DATA POLICY EU

Data Protection Statement

As of: 11/10/2024

Best Secret GmbH takes the protection of your personal data very seriously and collects and uses your personal data only in the scope of the applicable statutory provisions.

In order to let you feel safe when visiting our website, we provide you with an overview of how Best Secret GmbH together with its affiliated companies pursuant to Sections §§15 et seqq. German Stock Corporation Act (together the "BESTSECRET Group") ensures this protection and what kind of data we collect for what purpose below. The data protection statement is available on our website at any time.

1. Information about data processing within the BESTSECRET Group

1.1 General information

As part of our business activities, it is therefore essential for data to be exchanged between branch locations and divisions on a regular basis in order to promote and facilitate cooperation within the Group. For this reason, central processes are not limited to a single Group company, but also include its affiliated companies pursuant to Sections §§15 et seqq. German Stock Corporation Act. Companies within the BESTSECRET Group therefore work together in many areas and act as so-called joint controllers within the meaning of data protection law.

1.2 Information about the primary contents of the contract in the case of joint controller authority within the BESTSECRET Group

In light of their joint role, the member companies of the BESTSECRET Group have concluded a contract as joint controllers within the meaning of sect. 26 in conjunction with sect. 4 7 GDPR to guarantee the security of processing and the effective exercise of your rights.

Without limitation, this contract addresses the following points:

- Subject, purpose, means and scope as well as competences and responsibilities with regard to data processing
- Providing information to data subjects
- Fulfilment of other rights of data subjects
- Security of processing
- Involvement of contract data processors
- Procedure in the event of personal data breaches

- Cooperation with supervisory authorities
- Liability

2. Controller and Data Privacy Officer

The controller responsible for processing your personal data are all companies of the BESTSECRET Group as joint controllers. In particular, you may contact Best Secret GmbH, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany (hereinafter referred to as BESTSECRET) in order to assert your rights. Member companies belonging to the BESTSECRET Group have each appointed a data protection officer. You may contact the controllers and the data protection officer at:

Data processing controller	**Data protection officer of the controller**
Best Secret GmbH represented by Dr. Moritz Hahn, Axel Salzmann, Dr. Andreas Reichhart and Dominik Rief Margaretha-Ley-Ring 27, 85609 Aschheim, Germany Phone: +49 (0) 89 / 24600 000 Email: dataprotection@bestsecret.com	Best Secret GmbH Data protection officer Margaretha-Ley-Ring 27, 85609 Aschheim, Germany Email: data-protection@bestsecret.com

3. Appropriate safeguards for processing personal data in third countries.

If we use service providers outside the EU or the European Economic Area (EEA), we take appropriate and suitable measures to ensure a sufficient level of data protection when transmitting personal data in accordance with sect. 44 et seq. GDPR, e.g. conclusion of EU standard contracts, additional technical and organisational measures such as encryption or anonymisation. Please note that despite the careful selection and obligation of a service provider, the latter may process data outside the EU/EEA or be subject to another jurisdiction owing to the location of its registered office and may not provide an adequate level within the meaning of the GDPR of data protection. Please note that if your data is transferred to the USA, there is a risk that your data may be processed by US authorities for control and monitoring purposes; in such cases, it may be possible that you are not entitled to any legal remedies.

4. General data collection when visiting our website

If you use our website for information only, i.e. if you do not register or otherwise submit any information to us, we will only collect the personal data your browser submits to our server.

These data are technically required for us in order to show our website to you and to ensure stability and safety (the legal basis for this is our legitimate interest pursuant to sect. 6 para. 1 s. 1 lit. f GDPR).

For technical reasons, these are saved by default as logfiles (protocol files).

Data	Purpose of processing	Legal basis for processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call	Optimised website representation Ensuring proper website operation	Sect. 6 para. 1 s. 1 lit. f GDPR	Deletion after 60 days at most
IP address	Ensuring proper website operation	Sect. 6 para. 1 s. 1 lit. f GDPR	Deletion after 60 days at most

Error analysis by Rollbar

We use the Rollbar error analysis system provided by Rollbar Inc. (Rollbar, 51 Federal Street, San Francisco, CA 94107, USA) in order to ensure system stability for our website. With the help of Rollbar, we are able to detect technical errors that occur on our website, and then immediately rectify any such errors. The purpose of the related data processing is to technically monitor our website and to document error messages in order to protect and optimize the stability of our website.

In the event of application errors, the following data is transmitted to Rollbar for such purposes:

- IP address of the inquiring computer
- User Agent
- Operating system, language and version of the inquiring device
- Browser version of the inquiring computer
- Language of the browser
- Document Object Model (DOM) event (e.g., “clicked button xy”)
- Time zone difference to Greenwich Mean Time (GMT)
- Name of the file requested
- Date and time of access;
- Information about the relevant error (e.g. JavaScript error, network error)

The legal basis for this data processing is sect. 6 para. 1 lit. f GDPR. Our legitimate interest consists in offering a technically stable website and enabling us to offer you the error-free use of our website to the greatest extent possible.

Data is deleted 90 days after collection.

To enable data processing, data is transferred to Rollbar in the United States where the error analysis system is operated at Google data centres (Google Data Center, Council Bluffs, Iowa 51501/USA) (Google Cloud). We have concluded a contract processing agreement with Rollbar in accordance with sect. 28 GDPR according to which Rollbar undertakes to ensure the necessary protection of your data and to process it exclusively on our behalf and in accordance with our instructions in accordance with applicable data protection regulations. The use of the so-called EU standard contractual clauses pursuant to sect. 46 of the GDPR ensures an appropriate level of protection within the meaning of sect. 44 et seq. of the GDPR within the scope of contract data processing.

Additional information concerning data protection at Rollbar may be found at https://docs.rollbar.com/docs/privacy-policy and https://docs.rollbar.com/docs/security.

Monitoring and analysis by Datadog

We use the Datadog monitoring, and analysis platform provided by Datadog, Inc. (Datadog, 620 8th Ave, 45th Floor, New York, NY 10018) to effectively troubleshoot and perform security analysis. With the aid of Datadog, we are able detect technical errors that occur on our website using log files so that we can then trouble-shoot and correct these errors immediately. The purpose of the associated data processing is to ensure a technically stable and secure website as well as the continuous optimisation of our services.

The following data is processed during platform operation and on an ad hoc basis in the event of application errors:

- customerPK (Primary Key is the technical key assigned by BESTSECRET)
- customerId (customer number)
- customerUid (email)
- clientIp (IP address)
- SchuboCustomerNumber (customer number of the customer card holder; collected upon the occurrence of error messages)
- SchuboCardNumber (customer card number; collected upon the occurrence of error messages)
- Customer contact details (collected upon the occurrence of error messages) - the following components can be collected in this context: Mr/Ms, customer first name, last name
- Customer email address (collected upon the occurrence of error messages)
- Information about the respective error
- Operating system, language and version of the accessing browser or device
- Time zone difference to Greenwich Mean Time (GMT)
- Name of the accessed file
- Date and time of access

The legal basis for the processing is sect. 6 para. 1 lit. f GDPR, i.e. our legitimate interest in providing a technically stable and secure website and enabling you to use our website with as few errors as possible.

As a rule data collected in this context is deleted after 30 days, however no later than 60 days after collection.

We have chosen the EU Service Option offered by Datadog, i.e. data is stored and secured exclusively at data centres within the EU. The Google Cloud Platform in Germany is used for this purpose. However, within the context of the data processing referred to above, it cannot be ruled out that data may also be transmitted to the USA or that it may be possible to access such data from a third country for support purposes. We have concluded a commissioned processing agreement with Datadog in accordance with sect. 28 GDPR, under which Datadog undertakes to ensure the necessary protection of your data and to process it exclusively on our behalf and in accordance with our instructions in accordance with applicable data protection regulations. An adequate level of protection within the meaning of sect. 44 et seq. GDPR is guaranteed by the use of the so-called EU standard contractual clauses pursuant to sect. 46 GDPR within the scope of such commissioned data processing. For additional information, please see https://www.datadoghq.com/legal/eea-data-transfers/ and the Datadog privacy notices.

5. Data collection on login/registration on our website

If you log in or register at www.BESTSECRET.com, personal, behaviour-related and technical data will be saved.

Technical data will be saved anonymised and evaluated. Anonymised means that we cannot assign the data to a determined or determinable natural person, or that we would do so only with disproportional effort of time, costs and labour. We will evaluate these anonymised data in order to further improve the function of the shop and to make it more user-friendly.

In the scope of reconciliation of interests according to sect. 6 para. 1 lit. b GDPR, we have observed and considered our interest in provision of the data and your interest in data-protection-compatible processing of your personal data.

The following data are required for provision of our service in order to offer you our website and to ensure stability and safety, in particular to protect against abuse. Accordingly, we can - while ensuring data protection aligned with the state of the art – process these data, while appropriately considering your interest in processing them in a manner compatible with data protection.

Data	Purpose of processing	Legal basis of processing	Duration of storage
Personal information such as: Name, email address, ...	Registration purposes Customer communication	Sect. 6 para. 1 s. 1 lit. f GDPR	Deletion after expiration of purpose or until expiration of the obligation to preserve business records relating to commercial and tax law.

