Agreement pursuant to Article 26 (1) the General Data Protection Regulation (GDPR)

between

Trusted Shops SE

Subbelrather Str. 15c

50823 Köln (Cologne), Germany

-hereinafter referred to as "**Trusted Shops**"-

and

the **Member** or **User** specified in the Membership or User Agreement.

- hereinafter also referred to individually as "**Party**" and collectively as "**Parties**". The term Member shall hereinafter also mean any user of the Experience Feedback Platform -

§ 1 Subject matter of the agreement

(1) Trusted Shops offers various trust services for companies. In this context, personal data is processed under the joint controllership of the Parties. If Member does not act as a single controller but involves other controllers in the processing activities covered by this agreement, Member shall inform Trusted Shops of these other controllers so that they can join this agreement.
(2) The respective rights and obligations of the Parties under the GDPR, as well as the specified purposes and means of processing, are governed by this Agreement on the Joint Controllership pursuant to Article 26 GDPR (hereinafter referred to as “the Agreement”).

§ 2 - Description of data processing and responsibility

(1) The details of the purpose, nature and scope of the data processing are set out in the agreement in Appendix I and in specific provisions in this Agreement.
(2) The individual processing activities over which there is joint controllership of the Parties are precisely identified and allocated to the respective area of responsibility in Appendix I to this Agreement. Wherever the individual responsibilities are not specifically regulated, for the avoidance of doubt, both Parties will be equally responsible for the respective data processing.

§ 3 - Implementation of data subject rights and information obligations

(1) Data subject enquiries concerning this joint controllership should be directed to Trusted Shops if possible. Notwithstanding this, data subjects may address their enquiries to both parties in order to exercise the data subject rights to which they are entitled.
(2) The Parties are obliged to forward the requests addressed to them to the respective other Party insofar as this is necessary for the proper processing of the enquiry of the person concerned. This does not apply if the forwarding of this information is not permitted under data protection or professional law, in particular because the person concerned explicitly does not wish it to be forwarded. To this end, the Parties shall provide each other with contact addresses and notify each other of any changes in text form. The contact address of Trusted Shops can be found in Appendix I to this Agreement and is accessible at any time under https://www.trustedshops.de/impressum-datenschutz/#kontaktmoeglichkeiten-und-rechte. Both Parties undertake to provide the information to the data subject independently.
(3) The Parties may specify in Appendix I to this Agreement the primary responsibilities for fulfilling the information obligations under Articles 13 and 14 GDPR. Each Party is obliged to implement the information obligations arising from Articles 13 and 14 GDPR and Article 26 (2) GDPR vis-à-vis the data subjects. The Parties shall ensure that this information is accessible via the Internet and provide each other with the Internet addresses at which the respective information can be accessed.

(4) The Parties shall provide, free of charge, the data subject with the necessary data and information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

§ 4 - Erasure requests by data subjects

(1) In the event of erasure requests by data subjects, the Parties shall inform each other thereof. The erasure request has to be complied with in accordance with the requirements of Section 3 of this Agreement, provided that there are no legitimate reasons to oppose the erasure process. Legitimate reasons may, for example, lie in statutory data retention obligations of the respective Party.
(2) The erasure of personal data must be documented by the Parties.
(3) Obligations arising from Article 17 (2) GDPR must be fulfilled independently by the respective Party that has made personal data public. If the Parties have jointly made personal data public on websites operated by Trusted Shops, Trusted Shops is responsible for fulfilling the obligations arising from Article 17(2) GDPR.

§ 5 - Data security and data protection principles

(1) The Parties mutually undertake to comply with the technical and organisational measures required in each case in accordance with Article 32 GDPR, insofar as this relates to the processing of personal data for which there is joint controllership within the meaning of Article 26 GDPR.
(2) The data protection principles laid down in Article 5 GDPR must be complied with by the Parties; in particular, the Parties undertake to process data lawfully within this Agreement.
(3) The Parties agree that both Parties shall take the necessary technical and organisational measures for their respective areas. Trusted Shops' technical and organisational measures can be accessed at any time via the following link: https://help.etrusted.com/hc/en-gb/articles/360021040178.The User is required to adopt technical and organisational measures within its own area of responsibility, and to disclose these to Trusted Shops on request.
(4) In the event of irregularities and errors in the data processing under this Agreement, the Parties shall inform each other and assist each other in rectifying them. This also applies to violations of provisions of this Agreement.

