Appendix to the Trusted Shops membership contract on the processing of personal data by a data processor

between the member designated in the membership contract - responsible party -

- hereinafter referred to as **the Principal**

and **Trusted Shops GmbH, Subbelrather Str. 15C, 50823 Cologne, Germany**- processor -

- hereinafter referred to as the **Contractor**

- collectively referred to hereinafter to as **the Parties**

The Parties have concluded an Agreement for the merchant's membership in Trusted Shops (hereinafter referred to as the **Main Agreement)**, within the scope of which personal data can be processed by the Contractor on behalf of the Principal (**Processing by a Processor,** hereinafter for short: '**Processing**'). This Appendix defines the obligations of the Parties with regard to privacy deriving from the Main Agreement, as described in detail in the Processing. They shall apply to the following activities (not exhaustive) that are covered by the Agreement and by which the Principal's personal data shall be processed by employees or agents of the Contractor (hereinafter referred to as **Data**):

- Graphic representation of Trustbadge as third party content within the framework of the Member's online presence (Logfiles) covered under the Agreement;
- Gathering of e-mail addresses and sending rating reminders by e-mail, provided these are not based on a separate contractual agreement between Trusted Shops and the parties concerned (in particular Trusted Shops membership for buyers); this concerns, in particular, the use of optional "Review Collector", "AutoCollection" and API functions;
- Collection of contact data and other company information (if needed, name, email and postal address, and phone number) when using the Trusted Shops **GDPR Manager**;
- Upload of documents, e.g. Data processing agreements, which are to be connected with the records of processing activities generated via the **GDPR Manager**.

The Appendices to this Appendix can be retrieved at http://support.trustedshops.com/lp/en/legal_order_processing_appendices. Trusted Shops may amend this Appendix and its Appendices by giving notice in writing to Principal. Such amendments will be deemed to be approved by Principal unless Principal objects to the amendments in writing within thirty 30 days following receipt of such notice.

Definitions

For all terms mentioned hereunder, for which Art. 4 General Data Protection Regulation (hereinafter referred to as the **GDPR**) provides a definition, such statutory definition shall also apply to this Agreement.

A Object and duration of the order

A1 The object and duration of the order as well as the type and purpose of processing derive from the Main Agreement, including all Appendices and amendments.

A2 The categories of data to be processed as well as the categories of the data subjects concerned are set out in **Appendix 1** attached hereto.

A3 The term of this Appendix depends on the term of the Main Agreement, notwithstanding any additional obligations under the provisions of this Appendix.

B Obligations of the Contractor

B1.1 The Contractor and any Person under its authority with access to personal data may process Data on data subjects solely within the scope of the Agreement and on the documented instructions of the Principal, unless an exception within the meaning of Article 28(3)(a) of the GDPR is applicable.

B1.2 The Contractor shall inform the Principal immediately if it considers that an instruction violates applicable law. In such a case, the Contractor may suspend implementation of the instruction until confirmed or amended by the Principal.

B1.3 The instructions shall be initially set out in the Main Agreement and can be confirmed subsequently by the Principal in writing or in an electronic format (text form) and must be immediately transmitted to a location designated by the Contractor by way of special verbal instructions.

B1.4 Instructions that go beyond the contractually agreed services shall be treated as a request for a modification of service. Costs arising therefrom shall be borne by the Principal.

B2 The Contractor shall design the in-house organisation in its area of responsibility in such way that the specific data protection requirements are satisfied. It shall meet the technical and organisational measures for adequate protection of the Principal's Data, which satisfy the requirements General Data Protection Regulation (Art. 32 GDPR). The Contractor shall take such technical and organisational measures that ensure the permanent confidentiality, integrity, availability and resilience of the system and services related to the processing.

B2.1 The Contractor shall document the implementation of its technical and organisational measures before the start of processing, especially with regard to the precise execution of the order and submit it to the Principal for review.

B2.2 The documented and agreed technical and organisational measures are attached hereto as **Appendix 2** and are part of this Agreement. The Principal is familiar with these technical and organisational measures and shall be responsible for ensuring an appropriate level of protection for the risks to the data to be processed.

B2.3 The technical and organisational measures underlie technical progress and further development. Insofar as the Contractor is allowed to do so, it shall implement adequate alternative measures. In doing so, the security level must not fall short of the measures set out. Significant changes must be documented.

B3 The Contractor is solely authorised to correct, delete or limit the processing of Data processed by subcontractors in strict observance of the Principal's documented instructions.

B3.1 Excepted from this is the case of a data subject who makes a direct request regarding their rights to the Contractor. In this case the Contractor will contact the Principal to clarify whether the request of the affected party shall be processed by him or the Principal himself. After approval by the Principal, the Contractor is entitled to take all measures necessary to protect the rights of the persons concerned within the scope of his possibilities

B3.2 The Contractor shall provide support to the Principal in processing and responding to requests from data subjects whenever possible with the proper technical and organisational measures. Costs justified in this regard shall be borne by the Principal.

