Annexe au Contrat d'adhésion à Trusted Shops

Accord concernant la sous-traitance du traitement de données à caractère personnel au sens de l'article 28 du Règlement général sur la protection des données (RGPD)

Entre le membre désigné dans le Contrat d'adhésion

- Responsable de traitement au sens de l'article 4 du RGPD -

- ci-après dénommé **Responsable**, d'une part -

et la société **Trusted Shops GmbH, Subbelrather Str. 15C, 50823 Cologne, Allemagne**

- Sous-traitant au sens de l'article 28 du RGPD -

- ci-après dénommée **Sous-traitant**, d'autre part -

- ci-après conjointement dénommés **les Parties** -

Les Parties ont conclu un contrat fixant les conditions d'adhésion du commerçant à Trusted Shops (ci-après **Contrat principal**) et prévoyant la possibilité pour le Sous-traitant de traiter des données à caractère personnel pour le compte du Responsable (**Traitement en sous-traitance** au sens de l'article 28 du Règlement général sur la protection des données). La présente Annexe précise les obligations des Parties en matière de protection des données, telles qu'elles résultent des activités de traitement en sous-traitance décrites en détail dans le Contrat principal. Elle s'applique aux activités en lien avec le contrat et pour lesquelles des employés du Sous-traitant ou bien des sous-traitants qu'il a lui-même engagés sont amenés à traiter des données à caractère personnel (ci-après **Données**) du Responsable, à savoir les activités énumérées, de façon limitative, ci-après :

- Représentation graphique du Trustbadge, un contenu tiers inséré dans le site Internet objet du contrat d'adhésion du Membre (fichiers log) ;
- Collecte d'adresses e-mail et envoi d'e-mails d'invitations à émettre un avis, dans la mesure où ces opérations ne procèdent pas de contrats spécifiques conclus entre Trusted Shops et la personne concernée (en particulier par l'adhésion de celle-ci à Trusted Shops à titre d'acheteur) ; cela concerne en particulier l'utilisation des fonctionnalités optionnelles « collecteur d'avis », « AutoCollection » et l'API.
- Collecte des données de contact (le cas échéant nom, adresse électronique, adresse postale et numéro de téléphone) en cas d'utilisation de la « Protection des données 360 ».

Les appendices à la présente Annexe peuvent être consultés à l'adresse http://support.trustedshops.com/lp/en/legal_order_processing_appendices. Le Membre sera informé de tout changement apporté aux appendices –y compris les changements concernant les sous-traitants ultérieurs– et à la présente annexe de la manière décrite dans la section A8 du Contrat principal.

Définitions

Tous les termes définis à l'article 4 du Règlement général sur la protection des données (ci-après **RGPD**) sont employés dans le présent contrat au sens de cette définition légale.

A Objet et durée de la sous-traitance

A1 L'objet et la durée de la sous-traitance, ainsi que la nature et la finalité du traitement des Données, sont ceux spécifiés dans le Contrat principal et dans tous ses compléments et annexes.

A2 Les Données objets du traitement ainsi que les catégories de personnes concernées sont précisées dans l'**Appendice 1** au présent accord.

A3 La durée de vie de la présente Annexe est la même que celle du Contrat principal, sauf stipulations prévoyant des obligations de plus longue durée dans la présente Annexe.

B Obligations du Sous-traitant

B1 Le Sous-traitant et toute personne placée sous son autorité ayant accès aux données à caractère personnel ne doivent traiter les données des personnes concernées que dans le strict cadre de la sous-traitance et des instructions documentées qu'ils ont reçus du Responsable, à moins que ne se présente l'exception prévue à l'article 28, paragraphe 3, a) du RGPD.

B1.1 Le Sous-traitant informe sans délai le Responsable dès qu'il juge qu'une instruction reçue constitue une violation des lois applicables. Dans ce cas, le Sous-traitant est autorisé à suspendre l'application de l'instruction jusqu'à ce que le Responsable lui en donne confirmation ou en modifie la formulation.

B1.2 Les instructions sont initialement fixées dans le Contrat principal. Elles peuvent être modifiées par la suite sous forme écrite ou sous forme électronique (forme textuelle) en les communiquant à l'adresse du service indiquée par le Sous-traitant. Les changements communiqués oralement doivent être immédiatement confirmés sous une forme écrite ou textuelle.