Behaviour-related data such as: Last login, registration date, visited product pages, ...	Customer communication Measure of success Determination of target group for advertising purposes	Sect. 6 para. 1 s. 1 lit. f GDPR	Deletion after expiration of purpose, no later than 90 days after membership ends

Collection of the data described above for provision of the website and recording of the data described above in logfiles is mandatory for operation of the website. Accordingly, the user cannot object to this.

We use Auth0 (Auth0 Inc., 10900 NE 8th Street, Suite 700, Bellevue, WA 98004), a service provider specializing in secure authentication, as the authentication platform for your registration and login to our member area website. The purpose of using Auth0 is to provide secure authentication for our members as part of the login process for services requiring registration.

When you first register via the login form on our website, we collect your email address to verify your membership with us and then transmit the login data (email address and encrypted password) to Auth0. Auth0 stores this login data on our behalf for later comparison during login processes. The data is used exclusively for your authentication. When you log in to our website during the login process, the data you entered for the login, email address and encrypted password, is transferred to Auth0 for matching for the purpose of authentication. As part of this authentication process, we then receive the result of the verification back from Auth0. In the course of the verification process, Auth0 collects the following personal data: email address, login date, date of last login, IP of last login, browser used during login and operating system.

Your data will be used to set up, provide and personalize your member profile as part of the provision of a contractual service. The legal basis for the data processing is the fulfillment of the contract (sect. 6 para. 1 s. 1 lit. b GDPR) and our legitimate interest (sect. 6 para. 1 s. 1 lit. f GDPR) to maintain an effective and secure login system in the course of operating our services requiring registration.

Auth0 processes your data in data centers of Amazon Web Services (in short: AWS) in Frankfurt am Main/Germany and Dublin/Ireland, an offer of Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxembourg. We have concluded a contract with Auth0 for commissioned processing pursuant to sect. 28 GDPR, in which Auth0 undertakes to process the data only in accordance with our instructions and to comply with the EU data protection level. To ensure an adequate level of data protection, we have also concluded EU standard contractual clauses as appropriate safeguards under sect. 46 GDPR with Auth0.

Your data will be stored within the scope of legal obligations and subsequently deleted. In principle, personal data will only be stored for as long as is necessary for the aforementioned purposes and legal obligations to provide proof and to retain data do not oblige the company to store it for longer. In the aforementioned sense, your data as a member registered with us will be

deleted by us when your membership ends. Simultaneously with the deletion of your user accounts, the data stored by Auth0 will also be deleted. You can find more information about Auth0's data protection at https://auth0.com/privacy/.

6. Data collection and use in the scope of provision

6.1 General information

The information that we receive from you helps us process your orders as smoothly as possible, to eliminate sources of error, to improve our service to you and to prevent abuse and fraud. Further information on data protection can be found in our data protection information for customers, which we have made available to you here: Link to information obligations

6.2. Orders after deletion requests

Should we receive a deletion request from you, we will do everything necessary to delete your BESTSECRET account in accordance with Art. 17 of the General Data Protection Regulation (GDPR). If you place an order with us before we are able to delete your data, we will understand the order as a request to revive your membership with us. We hereby accept any such request and will therefore not delete your BESTSECRET account or your data. The legal basis for this data storage is then our legitimate interest (Art. 6 para. 1 lit. b GDPR).

6.3 Processing of orders and payments

We use your data for the processing of orders and payments, delivery of the goods and rendering of services. The service providers we use for processing orders (such as carriers, logistics specialists, banks or our marketplace partners) receive the data necessary for handling and processing orders. The same shall apply to processing returns. If you order a product on our marketplace, the data necessary for handling and processing orders will also be passed on to the respective marketplace partner so that they can carry out the delivery of the order.

In some countries, it may be necessary to pass on the telephone number and e-mail address you have provided to the delivery company so that the goods you have ordered can be delivered. In these cases, we will pass on the data you have provided to the relevant delivery company without requiring your separate consent.

Whether additional data, such as the email address, should be passed on to report the specific delivery date or not can be indicated and changed in the ordering process or at any time in your personal settings. If you choose Pick Up Point as the delivery method, we must disclose your email to the relevant delivery service for handling and processing your order. If not, the delivery service will be unable to inform you that the parcel has arrived at the respective Pick Up Point. In such cases, you do not have the option to prevent such information being disclosed by adjusting your settings.

When processing payments, we will disclose your payment data to the payment service providers we have commissioned. When you make a purchase from us, your data (e.g. name, payment amount, account details, credit card number) is processed by the payment service provider for the purpose of processing the payment in question. The relevant provider's ap-plicable contractual and data protection provisions apply to these transactions. Payment ser-vice providers are used on the basis of Article 6(1)(b) GDPR (contract processing) and in the interests of the smoothest, easiest and most secure payment process possible (Article 6(1)(f) GDPR). When your consent is requested for certain actions, Article 6(1)(a) GDPR is the legal basis of the data processing. The following section contains more detailed information about our individual payment processors.

6.4 Information about individual payment processors

6.4.1 Adyen

With BESTSECRET, you can make use of the following payment options via the payment ser-vice provider Adyen N.V, Rokin 49, 1012 KK, Amsterdam, Netherlands): payment by credit card (Mastercard, VISA, American Express, Diners, Discover, Maestro, Carte Bancaire), Blik (Poland), iDeal (Netherlands), Bancontact (Belgium).

When you use the various payment options, this will involve transferring certain personal data to Adyen. Your data will be disclosed to Adyen and the respective payment processors solely for the purpose of processing the payment in question, and only to the extent necessary. Adyen is responsible for recording and storing the data, including for the purpose of conducting identity and credit checks, before disclosing it to the respective payment processor. However, we do not store your payment data here. Further information on data protection can be found in Adyen's Privacy Policy at https://www.adyen.com/policies-and-disclaimer/privacy-policy.

The following section contains more detailed information about the individual payment options.

Payment by credit card

When making a payment by credit card (Mastercard, VISA, American Express), Adyen will typically receive your name, address, bank account details, card information (i.e. card number, expiry date, system/issuer) and information about your transaction (i.e. transaction number, currency, issuer country, date of transaction and transaction amount), along with technical information, such as your browser info, risk data and shopperID.

More information about data protection measures implemented by credit card companies can be found here:

- Mastercard https://www.mastercard.com/global/en/vision/corp-responsibility/commitment-to-privacy/privacy.html
- Visa https://www.visaeurope.lu/en_LU/legal/global-privacy-notice.html
- American Express https://www.americanexpress.com/content/dam/amex/de/customer-service/PDFs/Datenschutzerklaerung_f%C3%BCr_Karteninhaber.pdf

- Diners https://www.dinersclub.com/content/dam/discover/en_us/diners-club/docs/DGN%20Global%20Privacy%20Statement_Fully%20Approved_Final.pdf
- Discover https://www.intercard.de/de/karteninhaber/datenschutzinformationen
- Maestro
- Carte Bancaire https://www.cartes-bancaires.com/protegezvosdonnees/porteurs/

Blik

Blik is an online payment system operated by Polski Standard Płatności sp. z o.o. Czerniakowska 87A St. 00-718 Warsaw, Poland. If you select Blik as the payment method, you will need to have an account with and access to the online banking system of a participating Polish bank. Information on data protection at Blik can be found at https://blik.com/media/PRIVACY-POLICY-AND-COOKIE-POLICY.pdf.

iDEAL

iDEAL is an online payment system operated by the service provider Currence iDEAL B.V., Gustav Mahlerplein 33-35, 1080 AB MS Amsterdam, Netherlands. Customers who hold Dutch bank accounts can pay using iDEAL. If you select iDEAL as the payment method, you will need to have an account with and access to the online banking system of a participating Dutch bank. Further information on data protection at iDEAL can be found at https://www.ideal.nl/en/privacy-cookie-statement/

Bancontact

If you select one of the payment services offered by Bancontact, we will disclose your payment data to Bancontact Payconiq Company, Rue d'Arlon 82, 1040 Brussels, Belgium (hereinafter referred to as "Bancontact") in order to process the payment in question. Customers who have a Bancontact card issued by a participating Belgian bank can pay using Bancontact. You can find Bancontact's terms of use here: https://www.bancontact.com/en Further information on data protection at Bancontact can be found at https://www.bancontact.com/files/privacy.pdf

6.4.2 Bambora

With BESTSECRET, you can make use of the following payment options via the payment service provider Bambora AB, Vasagatan 16, 111 20 Stockholm, Sweden: payment by credit card (Mastercard, VISA, American Express) and payment by Klarna Sofort.

