responsibility per Art. 26 GDPR under the conclusion of a joint responsibility agreement. Both parties are contact points for the exercise of rights according to Art.15-20 GDPR | RTB House S.A. |

| | | | | | |
|---|---|---|---|---|---|
| Criteo | Creating personalised advertising offers | 13 months | EU/EEA | Joint responsibility per Art. 26 GDPR under the conclusion of a joint responsibility agreement. Both parties are contact points for the exercise of rights according to Art.15-20 GDPR | Criteo SA |
| Floodlight | Performance analysis and optimisation of online advertising campaigns (the provider may use the data collected to contextualise and personalise ads on its own advertising network, especially if you are logged into an existing account from the service) | 2 years | EU/EEA, USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |
| Freshchat | Possibility to contact customer service via chat. | 400 days | EU/EEA, USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Freshworks Inc. |
| Freshdesk | Possibility to contact customer service via a phone service. | 400 days | EU/EEA, USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Freshworks Inc. |
| Klarna | Displaying available Klarna payment options to boost purchase motivation | As stated in the service provider's privacy policy | EU/EEA | Independent responsibility of the service provider as per Art 4(7) GDPR | Klarna Bank AB (publ) |
| LinkedIn Insight Tag | Performance measurement and optimisation of online advertising (the provider may use the data collected to contextualise and personalise the ads of its own advertising network, especially if you are logged into an existing account of the service) | 6 months | EU/EEA, USA | Joint responsibility per Art 26 GDPR by concluding a joint responsibility agreement with certification of the service provider as per the Data Privacy Framework (DPF) Programme. The provider is the point of contact for exercising the rights stipulated in Art 15-20 GDPR | Meta Platforms Ireland Limited |
| Meta-Pixel | Performance analysis and optimisation of online advertising campaigns (the provider may use the data collected to contextualise and personalise ads on its own advertising network, especially if you are logged into an existing account from the service) | 3 months | EU/EEA/USA | Joint responsibility per Art. 26 GDPR under the conclusion of a joint responsibility agreement with certification of the service provider as per the Data Privacy Framework (DPF) Program. The provider is the contact point for exercising the rights as stipulated in Art 15-20 GDPR. | Meta Platforms Ireland Limited |

| | | | | | |
|---|---|---|---|---|---|
| Google Ads | Targeted display of online advertising (The provider may use the data collected to contextualise and personalise the ads of its own advertising network, especially if you are logged into an existing account of the service) | 3 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |
| Google Analytics | Analysis and statistical evaluation of the website (under privacy-protecting settings, in particular, the deactivation of Google Signals, User ID, personalised ads, data sharing for Google products and services, and the restriction on collection of location and device data from individual regions). | maximum 14 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |
| Google Consent Mode | Upstream interface for legally binding consent to the provider as per the Digital Markets Act for all its marketing and advertising services. Implemented in the basic version, according to which no data is transmitted to the provider in the event of refusal. | 14 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |
| Google Customer Reviews | Participation in surveys | 90 gays | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |
| Google Tag Manager | Integration of Google Tag Manager for easy reloading of services | 24 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link https://business.safety.google/privacy/ |
| Hotjar | Optimisation of our online offers and website presentation | 12 months | EU/EEA | Data processing per Art. 28 GDPR | Hotjar Ltd. |
| Hubspot | Optimisation of our online offers | 6 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | HubSpot, Inc. |

| | | | | | |
|---|---|---|---|---|---|
| Click-based product recommendations | Display of recommended or similar products based on the last 25 products viewed on our website. | 12 months | EU/EEA | Server-side hosting; no data is transferred to external service providers. | - |
| Microsoft Advertising | Targeted display of online advertising (The provider may use the data collected to contextualise and personalise the ads of its own advertising network, especially if you are logged into an existing account of the service) | 13 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Microsoft Corporation |
| Omniconvert | Optimisation of our online offers and website presentation | 6 months | EU/EEA | Data processing according to Art. 28 GDPR | Omniconvert SRL |
| Pinterest Tag | Performance measurement and targeted display of online advertising | 12 months | EU/EEA, US | Data processing per Art. 28 GDPR under conclusion of the final standard data protection clauses as per Art. 46 Para. 3 lit a GDPR | Pinterest Inc. |
| reCAPTCHA | A security service that keeps our contact forms safe from misuse and automated submissions | 6 months | EU/EEA, US | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |
| Sovendus | Display and performance measurement of Sovendus voucher offers | 30 days | EU/EEA | Independent/separate controllership of the service provider pursuant to Article 4(7) GDPR. | Sovendus GmbH |
| TikTok Pixel | Measuring the success and optimisation of online advertising (The provider may use the data collected to contextualise and personalise the ads of its own advertising network, especially if you are logged into an existing account of the service) | 13 months | EU/EEA, US, Malaysia, Singapore | Joint responsibility per Art. 26 GDPR under the conclusion of an agreement on joint responsibility, including the final standard data protection clauses as per Art. 46 Para. 3 lit a GDPR. The provider is the point of contact for exercising rights as per Articles 15-20 GDPR. | TikTok Technology Limited |
| Tracify | Performance measurement and optimisation of online advertising | 400 days | EU/EEA | Data processing per Art. 28 GDPR | Tracify GmbH |

