

# Privacy Policy EN

## Privacy Policy for BESTSECRET Onlineshop and BESTSECRET Stores

**Last amended: June 2025**

Best Secret GmbH and Best Secret Retail Wien GmbH, together with their affiliated companies pursuant to Sections 15 et seq. German Stock Corporation Act (AktG), belong to the BESTSECRET Group (jointly the “**BESTSECRET Group**”).

For the purposes of better readability, both Best Secret GmbH and Best Secret Retail Wien GmbH are hereinafter referred to individually and collectively as “**BESTSECRET**”.

Below you will find a list of all companies belonging to the Best Secret Group that are involved in the processing of personal data:

1. Best Secret Group SE  
Margaretha-Ley-Ring 27  
85609 Aschheim  
Germany
2. Best Secret GmbH  
Margaretha-Ley-Ring 27  
85609 Aschheim  
Germany
3. Best Secret Logistik GmbH  
Parsdorfer Str. 13  
85586 Poing  
Germany
4. Best Secret Retail Wien GmbH  
Gonzaga Gasse 9/11/13  
1010 Vienna  
Austria
5. Best Secret Hellas S.M. S.A.  
131 Dodonis  
45221 Ioannina  
Greece

6. Best Secret Poland Sp. z.o.o.  
ul. Stefana Banacha 2,  
66-100 Krężoły  
Poland

7. Best Secret S.r.l.  
Via Generale Gustavo Fara 26  
20124 Milan  
Italy

BESTSECRET takes the protection of your personal data very seriously and collects and uses your personal data exclusively within the framework of the applicable statutory provisions.

To ensure that you feel safe when using our services, we provide you with an overview of how the BESTSECRET Group guarantees this protection and which types of data are collected for which purpose. The current version of the Privacy Policy is available on our website at any time.

The Privacy Policy applies to the following services:

- Onlineshop [www.bestsecret.com](http://www.bestsecret.com) including all localised domains thereof (“**Onlineshop**”) and their mobile applications, operated by Best Secret GmbH, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany
- Visiting and shopping in the BESTSECRET Stores (BESTSECRET Premium & Outlet Stores, Margaretha-Ley-Ring 23-27, 85609 Aschheim or BESTSECRET Premium & Outlet Stores, Ingolstädter Str. 40, 80807 Munich, BESTSECRET Premium & Outlet Store, Marktstrasse 6, 2331 Vösendorf) or in Austria (BESTSECRET Premium & Outlet Store, Marktstrasse 6, 2331 Vösendorf) of Best Secret Retail Wien GmbH, Berggasse 16, 1090 Vienna (hereinafter jointly referred to as “**BESTSECRET Stores**”).

After providing general information in Section A., Section B. deals specifically with the processing of personal data in the Onlineshop. Section C. deals with specific features of processing in the BESTSECRET Stores and Section D. with data processing within the scope of the BESTSECRET Loyalty Programme, which applies to customers of both the BESTSECRET Stores and the Onlineshop. Section E. deals with data processing for advertising purposes. If data is processed by BESTSECRET as part of a job application, Section F applies. Section G. contains country-specific special regulations, which accordingly only apply to customers and website visitors in certain countries.

### **How to use this Privacy Policy:**

In order to ensure the best possible readability and to make it as easy as possible for you to find relevant information, we have structured this Privacy Policy as follows: The essential content is summarised at the beginning of each chapter. This section is headed “At a glance”. Further down in the same chapter you will find the section “More details”, where you can find further details on the chapter content, should this be of particular interest to you. We have moved some detailed

information to a second layer, which you can access via a link embedded in the relevant passages.

## A. General information

### 1. Who processes your data?

#### At a glance:

Your point of contact for data processing in the Best Secret Group is Best Secret GmbH.

As part of the business activities of the BESTSECRET Group, it is necessary for other companies belonging to the BESTSECRET Group to receive and process your data in addition to Best Secret GmbH. A joint control agreement within the meaning of Art. 26 in conjunction with Article 4 No. 7 of the General Data Protection Regulation (GDPR) has been concluded between the Group companies involved in the customer business in order to ensure the security of processing and the effective assertion of your rights.

The following companies of the BESTSECRET Group may have access to your data within the framework of group-wide co-operation:

<b>Manufacturing Group company</b>	<b>The purpose of the processing</b>	<b>Legal basis of the data processing</b>
Best Secret GmbH, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany	Implementation of the membership as well as operation and provision of the Onlineshop and all services in connection with the membership with BESTSECRET.  For the provision of BESTSECRET Stores in Germany and the associated services, assertion of and defence against legal claims, security department, payment processing, order processing.	Article 6 para. 1 sentence 1 lit. b GDPR
Best Secret Group SE, Margaretha-Ley-Ring 27, 85609 Aschheim, Germany	For the provision of BESTSECRET Stores and Onlineshop, as well as the associated services, assertion of and defence against legal claims, security department, payment processing, order processing.	Article 6 para. 1 sentence 1 lit. b GDPR
Best Secret Logistik GmbH, Parsdorfer Straße 13, 85586 Poing, Germany	Dispatch of parcels and processing of returns	Article 6 para. 1 sentence 1 lit. b GDPR

Best Secret Poland sp. z o. o.	Dispatch of parcels and processing of returns	Article 6 para. 1 sentence 1 lit. b GDPR
Best Secret Retail Wien GmbH, Berggasse 16, 1090 Vienna, Austria	For the provision of BESTSECRET Stores in Austria and the associated services.	Article 6 para. 1 sentence 1 lit. b GDPR

### **More details:**

As part of our business activities, it is essential that data is also regularly exchanged between the branches and business establishments within the BESTSECRET Group in order to promote and enable Group-wide cooperation. For this reason, centralised processes are not limited to the area of an individual Group company but also extend to other affiliated enterprises within the meaning of Sections 15 et seq. of the AktG. BESTSECRET Group's companies therefore work together in many areas and act as "joint controllers" within the meaning of data protection law.

The joint controller agreement concluded between the Group companies regulates the following points in particular:

- Subject matter, purpose, means and scope as well as the competences and responsibilities with regard to data processing
- Information notice to the data subjects
- Fulfilment of the other rights of the data subjects
- Security of processing
- Engagement of processors
- Procedure in cases of data breach
- Collaboration with supervisory authorities
- Liability

In this respect, all operating companies of the BESTSECRET Group involved in customer business are responsible for the processing of your personal data as joint controllers. Even if there is joint control, the parties fulfil the data protection obligations in accordance with their respective responsibilities. Within the scope of joint control, you can assert your rights in connection with data processing in particular with Best Secret GmbH, which has been designated as the point of contact by the parties to the joint control agreement. The contact details of Best Secret GmbH and its data protection officer are as follows:

Contact person responsible for data processing	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  Telephone: +49 (0) 89 / 24600 000  email: <a href="mailto:datenschutz@bestsecret.com">datenschutz@bestsecret.com</a>	Best Secret GmbH  Data Protection Officer  Margaretha-Ley-Ring 27, 85609 Aschheim, Germany  email: <a href="mailto:datenschutz@bestsecret.com">datenschutz@bestsecret.com</a>

## 2. To whom do we transfer your data?

### At a glance:

We transfer your data in certain cases if there is a substantial interest on our part.

### More details:

#### 2.1 Disclosure to processors

We use service providers as processors. Where necessary, they also process personal data. These include:

- IT service providers,
- Maintenance service providers,
- Marketing service providers,
- Service providers for market and opinion research,
- Service providers for customer support,
- Payment service providers,
- Printing and dispatch service providers.

The service providers are carefully selected, monitored and regularly checked by us; in particular, we ensure that technical and organisational measures are implemented to protect your data. They process the data exclusively on our instructions.

#### 2.2 Disclosure to other third parties

Your personal data will only be passed on to other third parties if this is permitted by law (e.g. for the purpose of contract processing or invoicing or if you have given your prior consent). We expressly do not sell information on customers. The data will only be transferred for the purposes described in this Privacy Policy.