§ 6 - Data protection breaches

(1) In the event of a personal data breach within the meaning of Article 4 No. 12 GDPR (hereinafter referred to as "Data Protection Breaches") under this Agreement, the Parties shall notify each other without undue delay after becoming aware of the Data Protection Breach. The notification has to be made in text form. They shall provide each other with all the information necessary to investigate, remedy and assess the risk of the Data Protection Breach.
(2) Both Parties are responsible for processing and reviewing a Data Protection Breach. They undertake to provide mutual support and to comply with any notification obligations in accordance with Articles 33 and 34 GDPR immediately. The Parties' obligations to cooperate under Paragraph 1 must be within the bounds of what is reasonable and necessary.
(3) Data Protection Breaches and their processing must be documented by the Parties.

§ 7 - Documentation Duties

(1) The Parties undertake to independently comply with the documentation obligations contained in the GDPR. This applies, in particular, to the keeping of the register of processing activities in accordance with Article 30 GDPR. The Parties shall provide each other with the information necessary for the maintenance of the register in an appropriate form.
(2) The Parties shall support each other with regard to all other documentation obligations, in particular, those arising from Articles 32 to 36 GDPR.

§ 8 - Cooperation with data protection supervisory authorities

(1) The Parties undertake to inform each other without undue delay in the event of enquiries from a data protection supervisory authority concerning processing activities covered by this Agreement.
(2) Enquiries from the data protection supervisory authority will be processed jointly by the Parties unless otherwise agreed in individual cases.
(3) Formal enquiries about this Agreement shall – as far as possible – be handled by Trusted Shops. User forwards enquiries to Trusted Shops without being requested to do so, provided that the enquiry is directed to the User.
(4) Necessary information, access and inspection rights shall - within the framework of their statutory powers - be granted to data protection supervisory authorities by the Parties.
(5) This is without prejudice to the Parties' right to seek legal remedy.

§ 9 - Processor

(1) Processors in the sense of Article 4 No. 8 GDPR may be commissioned under this Agreement by each Party without the prior consent of the other Party.
(2) In the event of a commission such as described in Section 9 (1), the commissioning Party shall provide the other Party with all necessary information. The data processing agreement (DPA) must comply with the requirements of Articles 28 and 29 GDPR.
(3) Should a processor be commissioned outside the EU/EEA, the commissioning party shall implement appropriate technical, organisational and contractual measures to ensure that the personal data is processed exclusively within the EU/EEA and, prior to the transfer of personal data to the third country, provide guarantees in accordance with Art. 44 et seq. of the GDPR for an adequate level of data protection to the other party and document this in writing in the contract for the commissioned processing. The other party has the right to object after reviewing the guarantees. In the event of an objection, the parties shall examine whether another appropriate safeguard comes into question. If no other appropriate safeguard comes into question, consent pursuant to Art. 49 (1) a of the GDPR shall be obtained by the user for the transfer of personal data to a third country.
(4) Upon conclusion of a DPA, the concluding Party shall, upon request, provide the respectively other Party with a copy of the DPA.
(5) Trusted Shops publishes the used processors under https://help.etrusted.com/hc/en-gb/articles/360021040178-Technical-and-organisational-measures.

§ 10 - Liability

(1) The Parties are liable for their respective obligations towards the data subject in accordance with the statutory provisions.
(2) With regard to their internal relationship, the liability of the Parties is determined by their respective area of responsibility, without prejudice to the provisions of this Agreement and any other liability distribution agreements of the Parties. Where both Parties are responsible for an area of data processing, liability for damages is determined in accordance with Section 426 of the German Civil Code (BGB) Article 82 (4) and (5) GDPR.