| | | | | | |
|---|---|---|---|---|---|
| UET (Universal Event Tracking) Consent mode by Microsoft | Upstream interface for legally valid consent to the provider in compliance with the Digital Markets Act for all its marketing and advertising services. Implemented in the basic version, whereby no data is transmitted to the provider in the event of refusal. | 13 months | EU/EEA, USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Microsoft Corporation |
| uptain | Creation of personalised advertising and business offers | 12 months | EU/EEA | Data processing per Art. 28 GDPR | uptain GmbH |
| Vimeo | Playing Vimeo video services | 24 months | USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Vimeo.com, Inc. |
| Youtube | Playing YouTube videos. The service is implemented in the "extended data protection mode", which excludes "Tracking" by the provider and only transmits data that is absolutely essential for playing videos. | 24 months | EU/EEA, USA | Data processing per Art. 28 GDPR, with the service provider certified under the Data Privacy Framework (DPF) Program. | Google Ireland Limited<br>For more information on how Google handles data responsibly, please click on this link: https://business.safety.google/privacy/ |

Matching of customer data with online advertising providers

On the basis of your prior voluntary consent, we may also send you targeted ads external to our websites via the advertising channels of the online advertising providers listed below, but only if you are already registered with these providers or use their services (‘matching of customer data’ or ‘customer match’). For this purpose, we use your personal data in encrypted form to match it with the customer database of the respective providers. For this purpose, only data anonymised with an encryption process is used, which means that providers who do not already have your data will never receive your data. This is ensured by the fact that before your data is transmitted to the providers, we encrypt your data using a hash procedure, which results in a non-reversible character string (‘hash value’) that does not allow any conclusions to be drawn about your data. Only this hash value is transmitted to the providers. The providers encrypt their data using the same method. We then compare our hash value with the hash value of the provider. If our hash value matches that of one or more providers, we can be certain that you are already using the services of the respective provider and that we can therefore send you targeted ads via their advertising channels.

In order to offer you such ads through external online advertising providers, the following categories of data may be processed in addition to the data processed during your visit to our website:

- E-mail address
- Telephone number
- First name
- Last name
- Country
- Postcode
- Shopping behaviour and favourite products

Subject to your prior voluntary consent, we may send you targeted ads via the channels of the following online advertising providers after a successful ‘matching of customer data’ has been completed.

| Service | Place of processing | Provider and data privacy information of the provider |
|---|---|---|
| Criteo audience match | EU/EEA | Criteo (Criteo SA) |
| Google Customer Match | EU/EEA, USA | Google (Google Ireland Limited)<br>For additional information on the responsible use of data by Google, click here: https://business.safety.google/privacy/ |

| | | |
|---|---|---|
| LinkedIn Matched Audiences | EU/EEA, USA | LinkedIn (LinkedIn Ireland Unlimited Company) |
| Meta Custom Audiences | EU/EEA, USA | Meta (Meta Platforms Ireland Limited) |
| Microsoft Customer Match | EU/EEA, USA | Bing (Microsoft Corporation) |
| Pinterest customer list | EU/EEA | Pinterest (Pinterest Europe Ltd.) |
| TikTok Custom Audience | EU/EEA, USA, Malaysia, Singapore | TikTok (TikTok Technology Limited) |

Google Enhanced Conversions

Based on your prior voluntary consent, we may use Google's 'Enhanced Conversions' technology. This enables us to better understand and evaluate the success of our online advertising and to optimise our advertising strategies.