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

We will only share your personal data with third parties if:

- You have given your express consent,
- the transfer is necessary for the assertion, exercise or defence of legal claims and there is no reason to assume that you have an overriding interest worthy of protection in the non-disclosure of your data,
- there is a legal obligation for the transfer,
- it is legally permissible and necessary for the processing of contractual relationships with you,
- we are obliged to do so by an official or court decision, or
- this is necessary for legal or criminal prosecution.

Possible recipients can be:

- Auditors, tax consultants, lawyers,
- Courts and authorities,
- Logistics service provider,
- Service provider for document and data destruction,
- Banks and payment service providers,
- Other consultants.

### **2.3 Use of artificial intelligence**

We use applications that utilise generative artificial intelligence (AI). 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 that are used are located in another EU country, your data may be processed in another EU country.

## **3. How is the protection of your data ensured when data is processed in third countries?**

**At a glance:**

If we use service providers outside of the EU or the European Economic Area (EEA), we take appropriate safeguards to ensure an adequate level of data protection when transferring personal data.

### **More details:**

To ensure an adequate level of data protection when transferring personal data, we take appropriate safeguards in accordance with Art. 44 et seq. GDPR (e.g., entering into EU standard contractual clauses, additional technical and organisational measures such as encryption or anonymisation). Please note that despite careful selection and commitment, a service provider may process data outside of the EU or the EEA or may be subject to a different legal system due to its registered office and may therefore not offer a level of data protection in accordance with the GDPR.

Although an EU-US Data Protection Agreement is currently in force, BESTSECRET has decided to continue to conclude the EU Commission's standard contractual clauses with processors in the USA.

## **4. What are your rights in relation to data processing carried out by BESTSECRET?**

### **At a glance:**

Every data subject shall have the following rights:

- Right of access in accordance with Art. 15 GDPR
- Right to rectification in accordance with Art. 16 GDPR
- Right to erasure in accordance with Art. 17 GDPR
- Right to restriction of processing in accordance with Art. 18 GDPR
- Right to object to processing in accordance with Art. 21 GDPR
- Right to data portability in accordance with Art. 20 GDPR

You also have the right to complain to the competent Bavarian State Office for Data Protection Supervision (*Bayerisches Landesamt für Datenschutzaufsicht*) about the processing of your personal data.

### **More details:**

The restrictions under Sections 34 and 35 of the German Federal Data Protection Act (BDSG) or the respective national regulations, respectively, apply to the right to information and the right to erasure.

You also have the right to complain to the competent Bavarian State Office for Data Protection Supervision (*Bayerisches Landesamt für Datenschutzaufsicht*) about the processing of your personal data.

You can withdraw your consent to the processing of personal data at any time. This also applies to the notices of withdrawal of consent given to us before the General Data Protection Regulation came into force, i.e. before 25 May 2018. Please note that the withdrawal is only effective for the future. Processing that took place before the withdrawal is not affected hereby.

In accordance with Art. 21, para. 2 GDPR, you have the right to object at any time to the processing of your personal data for the purpose of direct marketing. In the event of an objection, your personal data will no longer be processed for such purposes. Please note that the objection is only effective for the future. Processing that took place before the objection is not affected hereby.

If we base the processing of your personal data on a balancing of interests, you can object to the processing. When objecting to the processing, we ask you to explain the reasons why we should not process your personal data as described by us. In the event of your justified objection, we will examine the situation and either discontinue or adapt the data processing or explain our compelling legitimate grounds to you.

## **5. Amendments to this Privacy Policy**

We reserve the right to amend this Privacy Policy at any time in compliance with the applicable data protection regulations or to adapt it to our actual processes, respectively.

## **B. Data processing in the context of the Onlineshop**

### **At a glance:**

Different data processing in connection with the Onlineshop takes place when a) accessing the website, b) registering and logging in as a member on the website and c) when ordering items in the Onlineshop. In addition, data is also processed for other functionalities that can be used via the web shop (such as the “Invite friends” function). The type of data processed and the purposes for processing differ in each case. The third-party tools used for the individual processing operations also differ.

When the website is simply accessed without registration or login or without the visitor having consented to the use of further cookies, we only collect data that is technically necessary to display the website. When you register or log in to the Onlineshop, additional data is also collected and processed that is required to carry out the membership or to display your information in your BESTSECRET Account (“**Account**”). When you place an order in the Onlineshop, we process your data in particular in order to be able to process the order and payment. For this purpose, individual data points are also passed on to our payment service providers to the extent necessary.



**More details:**

## **1. Data collection when visiting our website**

If you use the website purely for information purposes, i.e. if you do not register or otherwise transmit information to us, we only collect the personal data that your browser transmits to our server. This data is technically necessary for us to display our website to you and to ensure stability and security. We furthermore use the data to ensure your security and the security of the ordering process (legal basis is the provision of our service in accordance with Art. 6 para. 1 sentence 1 lit. f GDPR).

We may also use your data collected when you access our website or app for the purpose of ensuring a technically stable and secure website, for product development and for the continuous optimisation of our services and business processes, provided that the data protection requirements for such use are met.

### **1.1 Log files**

For technical reasons, personal data that is generated when our website is accessed is retained as “log files” by default.

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Technical data such as: Operating system used, browser type and version, device (smartphones, tablets or other end device), date and time of access	Optimised presentation of the website  Ensuring the proper operation of the website	Art. 6 para. 1 sentence 1 lit. f GDPR	Deletion after 60 days at the latest
IP-Address	Ensuring the proper operation of the website	Art. 6 para. 1 sentence 1 lit. f GDPR	Deletion after 60 days at the latest

The collection of the data described above for the provision of the website and the retention of the data described above in log files is strictly necessary for the operation of the website.

### **1.2 Monitoring and analysis tools**

We use error analysis services and a monitoring and analysis platform. In detail, these are:

#### **a. Error analysis by Rollbar**

We use the Rollbar error analysis service from Rollbar Inc. (Rollbar, 51 Federal Street, San Francisco, CA 94107, USA) to ensure the system stability of our website. With the help of Rollbar, we can recognise technical errors that occur on our website and then rectify these errors immediately. The purpose of this data processing is the technical monitoring of our website and the documentation of error messages in order to ensure and optimise the technical stability of the website.

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

- IP address of the accessing computer
- User Agent
- Operating system, language and version of the accessing end device
- Browser version of the calling computer
- Language of the browser used
- Document Object Model (DOM) event (e.g. “clicked on button xy”)
- Time zone difference to Greenwich Mean Time (GMT).
- Name of the retrieved file
- Date and time of the retrieval
- Information about the error that has occurred (e.g. JavaScript error, network error)

The legal basis for processing is Art. 6 para. 1 sentence 1 lit. f GDPR. Our legitimate interest is to offer a technically stable website and to enable you to use our website with as few errors as possible.

The data collected will be erased 90 days after collection.

To enable data processing, data is transferred to Rollbar in the USA, where the error analysis service is operated on Google data centres (Google Data Center, Council Bluffs, Iowa 51501/USA) (Google Cloud). We have concluded a data processing agreement with Rollbar in accordance with Art. 28 GDPR, according to which Rollbar undertakes to guarantee the necessary protection of your data and to process it exclusively on our behalf and in accordance with our instructions in accordance with the applicable data protection regulations. An adequate level of protection within the meaning of Art. 44 et seq. GDPR is guaranteed by the use of the “EU standard contractual clauses” pursuant to Art. 46 GDPR in the context of data processing. You can request a copy of the EU standard contractual clauses concluded with the provider from the BESTSECRET Group’s data protection officer.

Further data protection information concerning Rollbar can be found at <https://docs.rollbar.com/docs/privacy-policy> and <https://docs.rollbar.com/docs/security>.

#### **b. Monitoring and analysis by Datadog**

We use the Datadog monitoring and analysis platform from Datadog, Inc. (Datadog, 620 8th Ave, 45th Floor, New York, NY 10018) for effective troubleshooting and security analyses.