§ 11 - Final Provisions

(1) This Agreement is an integral part of the Main Contract and is effectively concluded upon the conclusion of the Main Contract. Regarding the term and termination of this Agreement, the provisions of the Main Contract apply. Should there be any inconsistencies with regard to data protection provisions between this Agreement and other agreements between the Parties, in particular the Main Contract, the provisions of this Agreement will prevail.
(2) Should any provision of this Agreement be or become invalid or contain loopholes, this will not affect the validity of the remaining provisions. The Parties shall undertake to replace the invalid provision with another, valid provision that comes as close as possible to the purpose of the invalid provision and meets the economic requirements as well as the requirements of data protection law.
(3) German law applies.

Appendix I - Description of the cooperation

Both Parties jointly determine the purposes and means for certain data processing within the context of the Trusted Shops services which constitutes their joint controllership under data protection law in the sense of Article 26 GDPR, at least for certain data processing operations or parts thereof. The following appendix describes the cooperation between the Parties and the distribution of responsibilities between them. Joint controllership is only in place if and to the extent that the Parties have entered into the respective agreements of the main contract required for the described data processing activities, or the described product is used by the User. The Parties are free to process personal data obtained in the context of joint controllership for further purposes of their own, provided that this is permissible under the applicable data protection regulations and the data subjects are informed of this by the respective Party.

Where the User is responsible for information obligations in accordance with Article 13 GDPR within the scope of the data processing activities described below, it must refer to the Trusted Shops privacy policy on an appropriate spot. The privacy policy is available at the following link:
http://www.trustedshops.eu/consumer-membership-terms-eu-en

Trusted Shops also provides additional information in its Help Centre. Among others, it contains a table of responsibilities and competences with the help of which the User can inform the data subjects about the essential contents of this Agreement pursuant to Article 26 (2) GDPR. Furthermore, there are non-binding working aids for the documentation of the balancing of interests mentioned in this Agreement.

The following processing activities are carried out by service providers with whom Trusted Shops has concluded a DPA. Where a third country transfer takes place, Trusted Shops is responsible for providing the appropriate legal framework, i.e. in particular, ensuring the existence of appropriate safeguards in the absence of an adequacy decision or an exemption pursuant to Article 49 GDPR. Trusted Shops will inform the User of any third country transfer that takes place within the scope of the joint controllership, so that the User can comply with information obligations it has towards data subjects.

Trusted Shops carries out monitoring and logging as part of all the listed processing activities to ensure system stability. In some cases, processors, also from the USA and other third countries, are used. The legal basis is Art. 6 para. 1 p. 1 lit. f GDPR. Trusted Shops carries out the necessary balancing of interests and is responsible for all documentation obligations. The user must inform the data subjects about the processing.

In the event that it is necessary to contact Trusted Shops, this should be done by e-mail to privacy@trustedshops.com.

1. Trustbadge and Widgets

1.1 Display of the widget

Data categories: Access data (IP address, time of access, etc.)

Trusted Shops provides various widgets (e.g., the Trustbadge) for the respective online presence of the User, and is solely responsible for their content and the data processing associated with them. The User's information obligations depend on the purpose for which the respective widget is integrated into the User's online presence.

The integration of the widget into the online presence enables the display of authentic customer reviews and, in the case of the Trustbadge, also the collection of customer reviews. The User is responsible for the display of the widget in the online presence. Its integration enables the display of the Trusted Shops Trustmark, the collection of reviews and the display of Trusted Shops services for buyers. The User must provide information on the integration of the Trustbadge in its privacy notices. The responsibility for securing the legal basis for this as well as for all associated information obligations rests with the User. Insofar as User invokes Article 6 (1) (f) GDPR as the legal basis for the data processing, it is responsible for documenting the legal basis and for carrying out the weighing of interests. Insofar as the User invokes Article 6 (1) (a) GDPR as the legal basis, it is responsible for documenting the legal basis and ensuring that it collects users' consent and can prove such consent. Trusted Shops will inform the User in case integrating the Trustbadge entails processing activities for which the data subjects' consent must be obtained, e.g. setting cookies.

When retrieving the Trustbadge, anonymous visitor server log files are stored. The data stored in particular includes the anonymised IP address, date and time of the visit, and the referrer. This serves the purpose of ensuring the proper functioning of the website and recording any unusual occurrences. The legal basis for creating and storing the log files is Article 6 (1) (f) GDPR. The User must provide information about the legal basis; Trusted Shops is responsible for documenting the weighing of interests.