We will use your personal data to compare it with Google's customer database for this purpose. However, we will only use data anonymised by an encryption process, which means that Google will never receive your data if you do not already have a Google account. This is achieved by encrypting your data using a hashing process before transmission, which results in a non-reversible character string ('hash value') that does not allow any information to be inferred from your data. This hash value is generated and transmitted to Google only if you carry out certain predefined actions or 'conversions' (such as orders) on our website. When such a conversion occurs, Google compares the hash value of your data with its own hash values, which are encrypted using the same method. If they match, your conversion can be assigned to your Google account and thus notify us of the success of our advertising placement.

The following categories of your data may be processed in encrypted and anonymised form:

- E-mail address
- Telephone number

| Service | Place of processing | Provider and data privacy information of the provider |
|---|---|---|
| Google Enhanced Conversions | EU/EEA, USA | Google (Google Ireland Limited)<br>For additional information on the responsible use of data by Google, click here: https://business.safety.google/privacy/ |

Click Fraud Technology and Bot Detection
If you reach our website by clicking on advertisements displayed via search engines, we can use services to analyse and prevent "click fraud". Click fraud occurs when clicks on ads are generated by automated tools or when multiple clicks on ads are unlikely to be driven by genuine interest.

| Service | Description | Duration of storage | Place of processing | Legal Basis for Data Processing and Data Transmission | Service Provider and Data Protection Information of the Provider |
|---|---|---|---|---|---|
| Ads Defender | Analysis of clicks on Google Ads, transmission of the IP address to Google Ireland Limited if click fraud is suspected | 365 days | EU/EEA | Overriding legitimate interests (Art. 6 Para. 1 lit f GDPR; you can submit your objection to the processing per Art. 21 GDPR here in the form of an "opt-out"), data processing as per Art. 28 GDPR | Hurra Communications GmbH |

If our firewall detects suspicious click behaviour based on preset parameters and a potential attack on our systems cannot be ruled out, we reserve the right to carry out an automatic internal Captcha verification. The authenticity of your enquiry will be verified by asking you to solve a simple picture puzzle. This is carried out without transferring data to third parties. This is justified by our overriding legitimate interest in the security of our systems (Article 6(1)(f) GDPR).

2) What data do we process when you subscribe to our online advertising channels?
E-mail Newsletter
The following categories of data may be processed (in addition to the data processed during your visit to our website) when you subscribe to our e-mail newsletters:

- E-mail address
- Products you have marked as favourites
- Newsletter and personalisation settings

We process this data for the following purposes:

- Sending regular newsletters with general or personalised offers
- Tailoring newsletter content and sending frequency based on a customer segment derived from your previous order history

- Measuring effectiveness

We send our newsletters and measure their effectiveness on the basis of your voluntary consent (Article 6(1)(a) GDPR). You may withdraw your consent at any time by unsubscribing via the link included in each newsletter. The lawfulness of any processing carried out before the withdrawal of your consent remains unaffected.

If you are a registered customer, we may also analyse your previous order history and use this to assign you to a customer segment. This enables us to tailor the content and sending frequency of our newsletters to your presumed interests. You may object to this personalisation at any time via your customer account or by using the relevant link in a personalised newsletter.

This analysis is carried out on the basis of our legitimate interest in making our newsletters more relevant and better tailored to your needs (Article 6(1)(f) GDPR). If you object to personalisation, your objection will remain stored and will continue to be respected even if you later subscribe to the newsletter again.

After objecting to personalisation, you will continue to receive our general newsletter at a limited frequency unless you unsubscribe from the newsletter altogether.

You are not required to provide this data. Without this processing, you will not receive a personalised newsletter or, where applicable, any newsletter at all.

To send our email newsletters, it may be necessary for us to disclose your data to the following recipients::

| Service provider and data protection information of the provider | Description | Place of processing | Legal bases for data transmission |
|---|---|---|---|
| Amazon Web Services EMEA SARL | Sending the e-mail newsletter | EU/EEA | Data processing according to Art. 28 GDPR |
| SendinBlue GmbH | Sending the e-mail newsletter | EU/EEA | Data processing according to Art. 28 GDPR |

3) What data do we process when you contact us?
When you contact us, the following categories of your data may be processed (in addition to the data processed during your visit to our website):

- Name
- Contact details
- E-mail address
- Telephone number
- Any order data
- Correspondence data, including any data you provide to us during communication

We process this data for the following purposes:

- Handling customer enquiries, customer care and other customer support services via e-mail, chat or telephone.

These categories of data are processed to the extent necessary for each case. The processing of this data is justified by our overriding legitimate interest in efficient and satisfactory communication (Art 6 Para 1 lit f GDPR).