With the help of Datadog, we can recognise technical errors occurring on our website on the basis of log files so that we can then rectify these errors immediately. The purpose of the data processing is to ensure a technically stable and secure website and the continuous optimisation of our services.

The following data is processed during operation of the platform and in the event of application errors:

- customerPK (Primary Key assigned as technical key by BESTSECRET)
- customerId (customer number)
- customerUid (email)
- clientIp (IP address)
- SchuboCustomerNumber (customer number of the customer card holder, recorded when error messages occur)
- SchuboCardNumber (customer card number, recorded when error messages occur)
- Customer contact details (recorded when error messages occur) - the following components may be recorded: Mr/Mrs, first name, last name of the customer (GMT)
- Customer email address (recorded in the event of error messages)
- Information about the error occurring
- Operating system, language and version of the calling browser or end device
- Time zone difference to Greenwich Mean Time (GMT).
- Name of the retrieved file
- Date and time of the retrieval

The legal basis for processing is Art. 6 para. 1 sentence 1 lit. f GDPR, our legitimate interest in offering a technically stable and secure website and enabling you to use our website as error-free as possible.

The data collected will be erased no later than 60 days after collection.

We have selected the EU service option offered by Datadog so that the data is retained exclusively in data centres within the EU. The Google Cloud platform in Germany is used for this. Within the scope of the data processing listed, however, it cannot be ruled out that data will also be transferred to the US or that there is a possibility of access from the third country for support purposes.

We have concluded a data processing agreement with Datadog in accordance with Art. 28 GDPR, according to which Datadog undertakes to guarantee the necessary protection of your data and to process it exclusively on our behalf and in accordance with our instructions in accordance with the applicable data protection regulations. An adequate level of protection within the meaning of Art. 44 et seq. GDPR is guaranteed by implementing the “EU standard contractual clauses” pursuant to Art. 46 GDPR in the context of data processing. You can request a copy of the EU standard contractual clauses concluded with the provider from the BESTSECRET Group’s data protection officer. Further information on this can be found at <https://www.datadoghq.com/legal/eea-data-transfers/> and in Datadog's data protection notice.

Our websites may contain links to websites of other providers. We would like to point out that this Privacy Policy applies exclusively to the websites of the BESTSECRET Group. We have no influence on and do not check whether other providers comply with the applicable data protection regulations.

## **2. Data collection during registration and/or login on our website**

If you register at [www.bestsecret.com](http://www.bestsecret.com) and/or log in, personal and user-related data as well as technical data are retained.

### **2.1 Technical data**

Technical data is retained and analysed anonymously in order to further improve the functionality of the shop and make it more user-friendly.

The following processing of data is necessary for the provision of our services and the operation of the website.

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Personal data such as: Name, email address, gender, country	Implementation of membership Customer communication	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose or until the expiry of commercial and tax retention periods (Section 257 German Commercial Code (HGB), Section 147 German Tax Act (AO))
Behavioural data such as: Last login, registration date	Customer communication Implementation of membership	Art. 6 para. 1 sentence 1 lit. f GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Personal data such as: Name, email address, country	For registration and login	Art. 6 para 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose or until the expiry of commercial and tax retention periods (Section 257 German Commercial Code (HGB), Section 147 German Tax Act (AO))

### **2.2 Authentication**

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

When you first register via the login form on our website, we collect your email address for this purpose, use the data to check whether you already have a membership with us and then transfer the login data (email address and encrypted password) to Okta. Okta retains this login data on our behalf for later synchronisation during login processes. The data is used exclusively for your authentication. As part of this authentication process, we then receive the verification result back from Okta. During the authentication process, Okta collects the following personal data: email address, date of registration, date of last login, IP of last login, browser and operating system used during registration.

BESTSECRET offers its members the option of registering via third-party services such as Google, Facebook or Apple and then logging in. In doing so, the member is redirected to the respective website of the provider and allows BESTSECRET to link to the respective service in order to transfer information necessary for setting up a membership or logging in (e.g. first name, last name, email address, profile picture, service ID). You can change or stop the transfer of information from the services to BESTSECRET at any time via the respective service. Please note that you may then no longer be able to log in to the Onlineshop. The legal basis for the use of third-party services is consent (Art. 6 para. 1 sentence 1 lit. b GDPR). Further information on third-party services can be found at:

[Facebook](#), [Apple](#), [Google](#)

Your data will be used to set up, provide and personalise your member profile as part of the provision of a contractual service. The legal basis for data processing is the fulfilment of the contract (Art. 6 para. 1 sentence 1 lit. b GDPR) and our legitimate interest (Art. 6 para. 1 sentence 1 lit. f GDPR) in maintaining an effective and secure registration system to operate our services that require registration.

Okta processes your data in data centres of Amazon Web Services (AWS for short) in Frankfurt am Main and Dublin/Ireland, an offer of Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxembourg. We have concluded a data processing agreement with Okta in accordance with Art. 28 GDPR, under which Okta 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 with Okta as appropriate safeguards in accordance with Art. 46 GDPR. You can request a copy of the EU standard contractual clauses concluded with the provider from the BESTSECRET Group's data protection officer.

Your data will be retained in accordance with legal obligations and then erased. Generally, personal data is only retained for as long as it is necessary for the aforementioned purposes and for as long as the company is obliged to store it due to legal obligations to provide evidence and retain data. Your data as a registered member will be deleted by us when your membership ends. At the same time as your Account is deleted, the data retained at Okta will also be deleted.

You can find further information on Okta's data protection policy at <https://okta.com/privacy/>.

## 2.3 Establishing contact

On this website we use a chat system that is used to answer enquiries and uses AI. During use, the chat content you share is processed for chat history purposes. Cookies can be used for the operation of the chat function, which enable the site visitor to be recognised. The processing of personal data in this context is based on our legitimate interest in providing efficient and fast customer support. This does not affect your cookie settings. Cookies are only set with your consent.

On the help page in the web shop, you also have the option of contacting customer support via chat. If you wish to use this, you will need to enter your name and email address so that the relevant customer support employee can assign you to an Account more easily and thus process the enquiry as efficiently as possible.

Data	Processing purpose	Legal basis	Retention period
Data for processing the member's enquiry	Processing the customer enquiry	Art. 6 para. 1 sentence 1 lit. b GDPR or Art. 6 para. 1 sentence 1 lit. f GDPR	Erasure after cessation of purpose or expiry of statutory retention obligations (Section 257 HGB)

## 2.4 Suspending your membership

We reserve the right to suspend your membership in individual cases. We use this option if a member is inactive for a longer period of time. In this case, you will be notified of the imminent cancellation of your membership by setting a deadline. If you do not make a purchase within the set period, the suspension will take effect. Your Account is then initially blocked but can be reactivated within one year under certain conditions. For this purpose, we will continue to store your personal data for a period of one (1) year from the effective date of Account suspension, unless you inform us within this period that you wish your Account to be reactivated or you no longer wish for it to be retained. Details on reactivation and the process in general can be found in our current [Terms and Conditions of Use](#). The legal basis for processing is Art. 6 para. 1 sentence 1 lit. f GDPR, our legitimate interest in reserving membership of the BESTSECRET Shopping Community for active members.

# 3. Data collection and use in the context of orders

## 3.1 General information

Information that we receive from you helps us to process your order as smoothly as possible, to eliminate sources of error, to improve our service for you and to prevent misuse and fraud.

## **3.2 Processing of orders and payments**

We use your data to process orders and payments, deliver goods and provide services. As part of order processing, for example, the service providers we use for this purpose (such as carriers, logisticians, banks or our marketplace partners) receive the necessary data for order and order processing. The same applies to the processing of returns. If you order a product on our Marketplace, the data required for order and order processing will also be passed on to the respective Marketplace partner so that they can deliver the order. In this case, BESTSECRET and the respective Marketplace partner are joint controllers.

In some cases, particularly in some countries, it may be necessary to pass on the telephone number and/or email 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.