Important information can be found in the following resources:

- Data protection guideline – displaying the Trusted Shops Widgets
- Data protection guideline – Information about cookies
- Data protection guideline - #trstd login integration – eTrusted
- Trustbadge documentation for online retailers

1.2 A/B tests

Data categories: Access data (IP address, time of access, etc.)
Trusted Shops occasionally conducts A/B tests to analyse user behaviour in the User's online presence based on different variants of the widgets. For this purpose, it is necessary to set a cookie or store information in the user's local storage. Trusted Shops will inform the User in good time before the A/B test is carried out. The User has the option to object to the A/B test for its online presence. The parties shall agree on an appropriate legal basis before conducting the A/B test. The User is responsible for informing the user of the legal basis and, if necessary, for obtaining and documenting their consent.

2. Offering the Trusted Shops Buyer Protection services

The processing activities required for offering the Trusted Shops Buyer Protection services partly fall under the joint controllership of Trusted Shops and the User. These processing activities are described in the Agreement. Trusted Shops and the User are separately responsible for processing activities related to the Buyer Protection Services that are not listed in this Agreement unless otherwise specified by the nature of the data processing. In such a case, the Agreement must be amended include such processing. Insofar as joint controllership arises from the nature of the processing, it is subject to this agreement.

2.1 Recognition of registered Trusted Shops Buyer Protection Service customers

Data categories: Hash value of the email address, transaction number, time of order, purchase amount

When integrating the Trustbadge, a hash value of the email address used by a buyer to make a purchase in the User's shop is transmitted to Trusted Shops after the order has been completed in order to check whether the buyer is already registered for the Trusted Shops Buyer Protection Services. Due to the contractual relationship between the Trusted Shops Buyer Protection Service customer and Trusted Shops, this verification is necessary in order to automatically enable the contractual services for orders placed on third-party websites. The hash value is collected through a DIV query. This leads to the Trustbadge accessing information stored in the purchaser's device, so that there is a consent requirement for this access in accordance with the ePrivacy directive and/or the respective local regulation. The user must ensure that consent for this access is obtained in accordance with the locally applicable ePrivacy regulation before any access takes place. Alternatively the user may integrate the Trustbadge in a way which may not require the user's consent due to local regulations. Trusted Shops offers integration options for this purpose. Information on this can be found in the Help Centre in the Data protection guideline – recognition of registered Trusted Shops customers.

The data collected consists of the buyer's order data, and is automatically deleted after verification. Article 6 (1) (f) GDPR constitutes the legal basis for the collection of the order data. The User must inform data subjects of the legal basis, whereas Trusted Shops is responsible for documenting the weighing of interests. Alternatively, the User may choose to base the processing on Article 6 (1) (a) GDPR; in this case, the User is responsible for fulfilling all obligations associated therewith under data protection law.

If the verification process determines that the buyer is already registered for the Buyer Protection Services, the order data necessary for activating the buyer protection for the purchase, i.e. for Trusted Shops fulfilling its contractual obligations under the contract it has with the buyer, is transmitted to Trusted Shops in accordance with Article 6 (1) (b) GDPR. The User shall comply with the information obligations under the GDPR (in particular under Article 13 GDPR). Trusted Shops also confirms the conclusion of the buyer protection by displaying the Trustcard in the checkout and sending an automatic email, and provides further information to the data subject.

2.2 Initial registration for the Buyer Protection Service by clicking on the Trustcard

Data categories: email address, transaction number, time of order, purchase amount, buyer protection product (Basic/Plus)

If the verification process described under Section 2.1 determines that the buyer has not yet registered for the Trusted Shops Buyer Protection Service, the buyer has the possibility to do so via the so-called Trustcard which is integrated into the User's online presence as part of the Trustbadge. By signing up for the Buyer Protection Service, the order data and the email address are transmitted to Trusted Shops for the purpose of setting up the Buyer Protection Account and securing the online purchase. Both the User and Trusted Shops are joint controllers in terms of this data transmission. The transmission of order data for the purpose of registering for the Buyer Protection Services, i.e. for Trusted Shops fulfilling its contractual obligations under the contract with the buyer, is based on Article 6 (1) (b) GDPR. Trusted Shops shall comply with the respective information obligations.

