AGREEMENT ON DATA PROTECTION

for use of an

Affiliate Marketing Platform

Between

Advertiser

and

WEBGAINS GMBH

("**WBG**")

(each individually "**Party**" and together, "**Parties**").

BACKGROUND

(A) WBG operates an Affiliate Marketing Platform. Advertisers can use this platform to provide the relevant advertising material for the marketing of their offers / services by publishers. For participation in the Affiliate Marketing Program of WBG, it is necessary that these advertising materials are equipped with a tracking code provided by WBG for the Advertiser. This is the only way to ensure that the service provision of WBG can be implemented technically for the Advertisers.

(B) Advertisers can search from the registered Publishers who are supposed to take over marketing of the advertising materials provided for them on their sales channels. The sales brokered for the Advertisers by the Publishers are recorded and processed with the Affiliate Marketing Platform provided by WBG. In addition, WBG provides a corresponding reporting for Advertisers and indicates which remuneration to pay to the Publisher for the brokerage activity or WBG for the use of the platform.

(C) WBG maintains contractual relationships both to the Publisher and to the Advertiser. The provision of WBG services requires the transmission of Personal Data to WBG and its processing, so that WBG can fulfil its own legal obligations. This includes the settlement of the brokerage activities of the Publishers as well as the settlement against the Advertiser for the use of the platform and the further calculation of the Publisher remuneration. In addition, the transmission of data to WBG is required for the development of services and functions as well as to prevent misuse or fraud.

(D) The details of the respective processing activities are described in more detail in **Part A** and **Part B** of this Agreement. **Part C** contains the template of the Joint Controller Agreement, which applies between the Advertiser and Publisher if the Publisher uses the advertising material provided by the Advertiser. With the provision of advertising material on the Affiliate Marketing Platform, the Advertiser offers to conclude the Joint Controller Agreement (in accordance with Part C), which is accepted by the Publisher when selecting the advertising materials.

(E) This Agreement shall ensure appropriate protection of Personal Data in the course of the transmission and processing of Personal Data within the framework of the applicable data protection laws. In addition, the Parties would like to implement appropriate measures with regard to the protection of privacy and the fundamental rights and freedoms of the Data Subjects.

Against this backdrop, the Parties make the following agreement:

1. DEFINITIONS

1.1 In this Agreement, the following terms have the following meanings:

(a) "**Personal Data**", "**Controller**", "**Processor**", "**Processing**", "**Data Subject**", **"Additional Processors"** (= "**Subprocessor or Sub-Service Provider**"), "**Technical and Organisational Measures**" and "**Supervisory Authority**" have the same meaning as in the GDPR.

(b) "**Country with an appropriate level of protection**" is every country outside the EEA for which the European Commission has decided that the country has an appropriate level of data protection due to its laws or international agreements into which it has entered.

(c) "**General Terms and Conditions of Business**" or "**GTC**" are the *General Terms and Conditions of Business* that are provided by WBG for the Advertiser, including all related agreements, conditions or other orders by which the use of the platform is regulated.

(d) "**Agreement**" means this agreement on data protection.

(e) "**Regulations**" refers to the regulations for processing and the joint controller regulations, (see below).

(f) "**Regulations for processing**" or "RFP" refers to the regulations in **Part A**.

(g) "**WBG**" refers to Webgains GmbH, Frankenstrasse 150C, D90461 Nuremberg, Germany, VAT DE 328967883, Companies House Nuremberg HRB no.371980 (hereinafter referred to as "WBG" or "service provider")

(h) "**Joint Controller Agreement**" is made up of the regulations in **Part B and Part C**. The Joint Controller Agreements regulate the transmission and processing of Personal Data between WBG and the Advertiser (**Part B**) and the relevant interactions between the Advertiser and Publisher(s) in regard to the data protection law according to Art. 26 GDPR (**Part C**). The respective regulations apply irrespective of whether the Parties actually are considered as a Joint Controller within the meaning of Art. 26 GDPR and shall ensure an appropriate protection of the transmission and processing of Personal Data regardless of this question.

(i) "**Processing**" is the processing of Personal Data on behalf of the Controller within the meaning of Art. 28 GDPR. The Advertiser acts as Controller and WBG as Processor.

(j) "**Advertiser**" includes all companies that use the Affiliate Marketing Services of WBG on the basis of the GTC or similar contractual agreements.