You can specify and change whether additional data, such as the email address for notification of the specific delivery date, should be passed on during the order process in the check-out area. If you select the Pick-Up and Drop-Off (PUDO) delivery method, it is necessary to forward your email to the respective delivery service for order and order processing, as otherwise the delivery service cannot inform you about the arrival of the parcel at the respective parcel shop. In this case, you do not have the option of preventing the transfer by making the appropriate settings.

You can find more information about the payment service providers we use here:

[https://www.bestsecret.com/uf/assets/documents/payment/Zahlungsmethoden-AGB-und-DSE\\_en.pdf](https://www.bestsecret.com/uf/assets/documents/payment/Zahlungsmethoden-AGB-und-DSE_en.pdf)

## **3.3. Orders after deletion requests**

If we receive a deletion request from you, we will take all necessary steps to delete your Account in accordance with Art. 17 of the General Data Protection Regulation (GDPR). If you place an order with us before we have been able to delete your data, we will understand this order as a request to revive your membership with us. We accept this request and will therefore not delete your Account and your data in this case. The legal basis for retention is then the fulfilment of our contract with you (Art. 6 para. 1 lit. b GDPR).

## **3.4 Notifications when an item is unavailable**

If you would like to order an item that we do not currently have in stock in the size you require, you have the option of being notified when the item is available again. If you select this option and have activated push notifications, you will be informed by push notification and email as soon as the item is available again in your desired size. This applies as long as the notification setting for the respective article is activated. If push notifications are not activated, we will only inform you by email when available. The legal basis for the notification is taking steps prior to entering into a contract (Art. 6 para. 1 lit. b GDPR).

### 3.5 Notifications about items on your wish list

If you have added items to the wish list in your Account, we can send you notifications about these items for as long as they are on your wish list. The content of these notifications can be, for example: Low stock of the item in question in the size you require, price reductions, etc. If you have activated push notifications, you will be informed via push notification, otherwise via email or in-app messages. The legal basis is taking steps towards the conclusion of a contract (Art. 6 para. 1 lit. b GDPR).

### 3.6 Information on dispatch status

As part of your order, you have the option of giving your consent to the sharing of your email address and telephone number to the respective shipping partner in order to enable the shipping partner to send you notifications about the shipping status.

Consent shall be on a voluntary basis and can be withdrawn at any time. Your consent given when making a purchase in the web shop will be saved for future purchases, so that the corresponding checkbox “Delivery tracking” is already selected in this case. If you do not wish to maintain your consent for your next purchase, you can deselect the checkbox in the order area of your shopping basket at any time. This selection is then also saved for all future purchases.

Please note that if you select the parcel shop delivery method (Pick Up Point), it is necessary to forward your email address to the respective delivery service for order and order processing, as otherwise the delivery service cannot inform you about the arrival of the parcel at the respective parcel shop. The processing of the email address takes place in this case of the selection of the delivery method parcel shop (Pick Up Point) on the basis of Art. 6 para. 1 lit. b GDPR.

Please note that in case of a change of your address the new address may be forwarded automatically to us by the delivery service provider. In these cases, we are therefore able to update your address in your Account without having received a notice about the address change from you.

Data	Processing purpose	Legal basis	Retention period
Personal data such as: email address, telephone number	Forwarding to shipping partners for delivery tracking	Art. 6 para. 1 sentence 1 lit. a GDPR	Until withdrawal
Time of consent	Delivery tracking	Art. 6 para. 1 sentence 1 lit. a GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Time of withdrawal	Proof of withdrawal	Art. 6 para. 1 sentence 1 lit. a GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership



### 3.7 Returns

You have the option of returning items you have ordered to us. The following data is processed:

Data	Processing purpose	Legal basis	Retention period
Customer information, order and returns data, collection and returns data	Processing returns	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

### 3.8 Assessment of creditworthiness

To be able to offer you the best possible payment options, we must protect you and ourselves from misuse. Therefore, depending on the payment method, we transfer the personal data required for an identity and credit check (first and last name, address, date of birth, gender, email address, telephone number, time of registration, purchases made and information on the amount of the claim and due date of the claim) to our payment service provider. The transfer is based on our legitimate interest in the prevention of misuse and the protection from payment defaults, because we deliver the goods upfront (Art. 6 para. 1 lit. f GDPR).

The probability of default is assessed on the basis of a mathematical-statistical procedure. Our payment service provider uses this information to make a balanced decision about the payment options to be granted to you.

You will be informed separately during the payment process before the actual transfer of personal data that and which personal data will be transferred and you can terminate the process if needed.

In addition, the general terms and conditions and data protection notices of our payment service providers apply. You can find more information about our payment service providers here: [https://www.bestsecret.com/uf/assets/documents/payment/Zahlungsmethoden-AGB-und-DSE\\_en.pdf](https://www.bestsecret.com/uf/assets/documents/payment/Zahlungsmethoden-AGB-und-DSE_en.pdf)

## 4. Tracking technology

### At a glance:

We use tracking technologies, such as cookies, to improve our services and optimise their use for you. Cookies are small text files that are retained on your computer's operating system when you visit our website. Cookies contain, among other things, a characteristic string of characters that

enables the browser to be uniquely identified when the website is accessed again and make it unnecessary to re-enter your data each time you visit the website.

There are various tracking technologies. Some are technically necessary for the smooth operation of the website. Other tracking technologies are beneficial for the optimisation of our website and app. A third category of tracking technologies enables us to personalise the website or app for your individual needs.

Apart from the technically necessary tracking technologies, you can refuse the use of tracking technologies. When the website is accessed for the first time, a corresponding cookie banner opens, which can be used to provide or refuse consent. The provided consent can be withdrawn at any time with effect for the future. You can do this at any time in the footer of the website under “Cookie settings” or in your Account.

## **More details:**

### **4.1 Technically necessary tracking technologies**

We use cookies as part of the technically necessary tracking technologies. These cookies are required for the operation of a website/app and its functions. This may include, for example, cookies that store certain user settings (e.g. shopping basket settings, language settings, gender preferences or log-in data), opt-out cookies, cookies from payment service providers that are set to carry out the payment process, cookies from shipping service providers that are necessary for tracking shipments, or the Google Tag Manager to manage your tracking settings. The legal basis for the use of technically necessary tracking technologies is Section 25 para. 2 no. 2 German Teleservices Data Protection Act (TDDDG) and our legitimate interest in offering you the respective function or service (Art. 6 para. 1 lit. f GDPR).

These cookies can nevertheless be deactivated by changing the settings of the respective browser. However, the (error-free) use of the website or the use of certain functions and services can then no longer be guaranteed.

### **4.2 Tracking for Optimisation & Performance of the website/app**

Tracking for Optimisation & Performance is used to evaluate the user behaviour of the BESTSECRET website and app for performance analysis and statistical purposes. Based on these evaluations, BESTSECRET can optimise the user-friendliness of the shop and correct any errors that may occur.

Tracking technologies for Optimisation & Performance include:

- Google Firebase
- Hotjar

The exact functionality and the affected data categories of the individual tracking technologies are described here: [https://www.bestsecret.com/uf/assets/documents/tracking/tracking\\_en.pdf](https://www.bestsecret.com/uf/assets/documents/tracking/tracking_en.pdf).

Tracking for Optimisation & Performance is only used if you have given us your consent to do so in accordance with Art. 6 para. 1 lit. a GDPR. Your consent also refers to Section 25 (1) TDDDG. The consent given on the website also applies to the mobile applications. The consent settings made in the mobile application apply to both the website and the mobile applications. You can withdraw your consent at any time by deselecting the tracking setting “Optimisation & Performance” in the cookie settings in the footer. For technical reasons, the opt-out usually only takes effect after 48-72 hours. If you make changes to the consent for the app, you can speed this up by restarting the app.