B1.3 Les instructions dépassant le cadre de la prestation contractuellement prévue sont traitées comme une demande de modification des prestations à fournir. Les coûts résultant de cette demande sont à la charge du Responsable.

B2 Le Sous-traitant doit disposer d'une organisation interne dans son domaine de compétence qui satisfasse aux exigences spécifiques de la protection des données. Il doit

mettre en œuvre les mesures techniques et organisationnelles protégeant de façon appropriée les Données du Responsable et respectant les exigences du Règlement général sur la protection des données (art. 32 RGPD). Il doit mettre en œuvre les mesures techniques et organisationnelles qui garantissent la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

B2.1 Avant le début du traitement, le Sous-traitant doit établir et soumettre à l'examen du Responsable une documentation détaillant les moyens de mise en œuvre de ses mesures techniques et organisationnelles, en particulier en ce qui concerne l'exécution concrète de la sous-traitance.

B2.2 Les mesures techniques et organisationnelles convenues par les Parties sont jointes en **Appendice 2** et font partie intégrante du présent contrat. Le Responsable a pris connaissance de ces mesures techniques et organisationnelles et estime sous sa seule responsabilité qu'elles offrent un niveau de protection adapté aux risques que présentent les Données à traiter.

B2.3 Les mesures techniques et organisationnelles évoluent au rythme des progrès techniques et des efforts de perfectionnement continu. À cet égard, le Sous-traitant est autorisé à mettre en œuvre d'autres mesures adéquates, tant que le niveau de sécurité qu'elles offrent n'est pas inférieur aux mesures convenues. Toutes les modifications substantielles doivent être documentées.

B3 Le Sous-traitant n'est autorisé à effectuer de sa propre initiative aucune opération de rectification, de suppression ou de limitation des possibilités de traitement sur les Données faisant l'objet de la sous-traitance; toute opération de cette nature doit suivre une instruction documentée du Responsable.

B3.1 Font exception au paragraphe précédent les cas où une personne concernée s'adresse directement au Sous-traitant pour faire valoir ses droits. Dans ce cas, le Sous-traitant contacte le Responsable pour savoir qui, du Responsable ou du Sous-traitant, prend en charge la demande de la personne concernée relative à l'exercice de ses droits. Suite à une autorisation de prise en charge par le Responsable, le Sous-traitant est en droit de prendre toutes les mesures nécessaires afin de préserver les droits des personnes concernées dans la mesure de ses capacités.

B3.2 Le Sous-traitant doit assister le Responsable dans l'examen des demandes des personnes concernées et dans les réponses à y apporter, autant qu'il lui est possible, et met en œuvre à cette fin des mesures techniques et organisationnelles appropriées. Les coûts que cette assistance justifie sont à la charge du Responsable.

B3.3 Si ces tâches sont incluses dans son champ de prestations, le Sous-traitant est tenu de garantir lui-même directement, sur la base d'instructions documentées du Responsable, un plan de suppression des Données, le respect du droit à l'oubli, ainsi que les droits à la rectification, à la portabilité et à la communication des Données.

B4 Outre les règles stipulées par la sous-traitance, le Sous-traitant doit également respecter les obligations légales prévues aux articles 28 à 33 du RGPD. Il garantit notamment dans ce cadre qu'il satisfait aux exigences suivantes :

B4.1 Le Sous-traitant communique au Responsable les coordonnées du délégué à la protection des données de son entreprise, dans la mesure où il est tenu d'en désigner un selon les termes de l'article 37 du RGPD. Le délégué à la protection des données exerce sa mission en conformité avec les articles 38 et suivants du RGPD.

Si le Sous-traitant n'est pas tenu de désigner un délégué à la protection des données, il indique au Responsable un interlocuteur auquel s'adresser pour toutes les affaires en lien avec le traitement des données à caractère personnel.

B4.2 Afin de préserver la confidentialité prévue à l'article 28, paragraphe 3, b), à l'article 29 et à l'article 32, paragraphe 4 du RGPD, le Sous-traitant n'exécute ses missions que par l'intermédiaire d'employés qui se sont engagés à respecter ces règles de confidentialité et ont préalablement été formés sur les règles de protection des données à observer dans le cadre de leur travail. Le Sous-traitant garantit que les employés en charge du traitement des Données et toutes les autres personnes travaillant à son service ont connaissance de l'interdiction de traiter les Données différemment des instructions reçues.