(l) "**Publishers**" are all natural persons or legal entities who have registered on the WBG platform on the basis of the General Terms and Conditions and promote the advertising material provided by a Advertiser in their media offers/sales channels.

(m) "**GDPR**" is the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 for the protection of natural persons in the processing of Personal Data and on the free movement of data and the repealing of Directive 95/46/EC (General Data Protection Regulation).

(n) "**Joint Controller**" means the processing of Personal Data by several (joint) Controllers who jointly define the purpose and means of processing (see Article 26 GDPR).

(o) **"Member State**" is a member state of the EU or a contractual state of the EEA.

(p) "**Affiliate Marketing Services**" or "**Services**" includes the services described or referred to in the General Terms and Conditions, including the provision of the Affiliate Marketing Platform by WBG that allows Advertisers to control Affiliate Marketing processes. In addition to the recording of sales by Publishers, this also includes corresponding reporting.

1.2 The following conditions apply to this Agreement:

(a) References to a statutory regulation include all subordinated legal provisions which are issued based on this provision;

(b) References to this Agreement include the parts (currently A, B, and C) and their Appendices;

(c) Headings are not to be included in the interpretation of this Agreement; and

(d) In the case of a conflict or contradictions within this Agreement, the conflict or inconsistency is resolved by the respective priority clauses.

2. SCOPE

2.1 The regulations for processing (Part A) and the Joint Controller Agreement (Part B) shall apply between the Parties in respect to their roles as Controller or Processor in relation to the Personal Data, which is transmitted and processed in accordance with the provisions in Part A or B. The respective processes and which Party is responsible within the framework of which processes for individual data processing are explained in more detail in Part A and Part B.

2.2 Each Party, depending on the process, can act in the role of a Controller, Joint Controller or Processor, whereby in the initial processes of this Agreement, only WBG acts also as a Processor in the sense of Art. 28 GDPR and Advertiser acts as Customer.

2.3 When commissioning Publishers via the WBG Affiliate Marketing Platform, the Advertiser concludes a separate agreement on Joint Control in accordance with Art. 26 GDPR (in accordance with Part C Joint Controller Agreement) with the respective Publisher(s). WBG agrees with the Publishers registered on the Affiliate Marketing Platform, to a corresponding obligation to conclude the Joint Controller Agreement (Part C) upon acceptance of an order. According to the common understanding of the Parties, the agreement of a Joint Controller Agreement (Part C) does not lead to the creation of a civil-law contractual relationship between the Advertiser and the Publisher. The Parties agree that the Advertiser (and Publisher) rights regarding the use of Affiliate Marketing Services are asserted exclusively within the framework of the contractual relationship with WBG.

2.4 Each party in its role as Processor or Controller, if applicable, shall obligate integrated Sub-Processors (including "subcontractors") to a protection level at least comparable to the respective regulations, and ensures that Sub-Processors comply with adequate security and data protection requirements before a corresponding agreement is carried out with a Sub-Processor.

2.5 In order to ensure an adequate level of protection in connection with the transmission and processing of Personal Data, the principles contained in Part B apply for any processing and transmission between the Controllers for the processing.

3. COMPLIANCE WITH THE CONTRACTUAL REGULATIONS

3.1 The Parties agree to comply with the obligations that are imposed on them in their role as a Controller and/or Processor within the framework of this Agreement.

3.2 Each Party is entitled to assert the claims of this Agreement towards the other Party to the extent that the other party operates in the corresponding role.

4. AMENDMENTS

4.1 The Parties agree that this Agreement can be amended and/or supplemented according to the following procedure.

4.2 WBG is entitled to amend or supplement this Agreement, provided WBG considers this necessary, in particular, to comply with the statutory obligations of the Parties in accordance with applicable data protection law.

4.3 WBG shall inform the other Party in writing at least in text form (e.g. by email) with a notice period of six (6) weeks prior to the planned entry into force of the amendment or supplement. If the other Party does not object to the changes to WBG in text form within four (4) weeks after receipt of the notification of the changes and continues to use the Affiliate Marketing Services after the expiry of this period, the amendment and/or supplement shall be deemed to have been accepted and the Agreement shall be accordingly amended with the expiry of the aforementioned six (6) weeks period.