We use the consent management tool “Usercentrics Consent Management Platform” from Usercentrics GmbH to manage your tracking settings. In this respect, the recipient of your data within the meaning of Art. 13, para. 1, lit. e) GDPR is Usercentrics GmbH. As part of order processing, we transfer your consent data to Usercentrics GmbH, Sendlingerstr. 7, 80331 Munich, Germany, in its quality of processor. Consent data shall mean the following data: Date and time of the visit or consent / refusal, device information. The data is processed for the purpose of compliance with legal obligations (obligation to demonstrate pursuant to Art. 7 para. 1 GDPR) and the associated documentation of consents and thus on the basis of Art. 6 para. 1 lit. c) GDPR. Local retention is used for the purposes of data retention. The consent data will be retained for 1 year. The data is retained in the European Union. Further information on the data collected and contact options can be found at <https://usercentrics.com/privacy-policy/>.

### **4.3 Tracking for personalisation**

Tracking for personalisation is used to create personalised advertising tailored to your interests on our websites and app or on the websites of our advertising partners and for other marketing purposes.

Tracking technologies for personalisation include:

- Google Ads
- Google Analytics
- Google Marketing Platform
- Criteo
- Salesforce
- Meta
- Snapchat
- TikTok
- RTB House
- Pinterest
- Adjust
- Socialbakers

In general, there are two ways in which tracking tools can receive personal data: a) certain information on your use of the Webshop can be collected by the tools directly and b) upon your prior consent, we can include your email-address in lists uploaded to tracking tools in the course of so-called ‘Audience Uploads’.

The exact functionality of the individual tracking technologies is described in more detail here: [https://www.bestsecret.com/uf/assets/documents/tracking/tracking\\_en.pdf](https://www.bestsecret.com/uf/assets/documents/tracking/tracking_en.pdf).

When tracking for personalisation, certain information about your behaviour in the Onlineshop (e.g. wish list behaviour, purchases) and about you personally (e.g. age, gender, region in which you live) is used to show you products that may be of interest to you. Due to the large number of items that we offer in our Onlineshop, it is necessary for us to present our content and offers in a way that suits your interests in order to make your shopping experience as easy and satisfying as possible.

Tracking for personalisation is only used if you have given us your consent to do so in accordance with Art. 6 para. 1 lit. a GDPR. Your consent also refers to Section 25 (1) TDDDG. The consent given on the website also applies to the mobile applications. The consent settings made in the mobile application apply to both the website and the mobile applications. You can withdraw your consent at any time by deselecting the tracking setting “Personalisation” in the cookie settings in the footer. For technical reasons, the opt-out usually only takes effect after 48-72 hours. If you make changes to the consent for the app, you can speed this up by restarting the app.

Your consent in this regard is also managed via Usercentrics. The information on Usercentrics in Article 4.2 of this Privacy Policy also applies in this case.

Some of our advertising partners use “click IDs”. This enables the advertising partner to assign you an ID when you load the page, which can be used to assign interactions on our website to you as an individual user. However, it is only possible to draw conclusions about your person when combined with other data. The information obtained via click IDs is important for us to be able to determine which advertising channels are most successful in generating new customers. You can find out more about this in the data protection information of the relevant advertising partners, which is also linked under the following [https://www.bestsecret.com/uf/assets/documents/tracking/tracking\\_en.pdf](https://www.bestsecret.com/uf/assets/documents/tracking/tracking_en.pdf).

## **5. Invite friends**

We offer you the opportunity to recommend our services to interested parties. To do this, go to the menu in your Account and click on “Invite friends”. By clicking on “Invite friends”, you will receive an exclusive invitation link that you can send via social media or email. The invitation is issued by you and sent directly to the person invited.

If you accept the invitation, we will retain the personal data of the person who invited you. As a closed shopping community, we only accept members who have been invited by existing members. The retention serves the purpose of verification and traceability and takes place for the fulfilment of the membership contract.

Once you have registered, you are subject to all the requirements defined above for members in Section B.2.

The member who invited you will receive a discount voucher when you order something from BESTSECRET. As each member can only issue a limited number of invitations, inviting members have an interest in being informed which invited person has registered and ordered. In this respect, your name will be passed on to the inviting member.

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Personal data of the invited person such as: email address, invitation message, time of invitation, geolocation (when using the invitation link)	Implementation of the membership contract	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Personal data of the inviting member: First name, surname, email	Implementation of the membership contract	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

As we are a closed shopping community and unfortunately can only accept a limited number of members, we offer interested persons the opportunity to be placed on a waiting list. This option is available if a member sends an invitation to a person, but the member no longer has any invitation rights.

We retain the following data as part of the waiting list:

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Personal data of the invited person such as: First name, surname, email address, time of the registration attempt	(Pre-contractual) measure for membership	Article 6 para. 1 sentence 1 lit. b GDPR	Erasure after cessation of purpose, at the latest 30 days after refusal or unconfirmed invitation by BESTSECRET

## 6. Compliance with customs regulations

Due to several EU regulations (2580/2001/EC, 881/2002/EC and 753/2011/EC) and other legal requirements, we as a company are required to compare our customers' data with publicly available foreign trade and embargo lists before concluding a purchase agreement. We carry out this comparison because the processing is necessary to fulfil the above-mentioned legal obligations (Art. 6 para. 1 lit. c GDPR). We only carry out the comparison when you place a paid order for goods on our website. Only the following inventory data is synchronised: First name,

surname and address. The data will be deleted after the statutory retention period of 10 years has expired.

## C. Data processing in the BESTSECRET Stores

### At a glance:

When you visit one of our BESTSECRET Stores, various data processing activities take place. This applies to your access to the BESTSECRET Stores, which is generally only available to certain members; in addition, personal data is also processed during cashless payments in the BESTSECRET Store or during interactions with customer service.

### More details:

Only selected members are authorised to access the BESTSECRET Stores. The specific requirements for access authorisation can be found in our Terms and Conditions of Use. We process the following data in order to clearly identify the member and prevent cases of abuse and fraud.

Data	Processing purpose	Legal basis	Retention period
Account data, photograph	Proof of access authorisation, identification, abuse and fraud prevention	Art. 6 para. 1 sentence 1 lit. f GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Purchase and visit history	Points as part of the loyalty programme, marketing purposes	Art. 6 para. 1 sentence 1 lit. a and b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

As part of the cashless payment of your purchase (e.g. using a bank card), your corresponding payment data (IBAN or credit card number, card expiry date, card sequence number, date, time, amount of payment, terminal identifier (location, company, branch)) will be forwarded to the responsible service providers (network operators, acquirers, banks) exclusively for the purpose of processing the purchase contract (Art. 6 para. 1 lit. b GDPR).

Your data will be erased after expiry of the statutory retention periods (Section 257 HGB, Section 147 AO).

The forwarding of the payment data is necessary to complete the payment process and the purchase. If you do not wish to provide your data for this purpose, you have the option of paying in cash or not making a purchase.

#### **a. Daily authorisations**

In addition, selected members can enable another person to visit the BESTSECRET Stores on a day of their choice within 30 days of the issuing of a respective day authorisation by providing it to the authorised representative. For this purpose, the first name, surname and email address of the authorised representative shall be provided. The legal basis for this is a legitimate interest pursuant to Art. 6 para. 1 sentence 1 lit. f GDPR in the access of non-members to the BESTSECRET Stores. The data will be erased no later than 90 days after termination of membership.

#### **b. Returns**

During your visit to the BESTSECRET Store, you have the option of returning parcels in the event of a return. The following data is processed:

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Customer information, order and returns data, collection and returns data	Carrying out returns	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

### **D. Data collection as part of the Loyalty Programme**

As part of the Loyalty Programme, members collect points or vouchers through various activities in the Onlineshop or BESTSECRET Store. Depending on the number of points, the member receives special benefits. The member also has the opportunity to receive commissions for the purchases of the recommended persons. The Loyalty Programme is part of the BESTSECRET membership. The legal basis for the processing of personal data to the extent necessary for the implementation of the Loyalty Programme is therefore Art. 6 para. 1 sentence b GDPR.