3. Evaluation invitations, evaluation submission and evaluation profile

Insofar as the User uses the Trusted Shops review system within the context of this Agreement, the following provisions apply. The User shall invariably be responsible for fulfilling the information obligations under Article 13 GDPR with regards to the dispatch of review invites.

Trusted Shops may use data transmitted by the user in the context of publishing a submitted rating, provided that there is a legal basis for this. The publication of the (abbreviated) name of a reviewer is based on the terms of use for the Trusted Shops feedback platform pursuant to Art. 6 (1) sentence 1 lit. b GDPR.

3.1. Collection of email addresses and sending of review invites

a) Sending review invites to Trusted Shops Buyer Protection Service customers

Data categories: email address, transaction number, time of order, product purchased (if provided), first name, surname and title (if provided)

Regarding the dispatch of review invites to Trusted Shops Buyer Protection Service customers, Trusted Shops and the User are joint controllers. Provided that the User integrates the Trustbadge, it must inform customers that their order data (email address, order number, order time) will be forwarded to Trusted Shops after placing their order for the purpose of receiving review invites. This is the only way to assign the reviews to a particular order. If the buyer is registered for the Trusted Shops services, the legal basis for this data transfer is the fulfilment of Trusted Shops' contractual obligations under its contract with the buyer in accordance with Article 6 (1) (b) GDPR. The review invites are sent on the basis of the contractual relationship between the Trusted Shops Buyer Protection Service customer and Trusted Shops in accordance with Article 6 (1) (b) GDPR. Trusted Shops is responsible for sending out the review invites, whereas the User may decide on the time of sending.

b) Sending review invites to non-buyer protection customers

Data categories: email address, transaction number, time of order, product purchased (if provided), first name, surname and title (if provided) and further optional data provided by the user

When using the Review Collector, the events API or AutoCollection, review invites are sent to buyers who are not registered for the Trusted Shops Buyer Protection Services. The User and Trusted Shops are joint controllers in terms of the respective data processing. The legal basis for the collection of email addresses and the

sending of review invites is Article 6 (1) (a) GDPR. Collecting the necessary data for the purpose of sending review invites is the responsibility of the User who is solely responsible for obtaining the necessary consent from the data subject, and for all other obligations associated herewith. The User has to particularly inform its customers of the transmission of the necessary order data to Trusted Shops. Insofar as consent is not obtained for such data transmission, the User must ensure that an appropriate legal basis is provided and document it. Trusted Shops is responsible for sending out the review invites, whereas the User may decide on the time of sending.

c) Sending review invites using the Trustcard

Data categories: email address, transaction number, time of order, product purchased (if provided), first name, surname and title (if provided)
In case the User has integrated the Trustbadge but does not offer buyer protection, the buyer may, after checkout, be offered to consent to receiving review invites. If the buyer consents to receiving review invites, Trusted Shops and the User are joint controllers in terms of sending the review invites. Sending of the review invite and obtaining consent is the responsibility of Trusted Shops, whereas the User may co-determine the time of sending. Trusted Shops Buyer Protection Service customers receive the review invite even if the User does not offer Buyer Protection itself. The User's responsibilities correspond with the ones laid down in Subsection a). With regard to the recognition of registered Buyer Protection Service Customers, Clause 2.1 of this Agreement shall apply accordingly.

d) The User sends out review invitations using the Trusted Shops API.

Data categories: email address, transaction number, time of order, product purchased (if provided), first name, name and title (if provided)
By using the API, the User sends out review invites using a unique link that is created by Trusted Shops with the help of the order data submitted by the User. The User is required to ensure the legal basis for the respective data transfer to Trusted Shops, and is responsible for the fulfilment of all information obligations in this context. Trusted Shops carries out the data processing on the basis of Article 6 (1) (f) GDPR.

e) Use of the Reputation Manager

Data categories: As per points a – d of this paragraph

Insofar as it uses the Trusted Shops Reputation Manager to send review invites that contain links referring to third-party platforms, the User shall be responsible for fulfilling the required information obligations vis-à-vis data subjects. The provisions of this Agreement, in particular the ones contained in Subsections a) – d) of this section, additionally apply to the dispatch of review invite that is based on them.