4.4 WBG shall inform the other Party with receipt of the notification of the consequences of further, unobjected to, use of the Affiliate Marketing Services.

4.5 If the other Party objects to the amendments or supplements, the Parties shall discuss any complaints and disagreements constructively and clarify them in an amicable manner. If the Parties do not find any solution, both WBG and the Advertiser have the right to terminate this Agreement or the corresponding commissions with a notice period of four (4) weeks.

5. TERM AND TERMINATION

5.1 This Agreement enters into force with the confirmation of its validity by the Advertiser in the previously communicated procedure, whereby the decisive date is when the last Party agrees either by signing this Agreement or by another way (in particular, by electronic acceptance of these conditions or by email or by implied agreement by the use of the Affiliate Marketing Services without objection). Each Party is bound to the provisions contained in the Agreement from the effective date.

5.2 This Agreement runs for an indefinite period and ends automatically at the end of the contractual relationship based on the GTC and the associated use of the Affiliate Marketing Services.

6. TERMINATION

6.1 Any notice of termination within the framework of this Agreement ("**Termination**") must be done in writing.

6.2 If WBG is entitled to terminate the contractual relationship based on the General Terms and Conditions and the use of the Affiliate Marketing Services pursuant to the GTC, WBG also has a right to terminate this Agreement.

6.3 The right to extraordinary termination remains unaffected for both Parties.

7. ASSIGNMENT

The Advertiser may not assign or transfer any rights or obligations from this Agreement without the prior written consent of WBG.

8. SEVERABILITY CLAUSE

8.1 If a provision of this Agreement is, in whole or in part, unlawful, invalid or unenforceable, the legality, validity and enforceability of the remaining provisions of this Agreement shall not be affected thereby.

8.2 The parties undertake to agree to an effective provision in place of the invalid provision, whose effect comes as close as possible to the economic objective that the Parties pursued with the invalid provision. The aforementioned provisions apply accordingly in the event that the contract proves to be incomplete.

9. APPLICABLE LAW, JURISDICTION

The place of fulfilment and place of jurisdiction is Nuremberg, Germany. The law of the federal Republic of Germany applies, excluding the use of any conflict of laws. The application of the uniform UN Sales Law based on the Treaty of the United Nations dated 11/04/1980 for Contracts on the International Sale of Goods is excluded.

10. RELATIONSHIP WITH THE GENERAL TERMS AND CONDITIONS OF BUSINESS

10.1 All circumstances not expressly regulated in this Agreement, including the liability of the Parties for the provision or use of the Affiliate Marketing Services are subject to the provisions of the General Terms and Conditions.

10.2 In the case of contradictions between the provisions of this Agreement and the GTC, the provisions of this Agreement shall have priority.

*****

Part A

Regulations for Processing

Preamble

These regulations for Processing ("**Regulations for Part A**") specify the data protection obligations of the Parties that arise from the Processing described below. The regulations in this Part A concern the processing of Personal Data by WBG on behalf of the Advertiser or third parties commissioned by the Contractor (hereinafter also "Sub-Contractors").

1. Roles of participants and responsibilities

For the implementation and processing of the Affiliate Marketing Services, the merchant as the client is dependent on the processing of Personal Data by WBG as the contractor. For this purpose, the Contractor provides services for the Client in the scope described in **Appendix 1** to this Part A.

2. Subject matter of the order, type, purpose and scope of the data processing

2.1 The subject matter of the order is the specific processing activities by WBG on behalf of, and according to the instruction of, the Advertiser as specified below and/or in the GTC including this specific documentation or in other supplemental agreements or an order (hereinafter referred to as the "**Commissioning**").

2.2 The types and categories of the collected and/or processed Personal Data as well as the categories of the Data Subjects affected by the handling of Personal Data within the framework of this order are specified in **Appendix 1**.

2.3 The purpose, type and scope of the collection, processing and/or use of the Personal Data within the framework of the order are specified in **Appendix 1** to this Part A.

3. Responsibility and rights of instruction of the Controllers

3.1 The Client alone is responsible for the assessment of the legal admissibility of the processing of Personal Data carried out within the framework of the contractual relationship by the Contractor with regard to the respective applicable provisions of data protection law.

3.2 The Contractor shall process the Personal Data of the Client exclusively to fulfil the obligations of the Order Processing Agreement, the Main Contract or supplementary individual instructions in accordance with Clause 2.