Your personal data will be transferred to Bambora during the payment process. Your data will be disclosed to Bambora solely for the purpose of processing the payment in question, and only to the extent necessary. Bambora is responsible for recording and storing the data, including for the purpose of conducting identity and credit checks, before disclosing it to the respective payment processor. However, we do not store your payment data here. Further information on data processing and data protection at Bambora can be found at https://www.bambora.com/privacy-policy/

Payment by credit card

When making a payment by credit card (Mastercard, VISA, American Express, Diners), Bambora will typically receive your name, address, bank account details, card information (i.e. card number, expiry date, system/issuer) and information about your transaction (i.e. transaction number, currency, issuer country, date of transaction and transaction amount), along with technical information, such as your session ID, user ID and authentication infor-mation. More information about data protection measures implemented by credit card com-panies can be found here:

- Mastercard https://www.mastercard.com/global/en/vision/corp-responsibility/commitment-to-privacy/privacy.html
- Visa https://www.visaeurope.lu/en_LU/legal/global-privacy-notice.html
- American Express https://www.americanexpress.com/content/dam/amex/de/customer-service/PDFs/Datenschutzerklaerung_f%C3%BCr_Karteninhaber.pdf
- Diners https://www.dinersclub.com/content/dam/discover/en_us/diners-club/docs/DGN%20Global%20Privacy%20Statement_Fully%20Approved_Final.pdf

Klarna Sofort

Klarna is a payment service provider operated by Klarna Bank AB Sveavägen 46, 111 34 Stockholm, Sweden (hereinafter referred to as "Klarna"), who we use to offer the "Sofort" payment method. Data is processed exclusively for the purpose of processing the selected payment method via the service provider, Klarna. We use your online banking details (PIN/TAN) to make a Sofort payment. The payment is transferred directly from your account via your bank. Further information on Klarna's data protection provisions can be found at https://cdn.klarna.com/1.0/shared/content/legal/terms/0/en/privacy#7 and https://www.sofort.com/1.0/shared/content/legal/terms/de-DE/SOFORT/

6.4.3 Braintree

With BESTSECRET, you can make use of the PayPal payment option via the payment service provider, Braintree. Braintree is a service operated by PayPal (Europe) S.à r.l. et Cie, S.C.A. (22-24 Boulevard Royal, L-2449 Luxembourg). Further information on data processing and data protection at Braintree can be found at https://www.braintreepayments.com/de/legal/braintree-privacy-policy

PayPal

PayPal is an online payment service provider that processes payments via PayPal accounts, which are virtual private or business accounts. PayPal's European operating company is PayPal (Europe) S.à.r.l. & Cie. S.C.A., 22-24 Boulevard Royal, 2449 Luxembourg, Luxem-bourg.

Your personal data will be transferred to PayPal and Braintree during the payment process. When making a payment via PayPal, Braintree and PayPal will typically receive your first name, surname, address, email address, IP address, telephone number, mobile phone number or other

data required to process the payment in question. Such personal data related to the respective order is also required to process the purchase agreement.

The personal data transferred to PayPal will, under certain circumstances, be transferred to credit referencing agencies by PayPal. The purpose of any such transfer is to conduct identity and credit checks. Where necessary, PayPal will also disclose such personal data to its affiliated companies and service providers or subcontractors, provided such action is necessary to fulfil contractual obligations or the data is to be processed by a commissioned data processor. The various data protection provisions applicable at PayPal can be accessed at https://www.paypal.com/de/webapps/mpp/ua/privacy-full.

Direct debit

When you choose SEPA direct debit as your payment method, your money is debited direct-ly from your bank account by our payment service provider, Telecash. The full Terms and Conditions of Business for payment by direct debit can be found at https://www.telecash.de/content/dam/telecash_de/de/de/pdf/agb/TeleCash_AGB.pdf .

6.4.4 Riverty

With BESTSECRET, you can make use of the following payment options via the payment ser-vice provider Riverty GmbH, Gütersloher Str. 123, 33415 Verl, Germany (formerly Arvato Payment Solutions GmbH) (hereinafter referred to as “Riverty”): purchase on account and SEPA direct debit.

Your personal data will then be transferred to Riverty during the payment process. Your data will be disclosed to Riverty and the respective payment processors solely for the purpose of processing the payment in question, and only to the extent necessary. Riverty also stores the data for the purpose of conducting identity and credit checks, enabling the active manage-ment of payment methods in order to be able to accurately assess your ability to pay when offering payment methods involving credit risk.

When making a payment via Riverty, Riverty will typically receive your contact details (name, address, date of birth where applicable, email address where applicable) as well as details of the items you have ordered (e.g. order value, product group, value of goods, route via which the enquiry was received where applicable and delivery method), which are re-quired to process the payment in question via Riverty.

Purchases on account

Further information on payment processing for purchases on account can be found here: https://documents.riverty.com/terms_conditions/payment_methods/overview/de_en.

SEPA direct debit

When you choose SEPA direct debit as your payment method, your money is debited directly from your bank account by our payment service provider, Riverty. The full Terms and Conditions of Business for payment by direct debit can be found at https://documents.riverty.com/terms_conditions/payment_methods/direct_debit/de_en/default.

All data is processed in accordance with the applicable data protection provisions in force, as well as in line with Riverty's privacy statements: https://documents.riverty.com/privacy_statement/checkout/de_en/default.

7. Tracking Technologies

7.1 General information

We use tracking technologies such as cookies in order to improve our website and to make it as user-friendly as possible. Cookies are small text files that are stored on your computer's operating system when you access our website. Amongst other things, cookies contain a distinctive character string that enables unique identification of your browser when you return to our website. Cookies store additional information, such as your language setting, the length of your visit to our website or certain entries you may have made whilst there. This avoids having to re-enter all required data each time you use our website. Cookies also enable us to recognise your preferences and to tailor our website to match your areas of interest.

Cookies store additional information, such as your language setting, the length of your visit to our website or certain entries you may have made whilst there. This avoids having to re-enter all required data each time you use our website. Cookies also enable us to recognise your preferences and to tailor our website to match your areas of interest.

7.2 Type of tracking technologies in use

We differentiate between tracking technologies that are technically necessary for the website, tracking to optimise our website/app and tracking related to personalised advertising.

7.2.1 Technically necessary tracking technologies

We use cookies within the scope of the technically necessary tracking technologies. These cookies are necessary for the operation of a website/app and its functions. These include session cookies and cookies that store certain user preferences (e.g. shopping cart, language preferences, gender preferences, or login information), opt-out cookies, cookies from payment service providers that are stored to complete the payment process, cookies from shipping service providers that are used to track shipments, or the Google Tag Manager to manage your tracking preferences. The legal basis for the use of technically necessary tracking technologies is our legitimate interest pursuant to sect. 6 para. 1 s. 1 lit f GDPR.

However, it is possible to disable these cookies by changing the settings in your browser. However, (error-free) use of the website can then no longer be guaranteed.

7.2.2 Tracking for purposes of website/app optimisation (optimisation & performance)

Tracking for optimisation and performance purposes aids in analysing user behaviour on the BESTSECRET website and app as part of a performance analysis or for statistical purposes. BESTSECRET can optimise the user-friendliness of the shop and correct possible errors on the basis of these evaluations.

Tracking technologies for purposes of optimisation and performance include:

- Google Optimize
- Google Firebase
- Hotjar

The exact mode of operation, and the relevant data categories, for each individual tracking technology will be described in more detail below, starting at no. 8 et seqq.

Tracking for purposes of optimisation and performance is only used if you have given us your consent in accordance with sect. 6 para. 1 s. 1 lit. a GDPR. Your consent also refers to sect. 25 (1) German Telecommunications-Telemedia Data Protection Act. The consent given on the website also applies to the mobile applications. Consent settings applied in the mobile application cover both the website and its mobile applications. You can revoke your consent at any time by deselecting the tracking setting 'Optimisation & performance' in the cookie settings of the footer. For technical reasons, this opt-out usually only becomes effective after 48–72 hours. When applying consent changes for the app, you can speed this up by restarting the app.

We use the consent management tool ‘Usercentrics Consent Management Platform’ provided by Usercentrics GmbH, Sendlinger Strasse 7, 80331 Munich, Germany, to manage your tracking settings. The following data is stored as part of this process:

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Tracking setting (including consent or rejection, time)	Verification purposes	Sect. 6 para. 1 s. 1 lit. f GDPR	Three years after withdrawal of consent or deletion of the account
Device data or data from any devices in use (including shortened IP address and time)	Verification purposes	Sect. 6 para. 1 s. 1 lit. f GDPR	Three years after withdrawal of consent or deletion of the account
User Identifier	Verification purposes	Sect. 6 para 1 s. 1 lit. f GDPR	Three years after withdrawal of consent or deletion of the account

7.2.3 Tracking for purposes of personalisation

Tracking for purposes of personalised advertising is used to create personalised advertising tailored to your interests on our websites/app or on websites operated by our advertising partners as well as for other marketing purposes.

Tracking technologies for purposes of personalisation include:

- Google Ads, Audiences et Conversion Tracking
- Google Analytics
- Google Marketing Platform
- Criteo
- Salesforce
- Meta Custom Audiences & Smartly
- Snapchat
- TikTok
- RTB House
- Pinterest
- Adjust
- Socialbakers

The exact mode of operation for each individual tracking technology will be described in more detail below, starting at no. 8 et seqq.

Tracking for purposes of personalisation is only used if you have given us your consent in accordance with sect. 6 para. 1 s. 1 lit. a GDPR. Consent must be given both on the website and its mobile applications. Consent settings applied in the mobile application cover both the website and its mobile applications. You can revoke your consent at any time by deselecting the tracking setting 'Personalisation' in the cookie settings of the footer. For technical reasons, this opt-out usually only becomes effective after 48–72 hours. When applying consent changes for the app, you can speed this up by restarting the app.