We retain the following data for this purpose:

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Status of the member	Implementation of the Loyalty Programme	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Points from purchases, recommendations from new members and other activities	Implementation of the Loyalty Programme	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

Commissions from purchases by recommended persons and resulting commissions	Implementation of the Loyalty Programme	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
---	---	--	--

## E. Advertising and other measures to optimise the offer

### At a glance:

The sending of newsletters is an essential part of your contractual relationship with BESTSECRET as a member of the BESTSECRET Community. For this reason, the sending of newsletters is an exclusive contractual service provided by BESTSECRET to its members, and as a member, you will automatically receive newsletters upon your registration with BESTSECRET, but you can unsubscribe at any time. Without prior consent, it is also possible for us to send you direct advertising for products that are similar to those that you have already purchased from us. When you use the app, we will also send you advertising via in-app notifications, in-app messages and inbox messages if you have given your consent. We also process your data as part of your participation in competitions and customer satisfaction surveys.

### More details:

#### 1. Newsletter

For the purposes of this Privacy Policy, a newsletter is defined as follows:

- Current information about brands, trends, offers, promotions or product categories,
- Updates on items that are on your wish list or in your shopping basket,
- Personalised recommendations of items if we assume that these could be of interest to you based on your previous orders and your behaviour in the web shop,
- Vouchers and status updates on your membership, and
- Updates on brands that you have marked as favourites on our pages.

Our newsletters are an integral part of the BESTSECRET membership and our member benefits, allowing you to take advantage of the exclusive benefits of the membership. Receipt of the newsletter is therefore essential for the registration of your membership. The legal basis for the sending of newsletters is the fulfilment of the contract pursuant to Art. 6 para. 1 sentence 1 lit. b GDPR.

However, you can unsubscribe from one or all newsletter categories at any time under the “Newsletter” menu item in your Account or via the unsubscribe links provided at the end of each newsletter. Such will be understood as your objection to the use of this contractual service and the respective processing of your data in the future. We will accept this objection without further assessment and unsubscribe you from the receipt of one or more newsletters for the future.



Alternatively, you can change the frequency or content of the newsletter in the “Settings” menu item in your Account at any time.

The newsletter may be sent by BESTSECRET or by Salesforce Inc, The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA.

To send the newsletter, BESTSECRET also uses the Salesforce Marketing Cloud service, which is operated by Salesforce.com Inc, The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA. Data may be transferred to the USA and thus to a third country when using Salesforce Inc.

To make our newsletters even more interesting for you in the future, standard market technologies such as cookies or tracking pixels are used in our newsletters. We evaluate your clicks in newsletters with the help of 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 your own ID so that clicks in newsletters can be clearly assigned to you. The user profile is used to customise the offer and our services to your interests. The legal basis for this is Art. 6 para. 1 sentence 1 lit. a GDPR. We take your cookie settings into account.

We also use certain data (e.g. gender, postal code, VIP status) to segment and personalise our newsletters accordingly. The legal basis for this is our legitimate interest pursuant to Art. 6 para. 1 sentence 1 lit. f GDPR.

You can change the frequency or content of the newsletter in your newsletter settings at any time or unsubscribe from the newsletter altogether.

The following data is processed for sending the newsletter:

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Personal data such as: email address, title, first name, surname, gender	Sending the newsletter	Art. 6 para. 1 sentence 1 lit. a, b GDPR	3 years after objection to receipt of newsletters or deletion of the Account
Confirmation to receipt of the newsletter, time of confirmation, newsletter preference	Sending the newsletter	Art. 6 para. 1 sentence 1 lit. a, b GDPR	3 years after objection to receipt of newsletters or deletion of the Account
Objection to receive newsletters	Proof of objection	Art. 6 para. 1 sentence 1 lit. a, b GDPR	3 years after objection to receipt of newsletters or deletion of the Account

Behavioural data such as: Opening and click rate	Analysis of user behaviour and creation of personalised advertising; segmentation for the purpose of sending push notifications	Art. 6 para. 1 sentence 1 lit. a, b GDPR	Deletion no later than 90 days after termination of membership
Personal data such as: Gender, postal code or purchases	Segmentation and personalisation	Art. 6 para. 1 sentence 1 lit. f GDPR	Deletion no later than 90 days after termination of membership

## 2. Other direct advertising

Even without express consent, we send direct advertising to the extent permitted by law. This concerns offers for products that are similar to those that you have purchased from us and through purchase of which we have received your email or postal address. The direct advertising can be sent by BESTSECRET. We also use the service provider BSZ Direkt Marketing GmbH, Wallensteinstraße 6b, 82538 Geretsried, Germany, for postal advertising via the Salesforce Marketing Cloud. Direct mail can be segmented based on demographic data, such as postcode or VIP status. You can object to the use of your email address for the purpose of direct advertising via a link provided for this purpose in the advertising email, or object to the use of your postal address by sending an email to [service@bestsecret.com](mailto:service@bestsecret.com).

Data	Processing purpose	Legal basis	Retention period
Personal data such as: email address, title, first name, surname, gender	Sending the marketing campaign	Art. 6 para. 1 sentence 1 lit. a GDPR	Until objection
Demographic data such as: Postal code, last purchase or VIP status	Sending the marketing campaign/personalisation	Art. 6 para. 1 sentence 1 lit. f GDPR	Until objection

## 3. Push notifications, in-app messages and inbox messages in the BESTSECRET App

### 3.1 Push notifications

In our app, you have the option of giving 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 in the app settings of your mobile device. If you activate push notifications, the device ID of your mobile device is sent to the service that provides the push functionality for your operating system (for Android: Google Cloud Messaging; for iOS: Apple Push Notification Service). A “Push Notification Identifier” is then created, which is used for further communication with the BESTSECRET PushServer. The

identifier does not allow any conclusions to be drawn about the user. To send the messages, BESTSECRET uses the Salesforce Marketing Cloud service, which is operated by Salesforce.com Inc, The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA. Data may be transferred to the USA and thus to a third country when using Salesforce Inc.

We also use certain data (e.g. gender, postal code, purchases) to segment and personalise our push messages and in-app messages accordingly. The legal basis for this is our legitimate interest pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR.

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Push Notifications Identifier	Sending the push notification	Art. 6 para. 1 sentence 1 lit. a GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Personal data such as: First name, surname or gender, VIP status or vouchers	Creation of the push notification	Art. 6 para. 1 sentence 1 lit. a GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

### 3.2 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. To send the messages, BESTSECRET uses the Salesforce Marketing Cloud service, which is operated by Salesforce.com Inc, The Landmark @ One Market Street, Suite 300, San Francisco, California, CA 94105, USA. Data may be transferred to the USA and thus to a third country when using Salesforce Inc.

We also use certain data (e.g. gender, postal code, purchases) as part of the in-app and inbox messages in order to segment and personalise our push messages and in-app messages accordingly. The legal basis for this is our legitimate interest pursuant to Art. 6 para. 1 sentence 1 lit. f GDPR.

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Device ID and App ID	Creation of the in-app message	Art. 6 para. 1 sentence 1 lit. f a GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

Personal data such as: First name, surname or gender, VIP status or vouchers	Creation of the in-app message	Art. 6 para. 1 sentence 1 lit. a GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
---	-----------------------------------	---	---

### 3.3 Tracking in Push Notifications, In-app Messages and Inbox Messages

To make our push notifications, in-app messages and inbox messages even more interesting for you, we evaluate your openings and clicks as well as the duration of your visit, among other things with the help of personalised links and embedded links (link wrapping). The collected data is linked to your subscriber ID. The user profile is used to customise the offer and our services to your interests. This only takes place if you have given us your consent in accordance with Art. 6 para. 1 lit. a GDPR as part of the cookie opt-in.