3.3 Within the framework of the contract, the Client reserves a comprehensive right of instruction regarding the type of data processing, the purpose of processing, the type of Personal Data and categories of Data Subjects, which he can specify by individual instructions. The rights of instruction to which the Client is entitled with regard to processing Personal Data are definitively specified by the functions provided in the scope of the applications and systems.

3.3 Clause 3.2 is restricted where the Contractor is obligated to do so by the law of the Union or Member States to which the Contractor is subject; in such a case, the Contractor shall inform the Client of these legal requirements prior to processing, provided that the relevant law does not prohibit such a notification due to an important public interest.

3.4 The Contractor shall inform the Client if he is of the view that an instruction violates data protection regulations. The Contractor is entitled to suspend the implementation of the corresponding instruction until it has been confirmed or changed by the Client.

4. Instructions and persons authorised to issue instructions

4.1 The Client or an authorised representative shall issue all instructions in text form (in writing by email). If oral instructions are issued in exceptional cases, the Client will immediately confirm this with email.

4.2 To the extent that instructions or directives under this Agreement are to be made to the other Party, these must be addressed to the persons named in Appendix 2.

5. Obligations of the Contractor

5.1 The Contractor is not permitted to correct, delete or restrict the processing of Personal Data unless there is a corresponding instruction beforehand or the deletion is made in accordance with Clause 15 of this Agreement (contract termination). Requests from Data Subjects, in particular for correction, deletion or blocking must be forwarded to the Client without delay.

5.2 The processing of the data takes place exclusively in the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the Client. If an exception has been approved by the Client, an appropriate level of protection must be ensured that meets the requirements of Art. 44 et seqq. GDPR

5.3 The Contractor shall not store or copy the data material or information that can be derived from it on its devices or data media unless this is necessary to execute the order.

5.4 If the Client needs information from the Contractor to be able to fully create its directory of processing activities, the Contractor shall provide the information on request.

5.5 The Contractor undertakes to establish an internal compliance structure with which the relevant data protection regulations and obligations of the Processing Agreement are implemented. This also includes - if necessary - support in carrying out a data protection impact assessment.

5.6 If required by law, the Contractor shall appoint a qualified commissioned officer for data protection, whose name and contact details in must be noted in **Appendix 2**. The Contractor shall inform the Client immediately about any changes to this.

6. Confidentiality of data processing and requirement of employees to be bound by the instruction

6.1 The Contractor is obliged to ensure that its employees who have access to Personal Data within the framework of the order fulfilment, process this data exclusively on instruction of the Controller. This is not applicable if the service provider is obligated to process the contractual Personal Data according to the Union law or the law of the Member States.

6.2 When selecting and using the employees, the Contractor must ensure that they comply with the statutory provisions concerning data protection and do not disclose any information obtained from the Client or otherwise exploit it.

6.3 The Contractor must instruct any person under its control who has access to Personal Data within the framework of fulfilment of the order on the contractually intended processing of the contractual data.

6.4 The Contractor shall only use employees who have been familiarised with the data protection provisions relevant to them and ensure that all employees who are involved in the processing of the data disclosed within the framework of this contract have been obliged to maintain confidentiality or are subject to an appropriate legal secrecy obligation.

7. Procedure for enquiries from Data Subjects or third parties

7.1 The Contractor shall inform the Client by email of the receipt of any enquiries or requests made by a data protection supervisory authority or a journalist regarding the subject matter of this contract within 48 hours in relation to the working days in the United Kingdom.

7.2 The Client, as Controller, is responsible for ensuring the rights of the Data Subjects. If not explicitly specified otherwise by instruction, enquires from Data Subjects will be answered exclusively by the Client. Insofar as a collaboration of the Contractor is required for the processing of enquires from Data Subjects, in particular for information, correction, restriction, data portability or deletion, the Contractor shall take the necessary measures in accordance with the instructions of the Client.

7.3 The Contractor shall inform the Client's person authorised to issue instruct instructions about the corresponding enquires immediately (within 48 hours) and in full. A procedure for the exchange of information shall be coordinated between the Parties with regard to the exchange of information.