B3.3 Provided they fall within the scope of services, the concept of data deletion, the right to be forgotten, rectification, data portability and information in accordance with the instructions of the Principal must be immediately ensured by the Contractor.

B4 In addition to compliance with the provisions of this assignment, the Contractor shall also ensure compliance with legal obligations pursuant to Art. 28-33 of the GDPR. In this particular regard, it shall ensure compliance with the following conditions:

B4.1 The Contractor shall provide to the Principal the contact details of the in-house data protection officer, insofar as one must be appointed pursuant to Art. 37 of the GDPR. The internal data protection officer exercises his/her activity pursuant to Art. 38 f. of the GDPR.

If the Contractor is not obliged to appoint a data protection officer, it shall designate for the Principal a contact person for matters related to the processing of personal data.

B4.2 To preserve confidentiality during the execution of the tasks pursuant to Art. 28(3), p.2, b, 29, 32(4) of the GDPR, the Contractor shall use solely employees who are bound by an obligation of confidentiality and who have been familiarised beforehand with the relevant provisions on data protection. The Contractor shall ensure that it is prohibited for personnel assigned to the processing of the Principal's Data and other persons acting on behalf of the Contractor to process the Data outside the scope of the instruction.

B4.3 The Contractor shall provide support to the Principal to the extent feasible for satisfying requests by the supervisory authorities or the queries and claims by data subjects pursuant to Chapter III of the GDPR, Art. 82 of the GDPR, as well as for compliance with the obligations set out in Art. 32 to 36 of the GDPR. Costs arising therefrom shall be borne by the Principal unless the Contractor is responsible for the assertion of such claims, inquiries and the occurrence of reporting obligations. Furthermore, the obligation to bear costs does not apply to the provision of information for the fulfilment of transparency obligations.

B4.4 The Contractor shall immediately inform the Principal of any serious disruption to operations or any serious breaches by the Contractor or its personnel of the provisions for the protection of personal data for the Principal's assignment, the specifications hereunder or any other anomalies related to processing of the Principal's Data. It shall take the required measures for securing Data and mitigating possibly more harmful consequences for the parties concerned.

B4.5 The Contractor shall immediately inform the Principal of control procedures and measures by the supervisory authority that are relevant to this assignment. This shall also apply to the extent that a competent authority investigates the Contractor's Processing as part of a regulatory or criminal offence related to the processing of personal data.

B4.6 Insofar as the Principal, for its part, is exposed to inspection by the supervisory authority, for an offence or criminal proceedings, for the liability claim of a data subject or third party or any other claim related to the Contractor's Processing, the Contractor shall support it to the best of its ability. Costs justified in this regard shall be borne by the Principal.

B4.7 The Contractor shall regularly inspect the internal processes as well as the technical and organisational measures to ensure that processing in its area of responsibility is consistent with the current requirements of data protection law and ensuring the protection of the data subject's rights.

C Obligations of the Principal

C1 As part of this Agreement, the Principal shall be solely responsible ("Responsible Party" within the meaning of Art. 4(7) of the DSGVO))for regulatory compliance with the statutory provisions of data protection laws, in particular for the legality of the Data transfer to the Contractor as well as for the legality of the data processing. In particular, the Principal is responsible for effectively obtaining all necessary consents from the concerned parties as part of the execution of the order.

C2 The Principal shall fully and immediately inform the Contractor of any errors or anomalies it detects from job results related to data protection provisions.

C3 The Principal shall provide the Contractor with the name of a contact person for any data protection issues arising under the Agreement.

D Subcontractor

D1 Subcontracting conditions in the context of this regulation means the provision of services by the Contractor to other Contractors commissioned in whole or in part for a service covered by the Agreement.

D1.1 Ancillary services that the Contractor uses e.g. as telecommunication services, post/transport services, maintenance and user service or the disposal of data carriers, as well as other measures aimed at ensuring the confidentiality, availability, integrity and resilience of hardware and software of data processing Appendices, do not belong to this group, unless the Subcontractor can gain access to personal data. In order to ensure the privacy and protection of the Principal's data, the Contractor is also obliged to make the appropriate and legal contractual arrangements regarding ancillary services, even such which do not allow access to personal data and to take control measures.

D2 The Contractor may only commission subcontractors (additional processors) under the following conditions:

D2.1 The Principal agrees to the commissioning of the subcontractor designated in **Appendix 3,** provided that a contractual agreement has been concluded between the Contractor and the Subcontractor for the processing of personal data on behalf of the Contractor, which imposes on this further subcontractor, by means of a contract or other legal instrument under Union law or the law of the Member State concerned, the same data protection obligations as those laid down in this Agreement or other legal instrument between the controller and the processor in accordance with Article 28 (3) GDPR.