Data	Processing purpose	Legal basis	Retention period
Behavioural data such as: Opening and click rate, time spent	Analysis of user behaviour	Art. 6 para. 1 sentence 1 lit. a GDPR	Deletion after withdrawal of consent, at the latest 90 days after termination of membership

## 4. Competition

In the case of competitions, we use your data for the purpose of notifying you of prizes and advertising our offers. Detailed information can be found in our conditions for participation for the respective contest.

Data	Processing purpose	Legal basis	Retention period
Personal details of the winner: First name, surname, email, address and social media contact information	Organisation of the competition, notification of the winner, sending of the prize in the event of a win	Art. 6 para. 1 sentence 1 lit. f GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

## 5. Data collection as part of the VIP Club

BESTSECRET rewards particularly loyal members with the VIP Club. You collect VIP points through certain activities. Depending on your score, you can achieve Silver, Gold or Diamond status. You can find out how to achieve the respective status and what benefits are associated with it [here](#) in the Help Centre under VIP Club. Certain benefits are offered in collaboration with co-operation partners. These benefits may be limited in time, may only apply in selected countries and jurisdictions and may be cancelled at any time in the future without giving reasons.

As part of your BESTSECRET membership, you have the opportunity to join our VIP Club.

We retain the following data for this purpose:

<b>Data</b>	<b>Processing purpose</b>	<b>Legal basis</b>	<b>Retention period</b>
Personal data of the invited person/inviting person: First name, surname, email	Realisation of the VIP Club	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership
Behavioural data such as: Orders, exchanged purchases of the invited person	Realisation of the VIP Club	Article 6 para. 1 sentence 1 lit. b GDPR	Deletion after cessation of purpose, at the latest 90 days after termination of membership

## **6. Use of data for customer feedback**

We use the services of Zenloop (Zenloop GmbH, Brunnenstr. 196, 10119 Berlin, Germany), Qualtrics (Qualtrics LLC, 333 River Park Drive, Provo, Utah 84604, USA) and Trustpilot (Trustpilot A/S, Pilestraede 58, 5th floor, DK-1112 Copenhagen K) to conduct customer satisfaction surveys. The legal basis for this is Art. 6 para. 1 lit. f GDPR. The content of the survey can be both product-specific and non-specific. This involves processing survey and contact data. When using Zenloop or Qualtrics, any data collected will not be processed under your name or email address, but only pseudonymised using your customer number. Once the data has been analysed, the customer number is erased from the data record so that the data is only available to us in anonymised form. In Qualtrics, we also process data that we have previously received from Salesforce, provided that you have consented to data processing by Salesforce. In the case of survey collection via Qualtrics, personal data may be transferred to a third country, namely the USA.

The situation is different when submitting a review via the Trustpilot review platform. You will receive an invitation to submit a review either from us or directly from Trustpilot. If you decide to submit a review, it will be personalised, i.e. it will allow conclusions to be drawn about you personally, for example by referring to your name, your email address or your customer number. You can find more information on this in Trustpilot's privacy policy (<https://de.legal.trustpilot.com/for-reviewers/end-user-privacy-terms>). Trustpilot's data processing may take place in Europe or the USA. In the case of processing in the USA, personal data may be transferred to the USA and thus to a third country.

Data processing in the context of Qualtrics and Zenloop takes place in Europe. Further information on data processing by Zenloop and Qualtrics can be found in Zenloop's privacy policy (<https://www.zenloop.com/de/legal/privacy>) and Qualtrics' privacy policy (<https://www.qualtrics.com/privacy-statement/>).

If you have decided to participate in customer feedback and no longer wish to do so, you can object to further processing (via the link contained in the email).

Further details on the categories of data concerned, the purposes of processing, the legal basis for processing and the retention period can be found in BESTSECRET's information on data protection for customer surveys.

## **F. Data processing on our careers page**

On our career pages we inform you about job offers at the BESTSECRET Group. You can find more information on data processing on the career pages [here](#).

## **G. Country-specific special rules**

### **1. Sweden**

In Sweden, the provisions from the Swedish Data Protection Act (DPA) (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning) apply in addition to the provisions of the GDPR and the BDSG. In addition to the TDDDG the Swedish Act (2022:482) on Electronic Communication (Lagen om elektronisk kommunikation) shall apply.

In section A.4, the following shall apply: You also have the right to complain to the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten) about the processing of your personal data.

### **2. Austria**

In Austria, the provisions from the Austrian Data Protection Act (österreichisches Datenschutzgesetz (DSG)) apply in addition to the provisions of the GDPR and the BDSG. In addition to the TDDDG the Austrian TKG shall apply.

In section A.4, the following shall apply: You also have the right to complain to the Austrian Data Protection Authority about the processing of your personal data.

### **3. Poland**

In Poland, the provisions from the Polish Data Protection Act apply in addition to the provisions of the GDPR and the BDSG. In addition to the TDDDG the Polish Electronic Communications Law shall apply.

In section A.4, the following shall apply: You also have the right to complain to the competent Polish Data Protection Authority at your place of residence, work or the place of the alleged infringement about the processing of your personal data.

The following sentence in section E.2. does not apply in Poland: “Even without express consent, we send direct advertising to the extent permitted by law. This concerns offers for products that are similar to those that you have purchased from us and through purchase of which we have received your email or postal address.”

In section A.4, the following shall apply: For individuals residing or working in Poland, below are the details of the Polish authority to which data protection complaints can also be submitted:

President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych – PUODO)

Address: ul. Stawki 2, 00-193 Warsaw, Poland

email: [kancelaria@uodo.gov.pl](mailto:kancelaria@uodo.gov.pl)

Phone: +48 22 531 03 00

Website: [www.uodo.gov.pl](http://www.uodo.gov.pl)

Individuals have the right to lodge a complaint with this authority if they believe that the processing of their personal data violates applicable data protection regulations.

#### **4. Switzerland**

In Switzerland, the provisions of the Swiss Data Protection Act (Schweizer Bundesgesetz über den Datenschutz) apply in addition to the GDPR and the BDSG.

The following shall apply in Switzerland:

Protection of your data in case of processing in third countries

We ensure that the third countries guarantee an adequate level of data protection as determined by the Federal Council.

To ensure an adequate level of data protection when transferring personal data to other countries, we take appropriate and suitable guarantees, such as the conclusion of the EU standard contractual clauses, risk assessment (transfer impact assessment), additional technical and organizational measures such as encryption or anonymization).

Although a US-Swiss data protection agreement is currently in force, BestSecret has decided to continue to conclude the EU standard contractual clauses with the Swiss addendum with processors in the USA.

The countries in which we process personal data are as follows: In Switzerland, in the member states of the EEA, in the USA, in the United Kingdom, in Australia. We cannot rule out the possibility that sub-processors may also process personal data in other countries around the world. In such a case, our sub-processors are obliged to take the necessary measures to ensure an adequate level of data protection.

## **5. Italy**

In Italy, the provisions of the Italian Personal Data Protection Code (Legislative Decree 196/2003) apply in addition to the GDPR and the BDSG.

In section A.4, the following shall apply: You also have the right to complain to the Italian Data Protection Authority (*Garante per la protezione dei dati personali*) about the processing of your personal data.

Section E.2. shall be replaced with the following paragraph in Italy: “Even without express consent, we send direct advertising to the extent permitted by law. This concerns offers for products that are similar to those that you have purchased from us and through purchase of which we have received your email address using the email address you provided us for the previous purchase. You can object to the use of your email address for the purpose of direct advertising via a link provided for this purpose in the advertising email.”

For Italy, the following addition applies to the statements regarding cookies in Article 4:

### **Cookie Management**

#### **Consent**

When you access the website, a cookie banner is displayed that allows you to accept or reject all cookies or to make your choice by category of cookies according to your prior consent



(strictly necessary cookies are enabled by default). As long as you have not given your consent, these cookies are deactivated by default and will not be installed on your end device.

## **Setting cookies**

You can change your cookie preferences at any time:

**On our site in the cookie banner that can be accessed when you browse the site and/or via the menu item “Cookie settings”, which can be accessed from all subpages.**

When the cookie banner appears on the page, you can make your selection per cookie category. The 'Select' field in the cookie banner leads to a page showing the different categories of cookies used on the website. You can select the purposes for which cookies may be used here.