8. Sub-service providers

8.1 The inclusion of additional processors in order fulfilment (= sub-service providers) by the Contractor is only permitted with the consent of the Client. The Contractor shall notify the Client in text form in advance about the inclusion of additional sub-service providers and the transfer of Personal Data to them for processing. If the Client does not object to this use within 6 weeks after notification, the consent of the Client is deemed to be granted.

8.2 The prerequisite for approval to engage additional sub-service providers is their specific designation with names and contact details together with further information on the subject matter, type, scope and purpose of the specifically intended data processing. Furthermore, the Contractor must verify that the sub-service providers will comply with the IT security measures according to the specifications of Appendix 4 and submit the findings made to the Client upon request. The Client shall not unreasonably refuse consent to commissioning sub-service providers.

8.3 Commissioning sub-service providers or sub-sub-service providers in third countries (outside EU/EEA) takes place, provided that the relevant requirements of the GDPR are complied with.

8.4 If a Commissioning is permissible, the Contractor must select the sub-service provider carefully with regard to the fulfilment of contractual obligations. He must design the contractual agreements with the sub-service provider in such a way that they meet the data protection provisions of the Order Processing Agreement. In particular, it has to contractually secure the rights of disposal regulated in this Agreement and the inspection rights of the Client vis-a-vis its sub-service providers. This contractual protection must be designed in such a way that the Client – without prejudice to the responsibility of the Contractor for the sub-service providers – is entitled to directly monitor the sub-service provider. At the request of the Client, the Contractor is obligated to immediately provide information to the sub-service provider about the contractual content for the monitoring and the implementation of the data protection relevant obligations by the sub-service provider.

8.5 The previously approved sub-service providers are listed in **Appendix 3** whereby the approval is subject to the reservation that compliance with data security measures is documented by the Contractor prior to the start of data processing and the specifications according to this Clause 8 are complied with. An updated list of sub-service providers is always retrievable under https://www.webgains.com/public/en/privacy-sub-processors/.

8.6 The Contractor must review the compliance with these obligations by the sub-service provider regularly by means of appropriate inspections (i.e. at least once a year) and provide a remedy in the event of violations. The inspections and the measures initiated in the case of detected deficiencies must be documented. The reports are to be made available to the Client on request.

8.7 Subcontracting relationships for specialist services for which the conclusion of an order processing agreement is not required are not subject to approval, in particular, ancillary services such as telecommunications services, postal services for the transport of letters or packages, cleaning services or activities of the professionals subject to secrecy (tax consultants, attorneys, external company physicians, auditors).

9. Specification of the technical and organisational measures

9.1 The Contractor's selection is carried out in particular based on the assessment that it provides sufficient guarantees of compliance with the technical and organisational measures for data security and the processing of Personal Data in accordance with the requirements of the legal regulations ensures a level of processing security appropriate to the risk to the rights and freedoms of the rights of the natural persons affected by the processing

9.2 If it is not a case of remote maintenance/remote access, the Contractor shall ensure the protection objectives of Art. 32 para. 1 GDPR, such as the confidentiality, integrity, availability and resilience of the systems and services used for data processing and their resiliency in regard to the type, scope, circumstances and purposes of the processing. In addition, it is ensured in this case that the availability of data and access to it is quickly restored upon the occurrence of a physical or technical incident and that as far as possible transport and storage encryption is used.

9.3 The Contractor has used a recognised methodology for the risk assessment for the processing of Personal Data under the contract, which takes into account the probability of occurrence and severity of the risks for the rights and freedoms of the Data Subjects.

9.4 For its area of responsibility, the Contractor guarantees the implementation of appropriate technical and organisational measures for compliance with the data protection regulations according to the current state of the art and permanent containment of the risk associated with data processing. The data protection concept described in Appendix 4 represents the selection of the technical and organisational measures appropriate with regard to the determined risk, taking into account the protection objectives in accordance with the state of the art, and in particular taking into account the IT systems and processing operations used at the Contractor and is determined in a binding manner.

9.5 The contractual processing of data in the home office is permissible if the Contractor ensures appropriate security measures for the criticality of the data processing – comparable to data processing in the office. The Contractor must take appropriate technical and organisational precautionary measures for this and provide proof upon request.