For this purpose, it may be necessary for us to transmit your data to the following recipients:

| Service provider and data protection information of the provider | Description | Place of processing | Legal bases for data transmission |
|---|---|---|---|
| Freshworks Inc | Customer inquiries and customer care services via email or chat | EU/EEA, occasionally USA if you contact us via social media platforms | Data processing per Art. 28 GDPR under certification of the service provider as per the Data Privacy Framework (DPF) Program |
| CallOne GmbH | Customer inquiries and customer care services via telephone | EU/EEA | Data processing per Art. 28 GDPR |

4) What data do we process when you use our webshop?
When you use our webshop, the following categories of your data may be processed (in addition to the data processed during your visit to our website):

- Name
- Contact details
- Billing and shipping address
- E-mail address
- Telephone number
- Order and delivery data
- Account and payment data

- Assigned account number
- Data that you enter via a contact form
- Correspondence data, including all data you provide in connection with your order
- Date of birth (in the case of legally required proof of age)

We process this data for the following purposes:

- Processing the entire contractual relationship with you
- Transfer of orders to payment service providers
- Commissioning shipping or forwarding services, including drop-shipping
- Communication for processing orders
- Legally required storage as defined by the § 132 BAO (Federal Fiscal Code)
- Legally permitted direct advertising (e.g.: per mail, e-mail, satisfaction surveys, congratulatory letters, statistical evaluations); We would like to expressly inform you that you can object to the processing of your data for the purpose of direct advertising
- Legally mandated notifications pertaining to product safety
- Prevention and clarification of cases of fraud or attempted fraud
- Assertion and defence of legal claims

Processing these categories of data occurs to the extent necessary in each case and required for the fulfilment of the contract (Art 6 para 1 lit b GDPR), required for the fulfilment of our legal obligations (Art 6 para 1 lit c GDPR) or is justified by our overriding legitimate interest in smoothly running our business (Art 6 para 1 lit f GDPR).

It may be necessary for us to transmit your data to the following categories of recipients as required for the use in our webshop:

| Service provider and data protection information of the provider | Description | Place of processing | Legal bases for data processing and data transmission |
|---|---|---|---|
| Credit card companies, banks, payment providers (Data protection information according to teh website of the selected provider) | Payment processing for your order | Usually EU/EEA – but also third countries in exceptional cases | Fulfilment of contract (Art 6 Para 1 lit b GDPR). If the recipient is in a third country without a valid adequacy decision – Art 49 Para 1 b and e GDPR |
| Logistics service provider (Data protection information according to the website of the selected provider) | Transportation and delivery of orders | Usually EU/EEA – but also third countries in exceptional cases | Fulfilment of contract (Art 6 Para 1 lit b GDPR). If the recipient is in a third country without a valid adequacy decision – Art 49 Para 1 b and e GDPR |
| Drop-shipping or Drop-shipping Service Provider (Data protection information according to the website of the selected provider) | Execution of orders for products that are not in stock and transfer to logistics service providers for transport | Usually EU/EEA – but also third countries in exceptional cases | Fulfilment of contract (Art 6 Para 1 lit b GDPR). If the recipient is in a third country without a valid adequacy decision – Art 49 Para 1 b and e GDPR |
| Debt Collection Service Provider (Data protection information according to the website of the respective service provider) | If necessary, for collecting outstanding debts | Usually EU/EEA countries, but also third countries in exceptional cases | Overriding legitimate interests (Art 6 Para 1 lit f GDPR). If the recipients are in a third country (non-EU) without valid adequacy decisions - Art. 49 Para 1 lit e GDPR |
| Amazon Web Services EMEA SARL | Sending automated emails | EU/EEA | Overriding legitimate interests (Art 6 Para 1 lit f GDPR), data processing in accordance with Art 28 GDPR |

Customer Account

You also have the option to register for a customer account. If you do so, the following additional categories of data may be processed:

- Order history and wish lists
- Product-related data (reviews, testimonials, questions, and answers about products)
- Assigned customer number
- Customer segmentation
- Marketing and personalisation settings

We process this data for the following purposes:

- Storing your information in your customer account, including publishing any product reviews, testimonials, questions and answers that you submit yourself
- Assigning customers to segments in order to offer relevant discounts or benefits
- Determining and displaying personalised product recommendations

The processing of this data is based on your voluntary consent (Article 6(1)(a) GDPR) or, as applicable, on our legitimate interests in obtaining product ratings and reviews, carrying out customer segmentation and providing personalised product recommendations (Article 6(1)(f) GDPR).