We use the consent management tool ‘Usercentrics Consent Management Platform’ provided by Usercentrics GmbH, Sendlinger Strasse 7, 80331 Munich, Germany, to manage your tracking settings. The following data is stored as part of this process:

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Tracking setting (including consent or rejection, time)	Verification purposes	Sect. 6 para. 1 s.1 lit. f GDPR	Three years after withdrawal of consent or deletion of the account
Device data or data from any devices in use (including shortened IP address and time)	Verification purposes	Sect. 6 para. 1 s.1 lit. f GDPR	Three years after withdrawal of consent or deletion of the account

User Identifier	Verification purposes	Sect. 6 para. 1 s.1 lit. f GDPR	Three years after withdrawal of consent or deletion of the account

8. Google Tag Manager

For reasons of transparency, please note that we use Google Tag Manager. Google Tag Manager itself does not record any personal data. Tag Manager makes it easier for us to integrate and manage our tags. Tags are small code elements that serve, among others, to measure traffic and visitor behaviour, to record the effects of online advertisements and social channels, remarketing or retargeting and setting up alignment with target and testing and optimising websites. For further information on the Google Tag Manager, see https://www.google.com/analytics/tag-manager/use-policy/.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Contract processor	YES	USA

9. Google Analytics & Google Optimize

BESTSECRET uses Google Analytics, a web analytics service provided by Google, Inc. We also use Google Optimize too. Google Optimize analyses the use of different versions of our website and helps us to improve user-friendliness based on the behaviour of the users on our website. Google Optimize is a tool associated with Google Analytics. In that capacity, all of the statements below regarding Google Analytics apply in the same way to Google Optimize.

Google Analytics, a web analytics service provided by Google LLC, is used on this website, provided you have given your consent. The data controller for users in the EU/EEA and Switzerland is Google Ireland Limited, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland (“Google”).

Google Analytics uses cookies that enable an analysis of your use of our website. The information collected by the cookies regarding your use of this website is usually transferred to a Google server in the USA where it is stored.

We use the User ID function. We can use this User ID to assign a unique, permanent ID to one or more sessions (and any activities during these sessions) and analyse user behaviour across multiple devices.

We use Google Signals. This enables Google Analytics to capture additional information about users who have activated personalised ads (interests and demographic data). The ads are then displayed to these users in remarketing campaigns across multiple devices.

With Google Analytics 4, anonymised IP addresses are enabled by default. As a result of this IP anonymisation, your IP address will be shortened beforehand by Google within Member States of the European Union or in other States party to the Agreement on the European Economic Area. Only in exceptional cases will the complete IP address be transferred to a Google server in the United States and shortened there. The IP address sent by your browser within the scope of Google Analytics will not be linked to any other data held by Google.

When you visit our website, your user behaviour will be captured in the form of "events". Events may include the following:

- page views;
- first time you visit a website;
- start of session;
- your "click path" and interaction with the website;
- scrolls;
- clicks on external links:
- internal search queries;
- interaction with videos;
- ads viewed / clicked.

The following information is also captured:

- your approximate location (region);
- your IP address (shortened);
- technical information regarding your browser and the devices you are using (e.g. language settings or screen resolution);
- your Internet service provider;
- the referrer URL (the website/advertising medium via which you came to this website).

Google will use this information on behalf of BESTSECRET for the purpose of evaluating your use of the website and compiling reports on website activity. The reports generated by Google Analytics are used to analyse the performance of our website, our app, and the success and management of our marketing campaigns, social media channels, online magazines and newsletters.

The recipients of this data may include the following:
Google Ireland Limited, Gordon House, Barrow Street 4, Dublin, Ireland (data processor pursuant to Article 28 GDPR)
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, a subsidiary of Meta Platforms, Inc., 1601 S California Ave, Palo Alto, California 94304, USA
It cannot be ruled out that US authorities will access the data stored by Google.

Where data is processed outside the EU/EEA in a location where there is no level of data protection equivalent to European standards, we have agreed EU standard contractual clauses with the service provider in question in order to establish an adequate level of data protection.

The parent company of Google Ireland, Google LLC, is headquartered in California, USA. It cannot be ruled out that data will be transferred to the USA and the data stored by Google will be accessed by US authorities. The USA is currently regarded as a third country from a data protection perspective. The country does not offer the same rights as those in place within the EU/EEA. You may not be entitled to any remedies against the authorities accessing your data.

The data sent by us and linked with cookies is automatically erased after 50 months. Data for which the retention period has expired is automatically deleted once a month.

The legal basis for this processing is your consent in accordance with Article 6(1)(1)(a) GDPR. Once given, you can revoke your consent at any time with future effect by adjusting your preferences in our tracking settings (see section above under “Tracking technologies”).

Alternatively you can delete your cookies (all of them or only those relating to this website). The selection banner will then be displayed again.

Alternatively, you can prevent the installation of cookies in advance by adjusting the corresponding settings in your browser software. However, if you configure your browser to reject all cookies, this may restrict the functionality of this website and other websites. You can also prevent the data generated by the cookies and related to your use of the website (including your IP address) being recorded by Google and the processing of this data by Google by

- not giving your consent to the cookie in question being installed; or
- downloading from HERE and installing the browser add-on used to disable Google Analytics.

For more information on the terms of use for Google Analytics or on data protection at Google, please visit https://marketingplatform.google.com/about/analytics/terms/de/ or https://policies.google.com/?hl=en.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Contract processor	YES	USA

Affected data category	Purpose of processing	Legal basis of processing	Retention Period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Evaluation of customer behaviour	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most

Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Evaluation of customer behaviour	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most
User ID, device ID	Evaluation of user behaviour on different devices/browsers	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most
Personal data such as email address, Google Click ID, Google Client ID, IP address, mobile advertising ID, order ID, user ID, voucher code	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after no more than 26 months

10. Google Ads, Audiences, and Conversion Tracking

In order to draw attention to our services, we place Google Ads advertisements and use Google Conversion-Tracking in the scope of this for the purpose of personalised interest- and site-based online advertisements.

The advertisements are displayed on Google's own websites, services, and apps. Advertisements are also displayed on websites of Google's advertising network. Detailed information on the Google advertising network can be found at https://support.google.com/google-ads/answer/1752334?hl=en. We are able to combine our ads with certain search terms. We can use cookies to place ads on our website based on the previous visits of a user.

When clicking an ad, Google sets a cookie on the user's Browser. Further information on the cookie technology used can also be found among the notes of Google on the website statistics under https://services.google.com/sitestats/en.html and in the data protection provisions under https://policies.google.com/privacy?hl=en.

With the help of this technology, Google and we as the customer receive information that a user clicked an ad and has been forwarded to our websites. The information acquired here is used only for a statistical evaluation for ad optimisation. We will not receive any information with which the visitors can be identified in person. The statistics provided to us by Google contain the overall number of users who clicked one of our ads and, if applicable, whether they were forwarded to a page of our website with a conversion tag. We can use these statistics to determine for which search terms our ad was clicked particularly often and which ads lead to contact by the user via the contact form.

We also use the custom match function in Google Ads. Using this function we can establish target groups to present specific advertising content to only a selection of users. To achieve this, we can provide Google with a customer list which contains the email address stored in their customer account.

Further information and the cancellation option can be found at: https://support.google.com/google-ads/answer/6379332 or https://adssettings.google.com/.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Contract processor	YES	USA

Affected data category	Purpose of processing	Legal basis of processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most
Behaviour-related data such as: registration date, visited product pages, ordered products, name of called website, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most
Personal data such as email address, Google Click ID, Google Client ID, IP address, mobile advertising ID, order ID, user ID	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most

11. Google Marketing Platform

Furthermore, we use Google Marketing Platform, a service of Google Inc. Google Marketing Platform uses cookies to place user-based ads. The cookies recognise which ad has already been shown in your browser and whether you called a website using a displayed ad. The cookies do not record any personal information and also cannot be connected to these.

For more information on how Google uses cookies, see the data protection statement of Google.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Contract processor	YES	USA

Affected data category	Purpose of processing	Legal basis of processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most
Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most
Personal data such as email address, Google Click ID, Google Marketing Platform Click ID, Google Marketing Platform Client ID, IP address, mobile advertising ID, order ID	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 26 months at most

12. Google Web Fonts (offline version)

This website uses web fonts provided by Google for the uniform display of fonts. When you open a page, your browser loads the required web fonts into your browser cache in order to display texts and fonts correctly. We have opted for the offline version, whereby the Google Fonts are stored locally on our web server. The management of the fonts is then possible – using CSS – as with any other font family. Neither IP addresses nor any other data is transmitted to Google.

The use of Google Web fonts is done in the interest of a uniform and appealing presentation of our website based on efficiency and cost-effectiveness considerations. This represents a legitimate interest within the meaning of sect. 6 para.1 s. 1 lit. fGDPR. A default font is used by your computer if your browser does not support web fonts. Further information about Google Web Fonts can be found at https://developers.google.com/fonts/faq and in Google's Privacy Policy.

13. Hotjar

Our website has Hotjar integrated (https://www.hotjar.com). Hotjar enables us to record and evaluate user behaviour (e.g. mouse movements, clicks, scrolling height) on our websites. For this purpose, Hotjar uses cookies on end units of the users and is able to save the data of users anonymised, e.g. concerning browser information, operating system, time spent on the page. Learn more about Hotjar under the following link: https://www.hotjar.com/privacy.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Hotjar, 3 Lyons Range, 20 Bisazza Street, Sliema SLM 1640, Malta	Contract processor	NO	/

Affected data category	Purpose of processing	Legal basis of processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Analysis of customer behaviour towards website optimisation	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 12 months at most
Behaviour-related data such as: Visited product pages, browsing behaviour on website, visited pages ...	Analysis of customer behaviour towards website optimisation	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 12 months at most

14. Criteo

On our pages, we collect information on the surfing behaviour of the website visitors for marketing purposes in a pseudonymised form using the technology of Criteo; cookies and web pixels are placed for this. This way, Criteo can analyse surfing behaviour and then display targeted product recommendations as matching advertising banners when other websites are visited. For this purpose, cookies from our partner websites are also placed via pixels. Under no circumstances can the pseudonymised data be used to personally identify website visitors. The data collected by Criteo are only used to improve the advertising offer.