B4.3 Le Sous-traitant prête assistance au Responsable, dans la mesure de ses possibilités, afin que ce dernier puisse satisfaire les demandes des autorités de contrôle ou les demandes de personnes concernées et les droits que celles-ci feraient valoir, conformément au chapitre III et à l'article 82 du RGPD. Il l'assiste de même dans le respect des obligations prévues aux articles 32 à 36 du RGPD. Les coûts que cette assistance justifie sont à la charge du Responsable, à moins que le Sous-traitant ne soit responsable de la survenance de l'exercice de droits, de demandes et de la survenance d'obligations de déclarations. En outre, l'obligation de supporter les coûts ne s'applique pas à la mise à disposition d'informations destinée à remplir les obligations de transparence.

B4.4 Le Sous-traitant notifie immédiatement au Responsable la survenance des cas suivants : de graves dysfonctionnements opérationnels affectent l'entreprise ; le Sous-traitant ou des personnes qu'il emploie dans le cadre de la sous-traitance ont gravement enfreint des règles de protection des données à caractère personnel du Responsable ou des règles stipulées dans le présent accord ; ou bien en cas d'irrégularité en relation avec le traitement des Données du Responsable. Il prend les mesures nécessaires pour sécuriser les Données et pour limiter les préjudices qui en résultent éventuellement pour les personnes concernées.

B4.5 Le Sous-traitant informe immédiatement le Responsable des opérations de vérification et des décisions des autorités de contrôle lorsqu'elles sont en rapport avec la présente sous-traitance. Cette obligation d'information s'applique également aux cas où une autorité compétente conduirait une enquête visant le Sous-traitant dans le cadre d'une procédure administrative ou pénale portant sur le traitement en sous-traitance des données à caractère personnel.

B4.6 Si inversement le Responsable est visé par un examen des autorités de contrôle, une procédure administrative ou pénale, une mise en cause de sa responsabilité par une personne concernée ou un tiers, ou bien par toute autre revendication en lien avec le traitement confié en sous-traitance au Sous-traitant, celui-ci est alors tenu de l'assister au mieux de ses capacités. Les coûts que cette assistance justifie sont à la charge du Responsable.

B4.7 Le Sous-traitant vérifie régulièrement ses procédures internes ainsi que les mesures techniques et organisationnelles, afin de garantir que le traitement dont il a la charge est conforme aux exigences du droit de la protection des données en vigueur et qu'il préserve les droits des personnes concernées.

C Obligations du Responsable

C1 Dans le cadre du présent contrat, le Responsable est seul responsable du respect des dispositions légales en matière de protection des données, en particulier de la licéité du transfert des données au Sous-traitant, ainsi que de la licéité du traitement des Données (il est le « responsable du traitement » au sens de l'article 4, point 7 du RGPD). En particulier, il est responsable du recueil en bonne et due forme de tous les consentements nécessaires auprès des personnes concernées dans le cadre de l'exécution de la sous-traitance.

C2 Le Responsable informe immédiatement et exhaustivement le Sous-traitant lorsqu'il constate que des erreurs ou des irrégularités sont commises au regard des dispositions relatives à la protection des données.

C3 Le Responsable indique au Sous-traitant l'interlocuteur chargé de répondre à toutes les questions concernant la protection des données qui peuvent naître dans le cadre du présent contrat.

D Sous-traitants ultérieurs

D1 On entend par relations de sous-traitance ultérieure au sens du présent contrat les accords de prestations de service par lesquels le Sous-traitant confie à d'autres sous-traitants tout ou partie des prestations prévues dans le présent contrat.

D1.1 En sont exclues les prestations que le Sous-traitant prend en charge à titre accessoire, par ex. les services de

télécommunication, d'expédition ou transport, de maintenance et d'assistance utilisateurs, ou l'élimination des supports de données, ainsi que toute autre action visant à assurer la confidentialité, l'intégrité et la résilience des composants matériels et logiciels des équipements informatiques，sauf si le sous-traitant ultérieur peut, à cette occasion, avoir accès à des données à caractère personnel. Afin de garantir la protection et la sécurité des Données du Responsable, le Sous-traitant est néanmoins également tenu, dans le cas d'externalisation de ces prestations accessoires, et ce, même dans les cas où il n'y a pas d'accès aux données personnelles, de stipuler des clauses contractuelles licites et appropriées, et de mettre en place des mesures de contrôle.