You may withdraw your consent to the storage of your customer account at any time. Any processing carried out before the withdrawal of your consent remains lawful. To delete your customer account and all personal data stored in it, select the menu item "Delete my customer account" in your customer account. You are not required to register for a customer account. However, without a customer account, we cannot provide the additional services described above.

You may object at any time to customer segmentation and to the determination and display of personalised product recommendations via the personalisation settings in your customer account. Once you object, your order history will no longer be used for personalised product recommendations.

In connection with testimonials or questions & answers about products, we may be legally required by the EU regulations for digital services (Digital Services Act) to contact you due to a restriction on content provided by you (Art 6 para 1 lit c GDPR).

“Stay logged in” function

During the login process, we offer you the optional “Stay logged in” function. If you actively enable this option by clicking it, we will place a cookie on your device that remains valid for 60 days.

The processing and placement of this cookie are based solely on your freely given and explicit consent (Article 6(1)(a) GDPR).

You can use your customer account without restriction even if you do not enable this function, although you will need to sign in again each time you visit.

You may withdraw your consent at any time by logging out of your customer account or by deleting the cookie via your browser settings.

Login via login provider (Single Sign-On / OAuth)
You have the option to log in to your customer account using an existing account with a selected external login provider with whom you are already registered. If you choose this login method, the respective provider will make certain data available to us after you have given prior confirmation.

The following categories of data may be processed in this context:

- Basic data confirmed by the login provider (e.g., name, email address)
- A technical identifier assigned by the login provider (e.g., user ID)
- Information on whether your account with the login provider has been successfully verified.
- Any additional data you explicitly authorise the provider to share (e.g. profile picture)

Which specific data are transmitted depends on the provider and the settings in your account with them. Authentication takes place exclusively between you and the external login provider. We only receive the information required to set up or use your customer account with us.

We process this data for the following purposes:

- Creating and using your customer account with the chosen login provider
- Carrying out authentication for subsequent logins
- Avoiding the need for a separate registration and password with us
- Ensuring account security and preventing misuse

This data processing takes place in order to carry out pre-contractual measures and to fulfil our contract with you concerning the use of our webshop and customer account (Art. 6(1)(f) GDPR), as well as on the basis of our overriding legitimate interest in offering a secure and user-friendly login function (Art. 6(1)(f) GDPR).

The respective login provider is an independent controller as per Art. 4 Z 7 GDPR for any further processing of your data (e.g. within your account with that provider). The nature, scope and purposes of such processing are set out in the provider’s own privacy notices.

Sovendus Voucher Network

Subject to your prior voluntary consent (Article 6(1)(a) GDPR), given via our "Privacy settings" banner (see Section 1), to the use of the third-party service “Sovendus”, we may display offers from the Sovendus voucher network after you have completed an order. For this purpose, a pseudonymised and encrypted hash of your email address and your IP address are transmitted to Sovendus GmbH, Hermann-Veit-Str. 6, 76135 Karlsruhe, Germany. Sovendus processes this data on the basis of Article 6(1)(f) GDPR and acts as an independent controller within the meaning of Article 4(7) GDPR in respect of the data it processes. The pseudonymised hash of your email address is used to take account of any objection you may have made to receiving advertising from Sovendus (Article 21(3) and Article 6(1)(c) GDPR). Your IP address is used by Sovendus solely for data security purposes and is generally anonymised after seven days (Article 6(1)(f) GDPR). For billing purposes between Sovendus and us, your order number, order value and currency, session ID, coupon code and time stamp are also transmitted to Sovendus in pseudonymised form (Article 6(1)(f) GDPR). If you wish to take advantage of a voucher offer from Sovendus, have not objected to receiving advertising at your email address and click on the voucher banner displayed to you in these circumstances, we will also transmit your name, postcode, country and email address to Sovendus in encrypted form so that your voucher can be prepared (Article 6(1)(b) and (f) GDPR). For further information on how Sovendus processes your data, please refer to the Sovendus Online Privacy Notice.

5) What data do we process when you order our products via Amazon Marketplace?

We also offer some of our products via the Amazon Marketplace. When you order our products through Amazon Marketplace, we receive from Amazon, or the respective responsible Amazon entity, the data necessary for processing your order as well as for the fulfilment of related legal and contractual obligations.