You can change your selection at any time by clicking on the 'Cookie settings' box on any page of our website.

## **In your browser**

You can set your browser so that the system prevents the retention of cookies.

Each browser has its own configuration for cookies and cookie selection. You should therefore check the functionalities of the browser you are using to see how you can change your consent to cookie retention in your browser.

To help you configure your browser, you can visit the following help pages, depending on which browser you are using:

- Internet Explorer: <http://windows.microsoft.com/it-IT/windows-vista/Block-or-allow-cookies>;
- Safari: <https://support.apple.com/it-it/safari>;
- Chromium: <http://support.google.com/chrome/bin/answer.py?hl=fr&hlrm=en&answer=95647>;
- Firefox: <https://support.mozilla.org/en-US/kb/block-websites-storing-cookies-site-data-firefox>;
- Opera: <http://help.opera.com/Windows/10.20/it/cookies.html>

## **How long will your selection be saved?**

Your choice to allow or reject cookies on our website will be saved for 6 months, after which you will be asked again for your consent or selection of authorised cookies.

## **List of third parties that use cookies on our web page**

The list contained below for France shall apply accordingly.

### **6. Belgium**

In Belgium, the provisions of the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data apply in addition to the GDPR and the BDSG.

In section A.4, the following additions shall apply:

“Please note that certain statutory exceptions may apply to the exercise of these rights in accordance with applicable national law. In Belgium, the restrictions to the right of access and the right to erasure are governed by the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, in particular:

- Article 11, which limits the right of access when the processing relates to personal data concerning criminal convictions, security measures or administrative sanctions, or when the data are processed for legal claims or journalistic purposes;
- Article 10, which allows restrictions where processing is necessary for archiving, scientific, or historical research purposes;
- Article 13, which provides specific conditions for the right to erasure (e.g. when data are required for legal obligations or public interest tasks).

You also have the right to complain to the competent authority. If you are based in Belgium, you can lodge a complaint with the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit) via [www.gegevensbeschermingsautoriteit.be](http://www.gegevensbeschermingsautoriteit.be)

### **7. The Netherlands**

In the Netherlands, the provisions of the Dutch GDPR Implementation Act ("DGIA") (Uitvoeringswet Algemene verordening gegevensbescherming) apply in addition to the GDPR and the BDSG. In addition to the TDDDG the Dutch Telecommunications Act (Telecommunicatiewet) shall apply.

In section A.4, the following shall apply: You also have the right to complain to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) via [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).

## **8. Bulgaria**

The shipping service provider used by BESTSECRET in Bulgaria carries out an automated verification process with the data provided to it in order to carry out the delivery. This concerns your name, address data, telephone number(s) and email address. This data is compared with the SDN and UN list as well as other comparable national and international lists.

## **9. France**

In France, the provisions of the French Data Protection Act apply in addition to the GDPR and the BDSG.

For France, the following addition applies to the statements regarding cookies in Article 4:

### **Cookie Management**

#### **Consent**

When you access the website, a cookie banner is displayed that allows you to accept or reject all cookies or to make your choice by category of cookies according to your prior consent (strictly necessary cookies are enabled by default). As long as you have not given your consent, these cookies are deactivated by default and will not be installed on your end device.

#### **Setting cookies**

You can change your cookie preferences at any time:

**On our site in the cookie banner that can be accessed when you browse the site and/or via the menu item “Cookie settings”, which can be accessed from all subpages.**

When the cookie banner appears on the page, you can make your selection per cookie category. The 'Select' field in the cookie banner leads to a page showing the different categories of cookies used on the website. You can select the purposes for which cookies may be used here.

You can change your selection at any time by clicking on the 'Cookie settings' box on any page of our website.

#### **In your browser**

You can set your browser so that the system prevents the retention of cookies.

Each browser has its own configuration for cookies and cookie selection. You should therefore check the functionalities of the browser you are using to see how you can change your consent to cookie retention in your browser.

To help you configure your browser, you can visit the following help pages, depending on which browser you are using:

- Internet Explorer: <http://windows.microsoft.com/fr-FR/windows-vista/Block-or-allow-cookies>;
- Safari: <https://support.apple.com/fr-fr/safari>;
- Chromium: <http://support.google.com/chrome/bin/answer.py?hl=fr&hlrm=en&answer=95647>;
- Firefox: <https://support.mozilla.org/en-US/kb/block-websites-storing-cookies-site-data-firefox>;
- Opera: <http://help.opera.com/Windows/10.20/fr/cookies.html>

### **How long will your selection be saved?**

Your choice to allow or reject cookies on our website will be saved for 6 months, after which you will be asked again for your consent or selection of authorised cookies.

### **List of third parties that use cookies on our web page**

<b>Third party</b>	<b>Data protection information notice</b>
<b>Essential cookies</b>	
Cloudflare	<a href="https://www.cloudflare.com/en-ca/privacypolicy/">https://www.cloudflare.com/en-ca/privacypolicy/</a>
Riverty	<a href="https://documents.myafterpay.com/consumer-terms-conditions/fr_ch/">https://documents.myafterpay.com/consumer-terms-conditions/fr_ch/</a>
Bambora	<a href="https://www.bambora.com/privacy-policy/">https://www.bambora.com/privacy-policy/</a>
Adyen	<a href="https://www.adyen.com/fr_FR/politiques-et-mentions-legales/privacy-policy">https://www.adyen.com/fr_FR/politiques-et-mentions-legales/privacy-policy</a>
Telecash	<a href="http://www.telecash.info/en/privacy-policy.html">http://www.telecash.info/en/privacy-policy.html</a>
<b>Target group measurement and cookies for analysis purposes</b>	
Google	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>
Hotjar	<a href="https://www.hotjar.com/privacy">https://www.hotjar.com/privacy</a>
<b>Cookies for advertising</b>	
Google	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>
Salesforce.com	<a href="https://www.salesforce.com/fr/company/privacy/">https://www.salesforce.com/fr/company/privacy/</a>

Meta	<a href="https://www.facebook.com/about/privacy/">https://www.facebook.com/about/privacy/</a>
Criteo	<a href="https://www.criteo.com/fr/privacy/">https://www.criteo.com/fr/privacy/</a>
RTB House	<a href="https://www.rtbhouse.com/fr/privacy/">https://www.rtbhouse.com/fr/privacy/</a>
Pinterest	<a href="https://policy.pinterest.com/fr/privacy-policy">https://policy.pinterest.com/fr/privacy-policy</a>
Teads	<a href="https://www.teads.com/privacy-policy/">https://www.teads.com/privacy-policy/</a>
Usercentrics	<a href="https://usercentrics.com/privacy-policy/">https://usercentrics.com/privacy-policy/</a>
TikTok	<a href="https://www.tiktok.com/legal/privacy-policy-eea?lang=fr">https://www.tiktok.com/legal/privacy-policy-eea?lang=fr</a>
Snapchat	<a href="https://snap.com/fr-FR/privacy/privacy-policy">https://snap.com/fr-FR/privacy/privacy-policy</a>
Qualtrics	<a href="https://www.qualtrics.com/privacy-statement/">https://www.qualtrics.com/privacy-statement/</a>

The *Commission Nationale de l'Informatique et des Libertés*, the French data protection authority, (CNIL) has advised that the lifetime of any trackers used must be limited to a duration that allows for a meaningful comparison of audiences over time and must not be automatically extended upon new visits; the information collected through these trackers must be retained for a period not longer than 25 months.

In section A.4 the following shall apply: In case you believe that we have not handled your personal data in accordance with the applicable data protection laws, you also have the right to lodge a complaint with the CNIL. For more information, we invite you to visit the CNIL website: <https://www.cnil.fr/fr>.

In the event of a data breach that could affect your rights, we will notify the data protection authority or you and the data protection authority within 72 hours, as required by law.