You can generally learn more about the data protection statement and data protection directives at Criteo at https://www.criteo.com/privacy/.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Criteo GmbH, Lehel Carré, Gewuerzmuehlstrasse 11, 80538 Munich, Germany	Controller	NO	/

Affected data category	Purpose of processing	Legal basis of processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 13 months at most

Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 13 months at most
Personal data such as email address, Criteo ID, IP address, mobile advertising ID, order ID	Evaluation of user behaviour on different devices/browsers to deliver ads on different end devices	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 13 months at most

15. Salesforce

For customer support, we use the Customer Relationship Management module “Salesforce Marketing Cloud” and “Salesforce Service Cloud” by Salesforce.com Inc. The data are processed in the USA. Further information on the Salesforce Marketing Cloud and Salesforce Service Cloud and the processed data is available at https://www.salesforce.com/company/privacy/.

If you give your express consent, these technologies will also evaluate information about user behaviour on websites, mobile apps, emails, push messages, in-app messages and other communications for marketing purposes. This is done using cookies and web pixels, as well as the iGoDigital tracking service, which is part of Salesforce. The information collected in this manner will be associated with your email address and is linked to a unique ID in order to clearly associate clicks in communications with you. The purpose of the user profile is to tailor our offerings and our services to your interests and to improve or marketing offerings and communications for you.

Designation of the provider	**Service provider type**	**Data transfer to a third country**	**Third country**
Salesforce.com Inc., The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA	Contract processor	YES	USA

Affected data category	**Purpose of processing**	**Legal basis of processing**	**Retention period**

Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Creation of profiles as part of the Salesforce CRM systems	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after expiration of purpose, no later than 90 days after membership ends
Behaviour-related data such as: Registration date, visited product pages, ordered products, use the FAQ/Help, name of called website, Products on the wish list	• Finding suitable product recommendations or other communication content for newsletters and special mailings and other messages such as push notifications or in-app messages • Improving the website and other communications	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after expiration of purpose, no later than 90 days after membership ends
User ID, device ID	• Finding suitable product recommendations or other communication content for newsletters and special mailings and other messages such as push notifications or in-app messages • Improving the website and other communications	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after expiration of purpose, no later than 90 days after membership ends

16. Meta Ads and Custom Audiences & Smartly

As part of our usage-based online advertising we use the Custom Audiences services of Meta Platforms Inc. (1601 S. California Avenue, Palo Alto, CA 94304, USA). As an EU company, our appointed processor is Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

By adopting usage-based online advertising via Custom Audiences, we can define the user target groups that see ads within the Meta network by choosing certain characteristics in Meta Ads Manager. Meta selects users by means of the profile information they have specified as well as other data supplied when using Meta. When a user clicks on an ad and is subsequently directed to our website, Meta is notified that the user clicked on the advertising banner by means of the integrated Meta Pixel on our website as well as the Meta Conversion API. Basically, this generates a non-reversible and non-personal hash total from your user data which is passed on to Meta for analysis and marketing purposes. A Meta cookie is set for this purpose. This collects

information on your actions on our website (e.g. surfing habits, sub-pages visited, etc.). In addition, your IP address is saved and used in order to drive advertising geographically.

Alternatively we can provide Meta with a customer list which contains the email address and your advertising ID you specified during registration.

The legal basis for our data processing is sect. 6 para. 1 s. 1 lit. a GDPR.

You can revoke your consent at any time with future effect by adjusting your preferences in our cookie settings. Alternatively you can delete your cookies (all of them or only those relating to this website). The selection banner will then be displayed again.

Insofar as you consent to the data processing described, Meta also has access to your data. In particular it is possible that Meta Platforms Inc., 1601 Willow Road, Menlo Park, California 94025, USA, in addition to Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland has access to your data. Meta Platforms Inc. is located in a third country.

Since 27/09/2021 Meta has provided a "Facebook EU Data Transfer Addendum" online, which is designed to include the standard contractual clauses in those cases in which Meta Platforms Ireland Limited processes data from the EU/EEA as processor and sends it to Meta Platforms Inc. as sub-processor.

You can find further information on Meta's Custom Audiences service at: https://en-gb.facebook.com/business/help/744354708981227?id=2469097953376494.

As a logged in user you can disable the "Meta Custom Audiences" function at https://www.facebook.com/settings/?tab=ads#_.

Please note that Meta is permitted to use the data we supply on your user behaviour as well as your email address for its own purposes. You can revoke your consent to targeting on Facebook on this website.

You can find further information on the purpose and scope of data collection and further processing and use of data by Meta as well as your privacy protection settings options in Facebook's Data Policy.

In addition we use the tool Smartly.io. The tool is a service of Solutions Inc., Elielinaukio 2 G, 00100 Helsinki, Finland. The platform provides a web-based desktop for creating and managing Facebook, Messenger, Instagram and WhatsApp campaigns. We use Smartly to create and run BESTSECRET advertising campaigns on Meta. The campaigns are created in Smartly and used via the interface with Meta. The statistics which Meta compiles to analyse advertising campaigns in this context are also displayed in Smartly. In order to use the tool we have concluded a processing contract with Smartly, in accordance with Section 28 GDPR, and in this way ensure adherence to the regulations of the Data Protection Act.

You can find further information on data protection when using Smartly.io at: https://cdn2.hubspot.net/hubfs/1570479/Privacy%20Policy/Smartly.io%20Privacy%20Policy.pdf?t=1541578381755.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Meta Platforms Inc. 1601 WILLOW ROAD MENLO PARK, CA 94025, USA	Contract processor	YES	USA

Affected data category	Purpose of processing	Legal basis of processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	12 months at most, currently 6 months
Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	12 months at most, currently 6 months
Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	12 months at most, currently 6 months

17. Snapchat

We use online services provided by Snapchat Inc. (Market Street, Venice Ca 90291 USA) for purposes of analyzing and optimizing our website and services.

Use of the Snap pixel makes it possible to specificy visitors to our website in the form of target groups and to place advertising in the form of Snapchat ads based on these groups. As part of this process we use Snapchat pixels to target specific audiences interested in the respective advertising or have certain interests in topics or products. In addition, it is possible for us to track the effectiveness of Snapchat ads using statistics.

Snapchat uses EU standard contractual clauses (sect. 46 para 2 and 3 GDPR) as the basis of data processing for recipients located in third countries (outside the EU) the transfer of data to such countries.

For more information about how Snapchat processes your personal data, please click on the following link https://snap.com/en-GB/privacy/privacy-policy .

The legal basis for this data processing is your consent in accordance with sect. 6 para. 1 s. 1 lit. a GDPR.

18. TikTok

We use TikTok Pixel on our website. This is a conversion tracking tool provided by TikTok, based in London, United Kingdom (6th Floor, One London Wall, London, EC2Y 5EB). This is a subsidiary of the TikTok parent company headquartered in China.

We would like to expressly state that TikTok stores data (e.g. IP address, preferences and personal interests or behavior) from users and uses such for commercial purposes. We have no influence on the processing and further use of this data, as TikTok alone determines how your personal data is processed. We are currently unaware of the extent to which, where and for how long the data is stored, to what extent the data is associated with other data and evaluated, and with whom the data shared.

TikTok processes data within Europe, China, Singapur, Malaysia and the USA. Please note that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for data transfers in some countries outside the European Union including the USA and China. We have concluded so-called EU standard contractual clauses with TikTok (sect. 46 para 2 and 3 GDPR) as the basis for data transfers to recipients located in third countries (outside the EU). In such agreements, TikTok undertakes to maintain and comply with the European level of data protection when processing your personal data, even if your personal data is processed in a third country.

For more information about how TikTok processes your personal data, please click on the following link: https://www.tiktok.com/legal/privacy-policy-eea?lang=en.

The legal basis for this data processing is your consent in accordance with sect. 6 para. 1 s. 1 lit. a GDPR.

19. RTB House

We use the technology of RTB House SA on our pages to collect information on the surfing behaviour of the website visitors for marketing purposes in a pseudonymised form by setting cookies and web pixels. This way, RTB House can analyse surfing behaviour and then display targeted product recommendations as matching advertising banners when other websites are visited. In no case must the anonymised data be used to personally identify the visitor of the website. The data collected by RTB House are only used to improve the advertising offer.

You can generally learn about the data protection statement and data protection directive at RTB House at https://www.rtbhouse.com/privacy/.

Designation of the provider	Service provider type	Data transfer to a third country	Third country

RTB House SA, Zlota 61/101, 00-819, Warsaw, Poland	Contract processor	NO	/

Affected data category	Purpose of processing	Legal basis of processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 13 months at most
Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 13 months at most
User ID, device ID such as Customer ID, Advertising ID and Client ID	Evaluation of user behaviour on different devices/browsers to deliver ads on different end devices	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after 13 months at most

20. Firebase

We use technology from Google Firebase (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, “Google”) with various functionalities in our apps. Firebase uses so-called “Instance IDs” to memorise individual settings within the mobile app. Because each Instance ID is unique to a mobile app and the mobile device you are using, Firebase is able to evaluate and respond to specific events within the mobile app. Information generated by the Instance ID about your use of this mobile app on your mobile device is generally sent to a Google server in the United States and stored there. Google ensures that the IP address is anonymised immediately if the IP address is also sent.