D2.2 Outsourcing to other subcontractors or changing the existing subcontractor is allowed, provided that:

- the Contractor shall notify the Principal of such outsourcing to subcontractors in writing or electronically with 30 days' prior notice.
- the Principal raises no objection in writing or electronically against the planned outsourcing until the moment of transfer of data to the Contractor; **and**
- a contractual agreement is prepared pursuant to Art. 28 Para. 2-4 of the DSGVO.

D2.3 If no objection is raised within the time limit, consent to modify shall be deemed granted. Where an objection is raised and it proves impossible to find an amicable solution between the Parties, the Parties shall grant an exceptional

right to termination with regard to the Main Agreement, until the time of transfer of the data to Subcontractor.

D2.4 The transmission of the Principal's personal data to the subcontractor and when it first takes action, are only allowed if all subcontracting conditions are met.

D3 If the Subcontractor performs the agreed services outside of the European Union/ European Economic Areas, the requirements of Section E shall also apply. The same shall also apply if service providers must be used pursuant to para. D1.1(2).

E Processing location

E1 The Contractor shall gather, process or use Data exclusively in a Member State of the European Union or of another State party to the European Economic Area Treaty.

E2 In special cases, the Contractor may derogate therefrom, provided the Contractor has ensured the permission to transmit to third countries under data protection law by the measures set out in Art. 44 et seq. of the DSGVO. Paragraphs D2.1and D2.2 shall apply mutatis mutandis.

F The Principal's monitoring rights

F1 The Contractor shall prove, by appropriate means compliance with the obligations set out hereunder, to the Principal.

F2 Proof of such measures that do not solely concern a definite order can be provided at the Contractors' discretion by:

F2.1 conducting a self-assessment;

F2.2 intragroup rules of conduct including external certification of compliance;

F2.3 compliance with authorised rules of conduct pursuant to Art. 40 of the DSGVO;

F2.4 certification in accordance with an approved certification process pursuant to Art. 42 of the DSGVO;

F2.5 current certificates, reports or report extracts from independent bodies (e.g. auditors, data protection officers, IT Security Department, revision, data protection auditors, quality auditors);

F2.6 an appropriate certification by means of an IT data security or privacy audit (e.g. according to the Federal Office for Information Security - Basic level of security (*BSI-Grundschutz*).

F3 If, in individual cases, inspections by Principal or an inspector commissioned by Principal should be necessary, because the proof specified in paragraphs F1and F2 is not sufficient, inspections shall be carried out during normal business hours without disrupting the course of operations after registration, taking into account a reasonable notice time. If the inspector commissioned by Principal is in a competitive relationship with Contractor, Contractor has a right of objection against this.

G The deletion and return of personal data

G1 Data copies or duplicates shall not be created without the Principal's knowledge. Exceptions are backups required for ensuring proper data processing and Data required for compliance with statutory obligations.

G2 Following completion of the contractually agreed work or earlier if so requested by the Principal – and no later than termination of the performance agreement – the Contractor shall return all documents, processing and user results compiled as well as Data files related to the contractual relationship in its possession, and hand them over to the Principal or destroy them according to the latter's choice, pursuant to data protection provisions, provided there is no storage obligation for personal data according to European Union law or the applicable law of the relevant Member State. The same shall apply for test and waste material. The deletion log must be presented upon request.

G3 The data records transmitted for the dispatch of review invites will be deleted 3 months after dispatch of the respective invite.

G4 Documentation intended for substantiating the order and for proper data processing, must be kept by the Contractor in accordance with the retention periods, beyond the term of the Agreement indicated. It can discharge itself of its liabilities by handing such documentation over to the Principal at the end of the Agreement.

G5 Any additional costs arising as a result of the Principal's deviating requirements for the issuing or deletion of the data shall be borne by the Principal.

H Liability and damages

The Principal and the Contractor shall also be liable vis-à vis data subjects insofar as there is a deviation from the agreed liability regulations in the Main Agreement - in accordance with the rules set out in Art. 82 of the DSGVO.

I Information requirements, written form and governing law

I1 Should the Principal's data with the Contractor be at risk of seizure or confiscation, insolvency or by other events or third party measures, the Contractor shall immediately inform the Principal thereof. the Contractor shall immediately inform all Responsible Parties in this regard thereof that the control and ownership of the Data lie exclusively with the Principal as "Responsible Party", pursuant to the General Data Protection Regulation.

I2 Modifications and amendments to this Appendix and all of its components – including any the Contractor warranties – must be agreed in writing. They may also be made in an electronic format (text form), with the express indication thereon that it is a change or amendment to these conditions. This shall also apply for the waiver to this form requirement.

I3 The regulations of this Appendix on data protection shall prevail over regulations of the Main Agreement in the event of any discrepancies in this regard.