In this context, in addition to the data processed by Amazon during your use of their services, we process the following categories of your data:

- Name
- Contact details
- Email address and/or communication data provided by Amazon
- Telephone number, insofar as required for delivery or establishing contact
- Billing and shipping address
- Order and delivery data
- Returns, refunds, and complaint data
- Payment and transaction data, insofar as these are made available to us by Amazon
- Correspondence data, including all data you provide to us in connection with your order via Amazon
- Any information required for tax or statutory purposes

We process this data for the following purposes:

- Processing your order via Amazon Marketplace
- Delivery of the goods ordered and engaging parcel delivery or freight forwarding services
- Communication with you regarding your Amazon order, particularly in the event of queries, delivery issues, returns, complaints, or warranty claims
- Invoicing and the fulfilment of tax and corporate law obligations
- Statutory record-keeping requirements in accordance with Section 132 of the Austrian Federal Fiscal Code (BAO)
- Handling of returns, refunds, customer enquiries, and other service-related matters
- Prevention and investigation of fraudulent activity or attempted fraud
- Establishing, exercising, or defending legal claims
- Fulfilment of our contractual obligations towards Amazon, insofar as this is necessary for sales via Amazon Marketplace

The processing of these data categories is restricted to the extent necessary for the performance of a contract (Art. 6(1)(b) GDPR) or for compliance with our legal obligations (Art. 6(1)(c) GDPR). Furthermore, processing is carried out where necessary for our overriding legitimate interests in ensuring seamless business operations, the secure handling of orders, and the establishment or defence of legal claims (Art. 6(1)(f) GDPR).

We do not use data received in connection with an order via Amazon Marketplace for our own newsletters, customer accounts, customer match services, personalised advertising, or other promotional purposes unrelated to the Amazon ordering process, unless a separate legal basis exists for such use.

In order to comply with Amazon’s data protection and data security requirements, we process data from Amazon orders only to the extent required in each case. Our internal systems and processes are designed to ensure that only such personal data as is actually required for the relevant purpose is used or disclosed. In particular, no unnecessary personal communication data is transmitted to shipping and logistics service providers.

For the processing of orders via Amazon Marketplace, it may be necessary for us to transmit your data, to the extent required, to the following categories of recipients:

| Service provider and the provider's privacy policy | Description | Place of Processing | Legal basis for data processing and transfer |
|---|---|---|---|
| Amazon or the responsible Amazon entity | Provision and processing of the Amazon Marketplace, order management, customer communication, returns and refunds processing | Generally, EU/EEA. In exceptional cases, also third countries | Independent controllership of the service provider pursuant to Art. 4(7) GDPR; performance of a contract (Art. 6(1)(b) GDPR), legal obligations (Art. 6(1)(c) GDPR), or overriding legitimate interests (Art. 6(1)(f) GDPR). For recipients in a third country in the absence of a valid adequacy decision - Art. 49(1)(b) and (e) GDPR |
| Logistics service providers | Transport and delivery of orders; personal communication data not required for delivery will not be transmitted | Generally, EU/EEA. In exceptional cases, also third countries | Performance of a contract (Art. 6(1)(b) GDPR). For recipients in a third country in the absence of a valid adequacy decision – Art. 49(1)(b) and (e) GDPR |
| Dropshipping or direct shipping service providers | Fulfillment of orders for products not in stock and handover to logistics service providers for transport | Generally, EU/EEA. In exceptional cases, also third countries | Performance of a contract (Art. 6(1)(b) GDPR). For recipients in a third country in the absence of a valid adequacy decision – Art. 49(1)(b) and (e) GDPR |

| | | | |
|---|---|---|---|
| IT, ERP, inventory management, accounting, and archiving service providers | Technical processing, storage, internal administration, invoicing, and archiving of orders | Generally, EU/EEA. In exceptional cases, also third countries | Data processing on behalf of a controller pursuant to Art. 28 GDPR; performance of a contract (Art. 6(1)(b) GDPR), legal obligations (Art. 6(1)(c) GDPR), or overriding legitimate interests (Art. 6(1)(f) GDPR) |
| Tax consultants, legal advisors, auditors, and public authorities | Fulfilment of legal obligations as well as the establishment and defence of legal claims | Generally, EU/EEA | Legal obligations (Art. 6(1)(c) GDPR) or overriding legitimate interests (Art. 6(1)(f) GDPR) |

We protect all data by means of appropriate technical and organisational measures, in particular through access restrictions, role-based permissions, logging, encryption during transmission, protection against unauthorised access, and regular reviews of the systems and service providers used.