For more information, see Firebase’s Terms of Use and Privacy Notice.

Provider name	Service provider type	Data transfers to third countries	Third country
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	Processor	YES	USA

The following functionalities are used specifically:

20.1 Firebase Remote Config

Firebase Remote Config enables the configuration of app settings. We can change the behaviour and appearance of your app on the user device without having to completely reinstall it from the app store. Find out all you need to know about how Remote Config works here.

Data category concerned	Purpose of Processing	Legal basis for processing	Retention period
Technical data such as: operating system in use, browser type and version, device (smartphones, tablets or other device), date and time of access, etc.	App optimisation	Sect. 6 para. 1 s. 1 lit. a GDPR	Erasure after achievement of purpose; no later than 180 days after request
Instance ID	App optimisation	Sect. 6 para. 1 s. 1 lit. a GDPR	Erasure after achievement of purpose; no later than 180 days after request

20.2 Firebase Performance Monitoring

Firebase Performance Monitoring allows us to track the performance of the app and respond to specific incidents within the app. Find out more information here.

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Technical data such as: operating system in use, browser type and version, device (smartphones, tablets or other device), date and time of access, etc.	App optimisation	Sect. 6 para. 1 s. 1 lit. a GDPR	Erasure after achievement of purpose; no later than 180 days after request
Instance ID	App optimisation	Sect. 6 para. 1 s. 1 lit. a GDPR	Erasure after achievement of purpose; no later than 180 days after request

20.3 Firebase Dynamic Links

We use the Firebase service Dynamic Links if you are using a mobile device with iOS or Android operating system. Firebase Dynamic Links are links that work on multiple platforms, regardless of whether you have already installed our app or not. When you open a dynamic link on iOS or Android, you are taken directly to the linked content in your app. If you have not yet installed our app, you will be directed to the App Store or Play Store via the link to install the

app. Your app then starts and can access the link. On the other hand, if you open the same dynamic link in a desktop browser, you will be redirected to the corresponding content on the website. In this way, we are always able to forward you directly to the right address. For functionality reasons, personal data such as the IP address and device specifications are used and temporarily stored in order to provide the services. Further information on Firebase Dynamic Links can be found here (https://firebase.google.com/docs/dynamic-links), on data protection and IT security at: https://firebase.google.com/support/privacy

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
IP address and device specifications (language and version of the browser software, operating system used and its interface, referrer URL, date and time of the server request, time zone difference to Greenwich Mean Time (GMT), content of the request (specific page), amount of data transferred, access status/HTTP status code.	Optimising the user experience when using links	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure once purpose no longer applies, at the latest 180 days after request

20.4 Firebase Crashlytics

In our mobile applications on Android and iOS we have integrated Firebase Crashlytics (https://firebase.google.com/products/crashlytics) for the purposes of detecting and reporting crashes and non-fatal crashes in the app. This information is used to improve the application performance and stability. For these purposes technical data such as the mobile device id, device type, model, operating system and approximate location of the mobile device is transmitted to provide more reliable analysis, for example to determine whether the issue is specific to one device type or to multiple devices.

For more information, see Firebase's Terms of Use and Privacy Notice.

Affected data category	Purpose of processing	Legal basis for processing	Retention period
Technical data such as: Operating system used, browser type and version, device (e.g. phone, tablet, ...), date and time of website call, ...	Evaluation of customer behaviour	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion no later than 180 days
Behaviour-related data such as: Registration date, visited product pages, ordered products, name of called website, ...	Evaluation of customer behaviour	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion no later than 180 days

User ID, device ID	Evaluation of customer behaviour	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion no later than 180 days

21.Business intelligence applications / Internal tools

We use various business intelligence technologies within our organisation to continuously improve our online shop and related services and to provide you with a successful shopping experience.

This is internal business analytics aimed at optimising our service in the long term, for example in the form of new applications (tools/apps). We process a small amount of already existing/collected personal data such as the user ID or order information in pseudonymised form and link them where appropriate. If it is technically possible to anonymise your personal data, we will anonymise it in order to prevent any identification of you as a person. The applied tools communicate based on existing interfaces in order to maintain the purpose of long-term optimisation.

You can make use of the “Best sellers for you” category to enjoy the most personalised shopping experience possible. The way products are displayed in this category is generally based on the choice of favourite brands you have entered manually. If you have not saved any favourite brands, we will use a “backup” list made up of 10 designers that sell well in our online shop. We do not use an algorithm here.

The data collection and storage are carried out for the performance of an already existing contract according to Sect. 6 para. 1 s. 1 lit. b GDPR in conjunction with our legitimate interest according to Sect. 6 para. 1 s. 1 lit. b GDPR. Our legitimate interest is to continuously improve our online shop and the associated shopping experience.

Your personal data will be deleted immediately after the purpose has been fulfilled.

22. Pinterest Ads

In addition, we use the Pinterest plugin provided by Pinterest Europe Limited, Palmerston House, 2nd Floor, Fenian Street, Dublin 2, Ireland. This allows us to track the behaviour of users after they have viewed a Pinterest advertisement. We can also use the Pinterest tag to measure the conversion rate of a campaign. This means that the Pinterest tag allows us to evaluate the effectiveness of a Pinterest ad, optimise future advertising campaigns and to make them more user-friendly. We are not able to identify users from the data collected. However, this data is also stored by Pinterest and can be associated with a user profile and used for marketing purposes. You can find more information about data protection at https://policy.pinterest.com/en/privacy-policy.

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Technical data such as: Device information, operating system in sue, device ID, date and time of access	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Up to 12 months
Behavioural data such as: Registration date, products visited, products ordered, name of pages accessed	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Up to 12 months
Personal data such as email address, IP address, Pinterest Client ID, mobile advertising ID, order ID	Ad delivery for customer segments	Sect. 6 para. 1 s. 1 lit. a GDPR	Up to 12 months

23. Adjust

We use the Adjust service provided Adjust GmbH, Saarbrücker Str. 37A, 10405 Berlin/Germany for our BESTSECRET Apps in order to analyse App use and to improve our mobile advertising campaigns. Adjust allows us to track App installations along with how the Apps are used and to evaluate and optimize the performance of mobile advertising campaigns across different marketing channels.

As part of this process, Adjust uses in particular the data listed in the table below. Data collected via Adjust may provide information concerning the installation and initial access to the App on a mobile device as well as concerning interactions within an App (e.g. in-App purchases, login). In addition, this data provides information about which advertisements have been seen or clicked on.

The legal basis is your consent pursuant to sect. 6 para. 1 s. 1 lit. a GDPR. You may withdraw your consent at any time with effect for the future.

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Technical data such as: Operating system and version used, browser type and version, device type (smartphones, tablets), HTTP header, user agent, app version, SDK version, app token, event token, date, and time of activity	Evaluation of user behaviour to optimize app-applications and analysis of mobile advertising campaigns on different marketing channels	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after purpose no longer applicable (e.g. revocation of consent), or until expiry of retention obligations under commercial and tax laws

Behavioural data such as Registration date; Installation and initial app access on the mobile device, interactions within an app (e.g. products viewed, products purchased, product searches) or information about which ads were seen or clicked on	Evaluation of user behaviour to optimize app-applications and analysis of mobile advertising campaigns on different marketing channels	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after purpose no longer applicable (e.g. revocation of consent), or until expiry of retention obligations under commercial and tax laws
Adjust Device ID (MAC address hashed), Google Click ID, Google Marketing Platform Click ID, Meta Click ID, IP Address, Mobile Ad ID, Vendor ID (IDFV, for iOS only), Order ID, User ID	Evaluation of user behaviour to optimize app-applications and analysis of mobile advertising campaigns on different marketing channels	Sect. 6 para. 1 s. 1 lit. a GDPR	Deletion after purpose no longer applicable (e.g. revocation of consent), or until expiry of retention obligations under commercial and tax laws

We have concluded a commissioned processing agreement with Adjust in accordance with sect. 28 GDPR, under which Adjust undertakes to ensure the necessary protection of your data and to process it exclusively on our behalf and in accordance with our instructions in accordance with applicable data protection regulations.

Adjust uses data centres provided by Leaseweb Netherlands B.V., Hessenbergweg 95, 1101 CX Amsterdam, within in the EU (Frankfurt am Main, Amsterdam) and the USA to operate its application.

In cases in which personal data is processed on servers outside the EU/EEA, e.g. in the USA, the contract for commissioned processing provides that Adjust must ensure an adequate level of protection with regard to data processing in the third country within the meaning of sect. 44 et seq. GDPR. This is done via so-called EU standard contractual clauses pursuant to sect. 46 GDPR along with additional measures.

For more information on data protection, please see: https://www.adjust.com/terms/privacy-policy/ or https://www.adjust.com/terms/gdpr/.

24. Socialbakers

In addition, we use Socialbakers, a service of Emplifi Czech Republic a.s., Pod Všemi svatými 17, Pilsen, Czech Republic. Socialbakers is a social media management and marketing system (social suite platform) which we use for market observation, advertising and marketing purposes.