3.2. Review submission

Data categories: Access data (IP address, time of access, etc.), e-mail address, name (if provided), place (if provided), submitted rating (text and stars), transaction number, product purchased (if provided), uploaded photo (if provided)

Trusted Shops is responsible for operating the review platform (in particular, the Control Centre, feedback forms, review forms or other types of forms) on which a data subject submits his/her review. Collecting and publishing the reviews falls under the joint controllership of Trusted Shops the User. Trusted Shops is responsible for providing the legal basis for the data processing and for fulfilling all information obligations in this context. This also concerns other processing activities carried out on the platform, such as tracking. As a general rule, Trusted Shops is solely responsible for tracking. Tracking falls under the joint controllership of Trusted Shops and the User insofar as tracking data is shared with the User. Trusted Shops is responsible for complying with Article 26 (2) GDPR.

Raters have the option of attaching photos to their review. To prevent offensive content or people from being visible on uploaded images, each image is analysed by AWS Rekognition before publication. The legal basis is Article 6 (1) (f) GDPR.

If the User comments on submitted reviews, or contacts the reviewer in any other way, in particular, via the Trusted Shops systems, the User is obliged under this Agreement to ensure that there is a legal basis for its actions. Trusted Shops is entitled to delete comments if the data subject concerned requests erasure and / or the User cannot provide the legal basis.

3.3. Blocklisting of email addresses

Data category: email address

As far as a data subject does not wish to receive review invites, he/she has the possibility to withdraw his/her consent vis-à-vis the User. Such withdrawal of consent only applies to review invites related to the individual User in question. Therefore, it is also possible for the data subject to unsubscribe from all review invitations by clicking on the unsubscribe link in the footer of the review invite emails, or by sending an email to Trusted Shops. Trusted Shops will then put the data subject's email address on a blocklist so that no more review invites - regardless of the User to whom they refer - are sent out. Trusted Shops is solely responsible for the blocklist which, however, has an impact on processing activities that are subject to the joint controllership.

In addition, data subjects can use the unsubscribe link in the footer of the review invite to unsubscribe from further review invites related to the channel (e.g. the shop in which the data subject has made a purchase) for which the review invite was sent.

3.4. Google integration

Data category: Submitted rating (text and stars),

If a member chooses to display collected reviews on their own Google company profile (Google integration), collected reviews are transmitted to the member's Google Merchant Center on a daily basis. Google does not receive any personal data, only the rating text and the associated star rating. However, it is possible that the reviewer publishes personal data in the review text, so that Google receives personal data in these cases. The legal basis for the processing is Art. 6 (1) p. 1 lit. b GDPR as the use of the review text is based on the terms of use.

4. Control Centre

4.1 General functions

Data categories: Access data (IP address, time of access, etc.), e-mail address, name (if provided), place (if provided), submitted rating (text and stars), transaction number, product purchased (if provided).

Trusted Shops provides the User with various information via the Control Centre that is either personal or based on the processing of personal data. This includes, in particular, the analytics data described in Section 3.2 of this Appendix for the sending and receipt of review invites, the management of submitted review in the form of commenting on reviews or reporting reviews, as well as the configuration options for the sending of review invites and the publication time of reviews.

If the User wishes to establish links between the Trusted Shops systems and its own systems or systems managed by the User (in particular, CRM or ticket systems), the User shall be responsible in this respect for all obligations arising from the GDPR within the scope of its joint controllership with Trusted Shops. In particular, it must ensure that all necessary data protection agreements are in place when it makes use of a third-party provider (e.g., for data processing), and that the necessary conditions for personal data transfers to a third country are met.