9.6 Technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. The specified measures may not fall below the security level. Significant changes that are significant for the security of the data (e.g. in the organisation of data processing on order) are to be coordinated with the Client in advance. The Contractor is obliged to carry out, as warranted but at least yearly, a review, assessment, and evaluation of the effectiveness of the technical and organisational measures for ensuring the security of the processing (Art. 32 para. 1 lit. d GDPR).

9.7 The Contractor shall provide the Client with its current data protection and data security concept as well as its IT security governance concept for processing in accordance with this Agreement.

10. General control and notification obligations of the Contractor

10.1 If the Contractor is of the opinion that an instruction violates the data protection regulations, the Contractor shall inform the Client immediately in text form. The Contractor is entitled to suspend the implementation of the corresponding instructions until it is confirmed or changed by the Client. The Contractor is not entitled to a substantive-law review.

10.2 At regular intervals, but at least once per calendar year, the Contractor is obligated to verify compliance with the specifications of this Agreement that are relevant to it. This particularly concerns compliance with data security requirements according to **Appendix 4**. The audit and the findings made must be documented.

10.3 If the Contractor is of the opinion that orders made by the Client are insufficient for data security, it shall inform the Client immediately.

11. Co-allocating violations of the Contractor / data loss

11.1 The Contractor shall inform the Client immediately of faults, violations by the Contractor or persons employed by it of data protection law or contractual provisions or specifications made by instructions or in this Order Processing Agreement as well as the suspicion of violations of the aforementioned data protection regulations or irregularities in the processing of Personal Data. This notification is to be sent by email to the Client's person authorised to issue instructions cited in Appendix 2.

11.2 With regard to any information obligations of the Client vis-à-vis Supervisory Authorities for data protection and/or the Data Subjects, the Contractor must inform the Client immediately (within 24 hours) of all incidents for which it cannot be ruled out that data was taken out of control or was otherwise disclosed, or could be disclosed, without authorisation to third parties. In this case, the Client can demand the collaboration of the Contractor in immediately clarifying the facts, working-up of the incident and taking measures to remedy or mitigate the consequences of the violation of the protection of Personal Data.

11.3 In the event that the Contractor determines, or the facts justify the assumption, that a violation of the protection of the data processed for the Client by the Contractor, led to the unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access in any other way, of Personal Data, due to a violation of IT security, the Contractor must inform the Client immediately and completely, in text form, about the time, type, and scope of the incident(s). The information must contain a presentation of the type of unlawful disclosure. The information should additionally include a presentation of possible detrimental consequences of the data security incident.

11.4 The Contractor shall create a directory of all data security incidents that occur, insofar as they affect the data processing under this contract and provide the directory to the Client upon request.

12. Inspection by the Client

12.1 The Client, or an appropriate representative, has the right to check the compliance with all instructions and provisions of this contract and the data protection provisions, provided they are applicable to the contractual data processing, by inspections of the Contractor, including regular reviews, during normal business hours, free of charge. The Contractor undertakes to tolerate corresponding reviews and to support the Client in performing its inspections in accordance with para. (3).

12.2 The Contractor confirms compliance with the security measures described in Appendix 4 by submitting a current certificate of an independent authority (e.g. IT security officer, data protection officer, data protection auditor) according to the sample **Appendix 5**. This confirmation does not restrict right of inspection according to para. 1.

12.3 The Contractor shall provide the Client with all necessary information for the proof of compliance with the obligations of the Order Processing Agreement and for the fulfilment of existing data protection obligations, including accountability. The Contractor grants the Client all rights of access, information and inspection required for the implementation of the inspection by the Contractor. The Contractor agrees, in particular, to grant the Client access to the data processing facilities and other documents in order to enable the inspection and review of the relevant data processing facilities and other documentation that are related to the collection or use of Client data. In this case, the Client shall appropriately take into consideration the operational procedures and legitimate non-disclosure interests of the Contractor.

12.4 A protocol must be prepared about the inspection and its results.

12.5 In accordance with the applicable data protection regulations, the Client and the Contractor are subject to public inspections by the competent Supervisory Authority. At the request of the Client, the Contractor shall support the Client in the framework of regulatory supervisory procedures to the best of its abilities, if and to the extent that the contractual processing of Client data is the subject matter of the supervisory procedure.

13. Completion of orders/end of the contractual relationship

13.1 Unless otherwise instructed, the following provisions apply:

(a) In the case of implementing individual orders, the Contractor shall irrevocably delete the Personal Data provided by the Client three (3) months after the individual order has been executed.