We store data from Amazon orders only for as long as is necessary for the relevant purposes. Insofar as Amazon specifies shorter retention, deletion, or anonymisation periods for certain categories of data, we take these specifications into account through corresponding internal processes. Data required exclusively for the operational processing of an Amazon order will be deleted, anonymised, or reduced to the legally required minimum once the relevant purpose no longer applies.

Where statutory retention obligations apply, in particular, retention obligations under tax and corporate law, we store the necessary documents for the statutory period. Once the purposes have been fulfilled or the retention periods have expired, the data will be deleted, anonymised, or disposed of in compliance with data protection laws. Where applicable, this also includes deletion or anonymisation from production systems, time-delayed removal from backups as part of technical deletion cycles, and the secure disposal of any paper documents or data carriers.

Amazon also processes your data in connection with the use of Amazon Marketplace as an independent controller. Further information on the processing of your data by Amazon can be found in Amazon's Privacy Policy.

6) What categories of your data do we process when you rate your shopping experience in our website?
In case you rate your shopping experience on our website after your purchase, the following categories of your data may be processed in addition to the data processed during your visit to our website:

- Name
- Contact details
- E-mail address
- Order and delivery data
- Rating data
- Correspondence data, including all data that you provide to us in connection with your evaluation

We process this data for the following purposes

- For evaluation of your shopping experience
- To contact you to discuss your shopping experience (with your prior voluntary consent only)

This data is processed based on your voluntary consent (Article 6(1)(a) GDPR) or is justified by our legitimate interest in analysing and improving our processes (Article 6(1)(f) GDPR). You may withdraw your consent to be contacted at any time; however, any data processing carried out before the withdrawal remains lawful. You are under no obligation to provide this data.

It may be necessary for us to transfer your data to the following recipients:

| Service provider and data privacy notice of the provider | Description | Place of processing | Legal basis for data transfer |
|---|---|---|---|
| Freshworks Inc. | Customer enquiries and customer care services via email or chat | EU/EEA, occasionally USA, if you contact us via social media platforms | Order processing as per Art 28 GDPR with certification of the service provider as per the Data Privacy Framework (DPF) Programme |

7) Which data do we process if you have a business relationship with us?
If you have a business relationship with us as a partner or supplier, we may process the following categories of your data:

- Name
- Company data
- Contact details
- E-mail address
- Telephone number
- Business data, order, delivery and invoice data
- Correspondence data, including all data that you provide to us in connection with our business relationship.

We process this data for the following purposes:

- The initiation, maintenance and processing of our entire business relationship with you (e.g. pre-contractual obligations, invoicing of services, dispatch of documents, communication for processing the contract).
- Legally required storage as defined by the § 132 BAO (Federal Fiscal Code)
- Internal administration and management of our business relationship to the extent required (e.g.: Processing your business case, forwarding business cases to various departments, filing, archiving purposes, correspondence with you).
- Assertion and defence of legal claims

These categories of data are processed to the extent necessary in each case. If you do not provide us with this data, we will unfortunately not be able to process your business transaction.

Processing this data is necessary for the contractual fulfilment of our business relationship (Art 6 Para 1 lit b GDPR), necessary for the fulfilment of our legal obligations in connection with retention periods (Art 6 para 1 lit c GDPR) or justified by our overriding legitimate interest smoothly running our business (Art 6 Para 1 lit f GDPR).

8) How long will your data be stored?
We only store your data for as long as is necessary for the purposes for which we collected your data. In this context, statutory retention obligations must be taken into account (for example, for reasons of tax law, contracts, order data or other documents from a contractual relationship must generally be retained for a period of seven years (§ 132 BAO)). Your name, address, purchased goods and date of purchase are also stored until the product liability expires (after 10 years according to § 13 Product Liability Law). In justified individual cases, such as for the assertion and defence of legal claims, we may also store your data for up to 30 years after the termination of the business relationship.

We store the data that we process in the context of contacting you for up to three years from the time you last contacted us.