D2 Le Sous-traitant n'est autorisé à confier une activité à des sous-traitants ultérieurs qu'après en avoir expressément reçu l'accord du Responsable sous forme écrite ou documentée.

D2.1 Le Responsable approuve la sous-traitance confiée aux sous-traitants ultérieurs nommés en **Appendice 3** à la condition qu'un accord ait été conclu entre le Sous-traitant et les sous-traitants ultérieurs quant à la sous-traitance du traitement de données à caractère personnel, au moyen d'un contrat ou d'un autre instrument juridique imposant à ce sous-traitant supplémentaire, conformément au droit de l'Union ou de l'État membre concerné, les mêmes obligations en matière de protection des données que celles prévues dans le contrat ou autre instrument juridique conclu entre le responsable du traitement et le sous-traitant en vertu de l'article 28, paragraphe 3 du RGPD.

D2.2 Une externalisation d'activités vers de nouveaux sous-traitants ultérieurs ou tout changement apporté à la liste actuelle des sous-traitants ultérieurs ne sont admissibles que si les conditions suivantes sont réunies :

- le Sous-traitant notifie cette externalisation au Responsable au moins 30 jours à l'avance, sous forme écrite ou textuelle,
- jusqu'à la date de transfert des Données, le Responsable n'émet pas d'objections auprès du Sous-traitant, sous forme écrite ou textuelle, concernant l'externalisation prévue, **et**
- l'externalisation est régie par un contrat satisfaisant aux exigences de l'article 28, paragraphes 2-4 du RGPD. Le paragraphe D2.1 s'applique également.

D2.3 S'il n'émet aucune objection dans le délai mentionné ci-dessus, le Responsable est réputé donner son accord. S'il émet une objection et que les Parties ne parviennent pas à résoudre de manière consensuelle ce différend, elles peuvent exercer, jusqu'à la date de transfert des Données au sous-traitant ultérieur, un droit de résiliation extraordinaire affectant la totalité du Contrat principal.

D2.4 Le transfert des données à caractère personnel du Responsable au sous-traitant ultérieur et l'entrée en opération de celui-ci ne sont autorisés que lorsque toutes les conditions pour la sous-traitance ultérieure sont réunies.

D3 Si le sous-traitant ultérieur exécute la prestation convenue à l'extérieur de l'Union européenne / de l'Espace économique européen, il est en outre soumis aux exigences de la section E. Celles-ci s'appliquent également si des prestataires doivent intervenir aux termes du paragraphe D1.1.

E Lieu du traitement

E1 Le Sous-traitant collecte, traite ou utilise des Données exclusivement dans un État membre de l'Union européenne ou dans un autre État partie à l'accord sur l'Espace économique européen.

E2 Dans certains cas particuliers et à condition qu'il ait garanti la licéité, au regard des dispositions sur la protection des données, du transfert des Données vers les pays tiers concernés en mettant en œuvre des mesures adaptées conformes aux articles 44 et suivants du RGPD, le Sous-traitant peut déroger à la règle du paragraphe précédent,. Les paragraphes D2.1 et D2.2 s'appliquent également.

F Droits de contrôle du Responsable

F1 Le Sous-traitant apporte la preuve au Responsable, par des moyens appropriés, qu'il respecte bien les obligations définies par le présent accord.

F2 Pour prouver la conformité des mesures qui ne concernent pas exclusivement cette sous-traitance, le Sous-traitant peut, à son libre choix, recourir à l'un des moyens suivants :

F2.1 la réalisation d'un audit interne ;

F2.2 la présentation des règles de conduite internes à l'entreprise, assorties d'une vérification externe du respect de ces règles;

F2.3 le respect d'un code de conduite approuvé conformément à l'article 40 du RGPD ;

F2.4 la certification selon une procédure de certification approuvée conformément à l'article 42 du RGPD ;

F2.5 des attestations, rapports ou extraits de rapports sur la situation actuelle, établis par des instances indépendantes (par exemple commissaire aux comptes, délégué à la protection des données, département de sécurité informatique, auditeur, auditeur de conformité de la protection des données, auditeur qualité) ;

F2.6 une certification adaptée délivrée après un audit de sécurité informatique ou un audit de conformité de la protection des données (par ex. selon les critères de la protection de base définie par le BSI [Office fédéral allemand pour la sécurité des technologies de l'information].