In doing so, Socialbakers enables us to observe, analyse and evaluate the activities on our social media channels and to carry out target group specific marketing measures on this basis. In addition, we use Socialbakers for customer support purposes in order to respond to existing customer enquiries via the respective social media communication channel. For this, we link Socialbakers with our social media platforms or websites that use Google Analytics. Within the scope of this process Socialbakers only collects and processes personal data which we obtain from you when visiting our social media channels and websites in accordance with data protection regulations. More information on this can be found in the privacy policies / consent management tools of our services.

The processing of personal data is based on sect. 6 para. 1 s. 1 lit. b and Sect. 6 para. 1 s. 1 lit. f GDPR. The processing of personal data is required for the fulfilment or initiation of a contract. In cases where no purchase initiation process takes place or has taken place in the past, our legitimate interest lies in optimising customer support.

Within the scope of the use of the tool, we have entered into a data processing contract with Socialbakers in accordance with sect. 28 GDPR. For more information on data protection when using Socialbakers visit: https://www.socialbakers.com/privacy-policy.

25. Newsletter

Our newsletter is a key element of our membership and the services we provide to our mem-bers, allowing them to make use of our exclusive membership benefits. Receiving the newsletter is therefore an essential part of registering your membership. You can of course unsub-scribe from the newsletter at any time via the settings in your customer account or clicking the "Unsubscribe" link in each newsletter.

By agreeing to receive the newsletter, you agree to regularly receive information about sales promotions, product recommendations, vouchers and VIP status at BESTSECRET.

For dispatch of the newsletter, BESTSECRET also uses the service Salesforce Marketing Cloud, which is operated by the company Salesforce.com Inc., The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA.

In order to make our newsletter even more interesting for you in future, common technologies such as cookies or counting pixels are used in our newsletter. We evaluate your clicks within the newsletter using so-called tracking pixels, i.e. invisible image files, as well as personalised links and embedded links (link wrapping). They are assigned to your email address and are linked to a dedicated ID in order to clearly link any clicks in the newsletter to your own ID. The user profile serves to coordinate the offer and our services with your interests. The legal basis for this is the legitimate interest purs. to sect. 6 para. 1 s. 1 lit. a, b) GDPR. We do so based on your cookie settings.

We also use certain information (e.g. gender, postcode, VIP status) to appropriately segment and personalise our newsletter. The legal basis for this is our legitimate interest according to sect. 6 para 1 s. 1 lit. f GDPR.

You may change the frequency or the content of the newsletter at any time or unsubscribe from the newsletter entirely.

The consent to the newsletter is voluntary and can be revoked at any time. The revocation can take place in the settings in your customer account and, of course, via the logout link in every newsletter.

The following data are processed for sending the newsletter:

Designation of the newsletter provider	Service provider type	Data transfer to a third country	Third country
Best Secret GmbH, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany	Controller	NO	/
Salesforce.com Inc., The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA	Contract Processor	YES	USA

Data	Purpose of processing	Legal basis of processing	Retention period
Personal data such as: Email address, form of address, first name, last name, gender	Newsletter delivery	Sect. 6 para. 1 s. 1 lit. a, b GDPR	Three years after withdrawal of consent or deletion of the account
Confirmation of newsletter delivery, time of confirmation, newsletter preferences	Newsletter delivery	Sect. 6 para. 1 s. 1 lit. a, b GDPR	Three years after withdrawal of consent or deletion of the account
Revocation of confirmation	Proof of revocation	Sect. 6 para. 1 s. 1 lit. a, b GDPR	Three years after withdrawal of consent or deletion of the account
Behavioural data such as: opening and click rate	Analysis of user behaviour and/or creation of personalised advertising	Sect. 6 para. 1 s. 1 li, b GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership
Personal data such as: gender, postcode or purchases	Segmentation or personalisation	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership

26. Direct mail without prior notification

If we have received your e-mail address or postal address in connection with the sale of goods or services, we reserve the right to send you regular offers for products from our assortment by e-mail or post. For purposes of postal advertising using the Salesforce Marketing Cloud, we use the Salesforce service provider Optilyz, Neue Schoenhauser Str. 19, 10178 Berlin, Germany. Direct mail can be segmented based on demographic data, such as postcode or VIP status. You can object to the use of your e-mail address for the purpose of direct marketing via a link provided for this purpose in the advertising e-mail, or to the use of your postal address by sending an e-mail to service@bestsecret.com.

Designation of the provider	Service provider type	Data transfer to a third country	Third country
Salesforce.com Inc., The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA	Contract Processor	YES	USA
Optilyz GmbH, Neue Schoenhauser Str. 19, 10178 Berlin, Germany	Contract Processor	NO	/

Data	Purpose of processing	Legal basis of processing	Retention period
Personal data such as: Email address, form of address, first name, last name, gender	Marketing	Sect. 6 para. 1 s. 1 lit. f GDPR	Until objection
Demographic data such as: postcode, most recent purchase or VIP status	Sending a marketing campaign/personalisation	sect. 6 para.1 s. 1 lit. f GDPR	Until objection
Objection	Proof of objection	Sect. 6 para. 1 s. 1 lit. f GDPR	Deletion after expiry of purpose, at the latest 90 days after termination of membership

27. Push notifications, in-app messages and inbox messages in the app

27.1 Push notifications

In our app, you have the option to provide your consent to receive push notifications. Push notifications are regular on-screen messages about your membership, sales promotions and the latest trends. You can switch these notifications on and off at any time using the app settings on your mobile device, thus giving or withdrawing your consent as applicable. If you subscribe to push notifications, the device ID of your mobile device will be sent to the service that provides the push function for your operating system (for Android: Google Cloud Messaging; for iOS: Apple Push Notification Service). A so-called identifier ('Push Notification Identifier') is created as part of this process, which is then used for further communication with the BESTSECRET PushServer. The Identifier does not permit identification of the user. BESTSECRET uses the Salesforce Marketing Cloud service to send these messages. This service is operated by Salesforce.com Inc, The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA.

We also use certain information (e.g. gender, postcode, purchases) to appropriately segment and personalise our push messages and in-app messages. The legal basis for this is our legitimate interest according to sect. 6 para. 1 s. 1 lit. f GDPR.

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Push Notifications Identifier	Sending the push notification	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership
Personal data such as: first name, last name or gender, VIP status or vouchers	Creating the push notification	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership

27.2 In-app and inbox messages

We also use in-app and inbox messages in our app. These messages show you information about sales promotions, vouchers or your VIP status within the app. BESTSECRET uses the Salesforce Marketing Cloud service to send these message. This service is operated by Salesforce.com Inc, The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA.

We also use certain information (e.g. gender, postcode, purchases) in in-app and inbox messages to appropriately segment and personalise our push messages and in-app messages. The legal basis for this is our legitimate interest according to sect. 6 para. 1 s. 1 lit. f GDPR.

Data category concerned	Purpose of processing	Legal basis for processing	Retention period

Device ID and app ID	Creating the in-app message	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership
Personal data such as: first name, last name or gender, VIP status or vouchers	Creating the in-app message	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership

27.3 Tracking in-push notifications, in-app messages and inbox messages

In order to make our push notifications, in-app messages and inbox messages even more interesting for you in future, we evaluate what you open and click, as well as dwell time, among other things, with the aid of personalised links and embedded links (link wrapping). All data collected in this manner is linked to your subscriber ID. The purpose of the user profile is to tailor our offerings and our services to your interests. This is only done if you have given us your consent as part of the cookie opt-in in accordance with sect. 6 para. 1 s. 1 lit. f GDPR.

Data category concerned	Purpose of processing	Legal basis for processing	Retention period
Behavioural data such as: open and click rate, dwell time	Analysis of user behaviour	Sect. 6 para. 1 s. 1 lit. a GDPR	Erasure after the purpose no longer applies; no later than 90 days after termination of membership

28. Data usage for customer feedback

We use services administered by Zenloop (Zenloop GmbH, Brunnenstr. 196, 10119 Berlin, Germany) and Qualtrics (Qualtrics LLC, 333 River Park Drive, Provo, Utah 84604, USA) to conduct customer satisfaction surveys. The legal basis for this is Section 6 para. 1s. 1 lit. GDPR. The content of the survey can be both product-specific and -non-specific. We use these services to process survey data and contact details. Any data collected is processed without attributing it to your name or email address. We use your customer number to pseudonymise our data processing. Once data analysis has been completed, your customer number is erased from the dataset, leaving us with purely anonymised data. We use Qualtrics to process data previously received from Salesforce, provided you have consented to data processing by Salesforce. Within the Qualtrics and Zenloop environment, data is processed in Europe. For more information on data processing by Zenloop and Qualtrics, please see the Zenloop privacy policy (https://www.zenloop.com/en/legal/privacy) and the Qualtrics privacy statement (https://www.qualtrics.com/privacy-statement). If you previously opted in to participating in customer feedback activities and no longer wish to do so, you have the right to object to the continued processing of your data by contacting us or using the link provided in the email.

Categories of data subjects	Purpose of processing	Legal basis for processing	Retention period
Request for the technical provision of the survey	Upstream request whether a survey may be presented	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure once purpose no longer applies
Survey data, contact details	Conducting and analysing customer satisfaction surveys	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure once purpose no longer applies
Technical data, such as: device information, operating system used, device code, browser type and version, date and time of access	Conducting and analysing customer satisfaction surveys	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure once purpose no longer applies
Demographic data such as: postcode, gender, language	Conducting and analysing customer satisfaction surveys	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure once purpose no longer applies
Order and turnover history or VIP status	Conducting and analysing customer satisfaction surveys	Sect. 6 para. 1 s. 1 lit. f GDPR	Erasure once purpose no longer applies

29. Delivery status notification

As part of your order, you have the option to consent to have your e-mail address and telephone number sent to the respective shipping provider in order to enable the shipping partner to send you shipment status notifications.