4.2. Smart Review Assistant

Data categories: submitted rating (text and stars)

Trusted Shops optionally provides the user with an AI-supported system to comment on reviews received. The system analyses the review comment and suggests a reply comment to the user, which the user can then

release for publication. The service provider does not receive any personal data, only the rating text and the associated star rating. However, it is possible that the reviewer publishes personal data in the review text, so that the service provider receives personal data in these cases. The legal basis for the analysis of the rating comment is Art. 6 para. 1 p. 1 lit. f GDPR. The user is obliged to carry out the balancing of interests and to inform the data subjects in accordance with Art. 13 GDPR. Trusted Shops is responsible for the technical implementation and associated obligations arising from the GDPR.

4.3 Sentiment Analysis

Data categories: submitted rating (text and stars)

Trusted Shops optionally provides the user with an AI-supported system to get aggregated qualitative review insights. The service provider does not receive any personal data, only the rating text and the associated star rating. However, it is possible that the reviewer publishes personal data in the review text, so that the service provider receives personal data in these cases. The legal basis for the analysis of the rating comment is Art. 6 (1) lit. f GDPR. The user is obliged to carry out the balancing of interests and to inform the data subjects in accordance with Art. 13 GDPR. Trusted Shops is responsible for the technical implementation and associated obligations arising from the GDPR.

4.4. #trstd Insights

Categories of data: Submitted review (text and star rating)

Trusted Shops optionally provides the user with an AI-based analysis tool that enables the analysis and interpretation of review data at the level of textual content in order to generate insights such as trends, forecasts, or recommendations for action. As a rule, the service provider does not receive any personal data, but only the review text and the star rating. However, it is possible that the reviewer publishes personal data in the review text, so that the service provider receives personal data in these cases. The user is responsible for the accuracy and lawfulness of the data collected and analyzed through #trstd insights. Processing is carried out for the purpose of analyzing review content pursuant to Article 6(1) sentence 1 lit. f GDPR. The user is obliged to independently carry out and document the required balancing of interests for its processing purpose. The user is responsible for informing the data subjects in accordance with Article 13 GDPR. Trusted Shops is responsible for the technical operation of the tool and the associated data protection obligations.

5. Integration of the #trstd Login

Categories of data: Access data (IP address, time of access, etc.);
Registration data (email address, first and last name, profile picture, trstd secret (name, color, date));
where available and enabled: usage data (purchased products, personal characteristics (e.g. age, shoe and clothing size), personal interests (e.g. sports practiced, information about pets), personal preferences (e.g. favorite brand)); address data (name, postal address).

If the user has integrated the #trstd login into its online presence, the following provisions shall apply:

The presentation of the #trstd login in the online presence is the responsibility of the user. The integration enables registration with and login to Trusted Shops. The user is obliged to inform users about the integration of the #trstd login in its data protection notices. The user is responsible for ensuring an appropriate legal basis and for complying with all related information obligations. Where Article 6(1) sentence 1 lit. f GDPR is relied upon as the legal basis, the user is responsible for documenting the legal basis and for carrying out a balancing of interests. Where Article 6(1) sentence 1 lit. a GDPR is used as the legal basis, the user is responsible for documenting the legal basis and for ensuring that consent can be demonstrated.

When accessing the #trstd login, anonymous server log files of website visitors are stored. In particular, storage includes the anonymized IP address, the date and time of the visit, and the referrer. This serves the purpose of ensuring the smooth operation of the website and detecting irregularities. The legal basis for the creation and

storage of the log files is Article 6(1) lit. f GDPR. The user must provide information on the legal basis; Trusted Shops is responsible for documenting the balancing of interests.

The processing of personal data that takes place during and after the login of the data subject is the responsibility of Trusted Shops, including compliance with all requirements of the GDPR. In particular, Trusted Shops is responsible for fulfilling the information obligations towards data subjects and for selecting an appropriate legal basis for the processing.

Due to the continuous expansion of processing activities in connection with the #trstd login, the parties expressly agree that Trusted Shops may, at its own discretion, decide which processing activities are added and which legal basis is selected in each case. The user may review the processing activities at any time by consulting the current data protection notices and may request the necessary documentation from Trusted Shops, such as documented balancing of interests.

Important information can be found in the following resources:

- Data protection guideline – displaying the Trusted Shops Widgets
- Data protection guideline – Information about cookies
- Data protection guideline - #trstd login integration – eTrusted