F3 Dans l'éventualité où il serait nécessaire pour le Responsable, dans un cas concret, de procéder à des inspections, parce que les preuves spécifiées aux paragraphes F1 et F2 ne sont pas suffisantes, ou d'avoir recours pour ce faire à un examinateur choisi par lui, celles-ci ont lieu durant les heures de bureau habituelles sans perturbation des activités de l'entreprise, après annonce et maintien d'un délai de préparation raisonnable. Le Sous-traitant dispose d'un droit d'opposition à l'encontre d'un examinateur choisi par le Responsable si celui-ci se trouve dans un rapport de concurrence avec le Sous-traitant.

G Suppression et restitution de données personnelles

G1 Aucune copie ou double ne doit être fait à l'insu du Responsable. Font exception à cette règle les copies de sécurité, si elles sont nécessaires pour garantir la conformité du traitement des données, ainsi que les copies de données que la législation sur la conservation des données oblige à conserver.

G2 Une fois achevées les tâches prévues contractuellement, ou à tout moment sur simple demande du Responsable, et au plus tard à la date de fin de validité du contrat de prestation, le Sous-traitant est tenu soit de remettre au Responsable l'intégralité des documents entrés en sa possession, les résultats produits par le traitement et l'utilisation des Données, ainsi que les jeux de données en lien avec la sous-traitance, soit de les détruire conformément aux règles de protection des données, dans la mesure où le droit de l'Union ou un droit applicable dans les États membres ne prévoit pas une obligation de sauvegarde des données à caractère personnel. La phrase précédente s'applique également à toutes les informations de test ou toutes les traces d'informations, quelle que soit leur forme. Les procès-verbaux des opérations de suppression doivent être présentés au Responsable à sa demande.

G3 Les ensembles de données transmis pour l'envoi d'invitations à émettre un avis sont effacés trois (3) mois après l'envoi de l'invitation correspondante.

G4 Les documents attestant de la conformité du traitement des Données à la réglementation et à la sous-traitance sont à conserver par le Sous-traitant au-delà de la fin du contrat, conformément aux délais de conservation respectifs. Il a également la possibilité de les remettre au Responsable à la fin du contrat et de se dégager ainsi de son obligation de conservation.

H Lorsque des frais supplémentaires sont occasionnés par des spécifications divergentes du Responsable concernant la restitution ou l'effacement des Données, ceux-ci sont à la charge du Responsable. **Responsabilité et dommages-intérêts**

Le Responsable et le Sous-traitant engagent leur responsabilité vis-à-vis des personnes concernées aux termes de l'article 82 du RGPD. Cela vaut y compris lorsque

les dispositions de cet article 82 diffèrent des règles de responsabilité stipulées dans le Contrat principal.

I Obligations d'information, forme écrite et choix du droit applicable

I1 Si les Données du Responsable sont menacées du fait d'une saisie, d'une procédure de confiscation, d'insolvabilité ou de conciliation judiciaire, ou de tout autre événement ou action de tiers, le Sous-traitant le notifie sans délai au Responsable. Le Sous-traitant informe sans délai les responsables des parties concernées que le Responsable est seul titulaire de droits à l'égard de ces Données, à titre de « responsable du traitement » au sens du Règlement général sur la protection des données.

I2 Toute modification et tout complément apporté à la présente Annexe et à une quelconque de ses composantes, y compris toute garantie donnée par le Sous-traitant, nécessitent une convention écrite, qui peut également prendre une forme électronique (forme textuelle), précisant expressément qu'il s'agit d'une modification ou d'un complément aux présentes conditions. La même exigence s'applique à une éventuelle renonciation à ces conditions de forme.

I3 En cas de contradiction, les clauses de la présente Annexe relative à la protection des données prévalent sur celles du Contrat principal.