Your consent is voluntary and can be withdrawn at any time. To do so, all you need to do is open the My BESTSECRET menu under Password and Contact Details/Personal Settings and deselect the option “Delivery tracking”.

Please note that if you choose Pick Up Point as the delivery method, we must disclose your email to the relevant delivery service for handling and processing your order. If not, the de-livery service will be unable to inform you that the parcel has arrived at the respective Pick Up Point. Your email address will be processed in such cases when choosing Pick Up Point as the delivery method on the basis of Article 6(1)(b) GDPR.

Relevant data category	Processing purpose	Legal basis for processing	Retention period
Personal data such as: e-mail address, telephone number	Disclosure to shipping partner for purposes of delivery tracking	Sect. 6 para. 1 s. 1 lit. f GDPR	Until withdrawn

Time at which consent is provided	Delivery tracking	Sect. 6 para. 1 s. 1 lit. f GDPR	Three years after withdrawal
Time at which consent is withdrawn	Verification of withdrawal	Sect. 6 para. 1 s. 1 lit. f GDPR	Three years after withdrawal

30. Inviting friends

We offer you the opportunity to recommend our website to other prospective customers. To do this, navigate to “Invite Friends” in the menu. By clicking on the button “Invite Friends”, you will receive an exclusive invitation link that you can send via social media or by e-mail.

In addition, we store personal data of the person who recommended you. As a closed shopping community, we only accept members who have been recommended by existing members. This data is used for verification and traceability and is necessary for the implementation of the membership contract.

Data	Purpose of processing	Legal basis for processing	Duration of storage
Personal data of invitee such as: Email address, invitation message, time of invitation	Implementation of the Membership Agreement	Sect. 6 para. 1 s. 1 lit. b GDPR	Deletion after expiration of purpose, no later than 90 days after membership ends
Personal data of the inviter: first name, surname, e-mail	Implementation of the Membership Agreement	Sect. 6 para. 1 s. 1 lit. b GDPR/p>	Deletion after expiry of purpose, at the latest 90 days after termination of membership

31. Waiting list

Since we are a closed shopping community and unfortunately can only accept a limited number of members, we offer people who are interested in joining the opportunity to be placed on a waiting list. This option is available when a member sends someone an invitation despite having run out of invitation permissions.

We store the following data in connection with the waiting list:

Data	Purpose of processing	Legal basis for processing	Retention period

Personal data of the invitee such as: First name, surname, email address, registration date and confirmation date	(pre-contractual) measures related to membership	Sect. 6 para. 1 s. 1 lit. b GDPR	Deletion once intended purpose no longer applies, no later than 30 days after rejection or unconfirmed invitation by BESTSECRET.

32. Competitions

For competitions (prize draws or prize competition), we use your data to inform you if you are a winner and for advertising our offers. For detailed information, see the participation conditions for the respective competitions.

Data	Purpose of processing	Legal basis for processing	Retention period
Personal data of winner such as: First name, last name, email address, address, and social media contact information	Lottery execution, winning notification, delivery of prices in case of win	Sect. 6 para. 1 s. 1 lit. f GDPR	Deletion after expiration of purpose

33. Compliance with customs provisions

Based on various EU regulations (2580/2001/EC, 881/2002/EC and 753/2011/EC) and other statutory specifications, we as a company are required to reconcile our customers' data with publicly available foreign trade and embargo lists before concluding a purchasing contract. We perform this reconciliation because we have an overruling legitimate interest in compliance with legal provisions and must protect ourselves from sanctions and fines (sect. 6 para. 1 s. 1 lit. c GDPR). We only perform the reconciliation if you order goods from our website and incur a payment obligation. Only the following present data are compared: first name, name and address. The data will be deleted at once after review.

34. Data processing on our careers site

Our careers site provides information about job openings at the BESTSECRET Group. You can find more information about data processing on the careers site here.

35. Passing on of data

35.1 Sharing data within the BESTSECRET group

As part of our business activities, it is essential for data to be exchanged between branch locations and individual companies of the BESTSECRET Group on a regular basis. Exchanging data in this context is essential for BESTSECRET membership and contract fulfilment. Data is

thus exchanged for contract performance in accordance with sect. 6 para. 1 s. 1 lit. b GDPR. The individual companies of the BESTSECRET Group are jointly responsible for data processing. The following BESTSECRET Group companies may have access to your data within the scope of Group-wide cooperation:

Controller	Purpose of processing	Legal basis for processing
Best Secret GmbH, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany	Membership management as well as the operation and provision of the BESTSECRET Online Shop. Establishment and defence of legal claims, security department, payment processing, linking the member card to BESTSECRET, participation in the commission system.	Sect. 6 para. 1 s. 1 lit. b GDPR
Best Secret Group SE, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany	Provision of the BESTSECRET stores and online store as well as the associated services, assertion of and defense against legal claims, security department, payment processing, order processing.	Sect. 6 para. 1 s. 1 lit. b GDPR
Best Secret Logistik GmbH, Parsdorfer Strasse 13, 85586 Poing, Germany	Package dispatch and returns handling and processing	Sect. 6 para. 1 s. 1 lit. b GDPR
Best Secret Poland sp. z o.o., Ul. Stefana Banacha 2 Krężoły, 66-100 Suléchow, Polen	Dispatch of parcels and processing of returns	Sect. 6 para. 1 s. 1 lit. b GDPR
Best Secret Retail Wien GmbH, Berggasse 16, 1090 Vienna, Austria	Member card linkage, participation in the commission system	Sect. 6 para. 1 s. 1 lit. b GDPR

35.2 Transfers to processors

We use other service providers as data processors in addition to the service providers expressly referred to above. They process personal data to the extent required. We carefully select, monitor and regularly review these service providers, in particular we have implemented technical and organisational measures to ensure that your data is protected. They process the data exclusively on our instructions. They include service providers such as IT service providers, marketing service providers and service providers for customer support.

35.3 Sharing data with third parties

Your personal data will only be passed on to third parties if this is required for contract processing or settlement or if you have consented to it in advance. Our business does not include selling such customer information. Data are only passed on in the scope of the presented purposes.

Your personal data will not be transferred to any third parties for any other than the purposes listed.

We shall only pass on your personal data to third parties if:

1. you have expressly consented to this,
2. forwarding is required for assertion, exercise or defence of legal claims and there is no reason to assume that you have an overriding protection-worthy interest in your data not being passed on,
3. we are legally required to pass them on, if it is legitimate by law and required for processing contractual relationships with you. In case of data transfer outside of the European Union, the high European data protection level generally does not apply. On transmission, it is possible that there is no current resolution on appropriateness of the EU commission within the meaning of sect. 45 para. 1, 3 GDPR. This means that the EU commission has not positively determined so far that the country-specific data protection level corresponds to the data protection level of the European Union due to the GDPR; therefore, we have created the above suitable guarantees,
4. we are obliged by an official or court decision, or
5. if this is helpful for legal or criminal prosecution.

Potential recipients include consultants, auditors, lawyers, courts or authorities.

36. Use of artificial intelligence

We use applications that use generative artificial intelligence. This is done, among other things, so that we can optimise our processes and offer you an improved service. If the providers of the applications used are located in other EU countries, your data may be processed in other EU countries.

37. Information on the rights of data subjects

Every data subject has the right to information according to sect. 15 GDPR, the right to rectification according to sect. 16 GDPR, the right of erasure according to section 17 GDPR, the right to restriction of processing according to sect. 18 GDPR, the right to objection from sect. 21 GDPR and the right to data portability from sect. 20 GDPR. The information right and erasure right are subject to the restrictions pursuant to §§ 34 and 35 BDSG or the respective national provisions.

38. Instructions on the complaint options

You also have the right to complain to the competent data protection supervisory authority about processing of your personal data by us.

39. Instruction on revocation of consent

You may revoke your consent granted to us for processing of personal data at any time. This shall also apply to revocation of declarations of consent that were granted to us before the application of the general data protection regulation, i.e. before 25 May 2018. Please note that the revocation will only be effective for the future. Processing that took place before the revocation is not affected by this.

40. Right in case of data processing for operation of direct marketing

You have the right according to sect. 21 para. 2 GDPR to object to processing of the personal data concerning you at any time. If you object to processing for the purpose of direct marketing, we shall no longer process your personal data for these purposes. Please note that the objection will only be effective for the future. Processing that took place before the objection is not affected by this.

41. Note on the objection rights on consideration of interests

As far as we base processing of your personal data on consideration of interests, you may object to processing. When exercising such an objection, please present the reasons why we should not process your personal data as described by us. In case of your justified objection, we will review the situation and shall either cease data processing or adjust it, or explain our mandatory grounds to be protected to you.

42. Links to other websites

Our websites may contain link to websites of other providers. Please note that this data protection statement only applies to the websites of www.BESTSECRET.com. We cannot influence or control whether other providers comply with the applicable data protection provisions.

43. Changes to the data protection statement

We reserve the right to change or adjust this data protection statement at any time under observation of the applicable data protection provisions.