9) Collection of data from other sources (Art 14 GDPR)
Data is collected from other sources solely to the extent necessary for the purposes described. This applies, in particular, where you intend to enter into a business relationship with us as a partner or supplier, or when you order our products through an external marketplace, specifically Amazon Marketplace. In such instances, we receive the data necessary to initiate, perform, or manage the fulfillment of the business relationship or order.

| Source | Publicly accessible? | Data concerned | Purpose/Justification |
|---|---|---|---|
| Company website | Yes | Contact and organisational data | Establishing contact for business purposes |
| Contractual partner | No | Name, address, phone no. | Performance of a contract, delivery |
| Amazon or the responsible Amazon entity | No | Name, contact details, billing and shipping address, data for orders, deliveries, returns, refunds and correspondence, as well as other data required for order processing | Order processing via Amazon Marketplace, delivery, customer service, returns, complaints, invoicing, statutory record-keeping obligations, and the establishment and defence of legal claims |

10) Does automated decision-making or profiling take place (Art 13(2)(f) GDPR)?
We do not use solely automated decision-making on our website where this would produce legal effects concerning you or otherwise significantly affect you.

For registered customer accounts, we may infer likely product interests from the products and product categories you have purchased in our shop in order to display personalised product recommendations within our shop. You may object to this use at any time via your customer account.

For registered newsletter subscribers, we may assign you to a customer segment based on your previous orders in order to tailor newsletter content and sending frequency. You may object to this personalisation at any time.

None of these measures affects prices, the products available to you, your ability to enter into a contract, available payment methods or any other decisions with legal or similarly significant effects.

During the ordering process, the payment service provider you select may also use automated processes, including profiling, for fraud prevention or payment verification. Further information can be found in the privacy information provided by the relevant service provider.

11) What rights do you have in relation to the processing of your personal data?
We would like to inform you that, where the applicable legal requirements are met, you have the following rights:

- to request information about the personal data we process about you (see Article 15 GDPR for details)
- to request the rectification or completion of inaccurate or incomplete personal data concerning you (see Article 16 GDPR for details)
- to request the erasure of your personal data, provided there are no legitimate grounds for retaining it (see Article 17 GDPR for details)
- to request restriction of the processing of your personal data (see Article 18 GDPR for details)
- to data portability, meaning the right to receive the personal data you have provided to us in a structured, commonly used and machine-readable format (see Article 20 GDPR for details)
- to object to the processing of your personal data where the processing is based on Article 6(1)(e) or (f) GDPR (Article 21 GDPR). You may object at any time, without giving reasons, to the processing of your personal data for direct marketing purposes, including any related profiling. We will then no longer process your personal data for those marketing purposes.

Where we process your personal data on the basis of your consent, you have the right to withdraw that consent at any time. Withdrawing your consent does not affect the lawfulness of any processing carried out before the withdrawal (Article 7(3) GDPR).

If, contrary to expectations, you believe that your right to the lawful processing of your personal data has been infringed, please contact us. We will endeavour to address your request without undue delay and, in any event, within the statutory period of one month. You also have the right at any time to lodge a complaint with the data protection supervisory authority responsible for your jurisdiction.

12) Who is responsible for data protection and how can you contact us?
The person responsible for Data Processing as presented here (as stipulated in Art 4 Z 7 GDPR) is:

Cosmeterie GmbH
Josefstädter Str. 7/16
1080 Wien
Österreich
global@cosmeterie.com
CEO: Mag. Sophie C Ryba, Roland Fink, Mag. Christoph Schreiner

Joint responsibility within the niceshops Group, or via commissioned processing by the niceshops Group, and your rights:
This website is operated by the niceshops Group, an Austrian e-commerce company that specialises in the development of online shops in various product segments.
The data processing outlined in this privacy statement can be carried out:

- under joint responsibility within the niceshops Group as per Art 26 GDPR (if necessary, we'd be happy to provide you with the essential contents of the relevant agreement upon request)

or:

- in the form of commissioned order processing as per Art 28 GDPR, where the niceshops Group processes the orders.

In both cases, you are free to assert your rights with all parties.

Contact information of the Data Protection Officer at the niceshops Group:
Email: privacy@niceshops.com
Post: niceshops GmbH, c/o the Data Protection Officer, Annenstrasse 23, 8020 Graz, Austria.

For persons and authorities in the United Kingdom, a representative has been appointed for data protection matters of the niceshops Group as stipulated in Art 27 United Kingdom General Data Protection Regulation (UK GDPR). The contact details of our representative are:
Email: info@rgdp.co.uk
Post: RGDP LLP, Level 2, One Edinburgh Quay, 133 Fountainbridge, Edinburgh, EH3 9QG, Scotland.
When contacting our representative, please state "niceshops / www.cosmeterie.com" in the subject line so your request can be promptly assigned.

Any use of this privacy policy, or parts of it, without the consent of the author constitutes a violation of copyright.