(b) If the term of the Order Processing Agreement, the term of the Main Contract, or a service agreement are equivalent and there is no case of an individual order, then the data accumulated in the context of the contract shall only be deleted after a separate instruction of the Client.

(c) The Client has the right to demand return of the data instead of a deletion.

13.2 After processing individual orders, the contractor confirms to the client without further request that the contractor has completely destroyed or irrevocably deleted the data provided, the temporarily stored data or the test and scrap material. Deletion/destruction must be documented in a suitable way – for example by logging. Documentation of deletion/destruction must be submitted upon request.

13.3 Documentation that serves to prove proper data processing must be stored by the Contractor in accordance with the respective retention periods beyond the end of the contract. The Contractor can transfer it to the Client at the end of the contract for its discharge.

13.4. The Client, or an appropriately authorised person, has the right to check the complete and contractual return or deletion of data or the destruction of test and rejection material by the Contractor. This can also be done by a visual inspection of the data processing systems at the Contractor' premises. The on-site inspection should be announced with a reasonable notice period by the Client.

13.5 If the term of this Agreement is based on the term of the Main Contract and the Main Contract ends, the Contractor is also entitled to further storage and processing of data beyond the end of the Main Contract only in the context of proper processing of the contract.

14. Appendices

The following Appendices are part of this Agreement

- Appendix 1: Instruction for processing data on behalf of the Client
- Appendix 2: Contact persons
- Appendix 3: Pre-authorised subcontractors
- Appendix 4: Data Security Requirements
- Appendix 5: Confirmation of compliance with data security

*****

PART A

Appendix 1: Instruction for processing data on behalf of the Advertiser to WBG

The specific instructions for processing the Personal Data for the provision of service are specified with this Appendix.

Order overview	
Basis for issuing instruction	On the basis of the service agreement between Advertiser and WBG, the Controller issues instructions for data processing to the Processor: ☒ in accordance with the General Terms and Conditions with a specific service description and ☒ according to subsequent specification:
Subject matter/type/scope of processing/specification of processing	☒ IT services according to the following type for • storage of cookies on the end devices of the users, provided they have given consent to the Advertiser on its website. • recording of access to the offers (advertising material) of the Advertiser, which are obtained by the tracking code provided by WBG and integrated by the Advertiser into its advertising material. • recording of the Publisher involved in a transaction. • creation and storage of a probabilistic-ID on the end devices of users, provided they have given consent. • storage of a deterministic ID on the end devices of users, provided they have given consent. _____ ☒ Advertising services according to the following type for • creation and provision of evaluations with regard to the data stored for the Advertiser using the evaluation tools provided by WBG _____ ☒ Services according to the following type for • creation of reports for the Publisher acting for the Advertiser on the basis of the data generated for the Advertiser • calculation of fees for Publishers • calculation of fees for the work of WBG • evaluation of the data collected for detection of attempted fraud and other misuse of the platform • remote maintenance and support for technical problems _____ ☒ Transmission of data to WBG based on the Joint Control Agreement (see Part B).
Purposes of processing the Personal Data of	Recording of the sales (transactions) brokered by the Publisher in the platform provided by the Contractor and creating analyses for the Client. This also includes the provision of evaluations

Data Subjects by the Client	regarding the scope of sales activities for the Advertiser. WBG also records for the Advertiser, the Publishers involved in the sale in order to enable an allocation of the remuneration to individual Publishers by the Advertiser. The proper recording is done by means of the tracking code provided by WBG, which is taken over by the Client and integrated into its advertising material that is delivered by the Publishers. This also includes – in so far as there is consent – the storage of cookies on the end devices used by the user by WBG as a service provider of the Client.
Start and end of processing	☒ continuous ☐ Individual order Start: : _____ End: : _____(*if applicable, indefinite)*
Data Subjects (categories)	☒ Customers ☒ Potential customers/prospective customers ☒ Other: Publisher data
Types of Personal Data	☒ Transaction data: transaction ID, Publisher ID, order reference number, timestamp ☒ Contract data: product info; user country, value ☒ Contract billing data: sales value, currency, commission type ☒ Information on the devices of the user / browser, cookie ID, cache reference ID ☒ Other: IP-Address, User-Agent, Campaign-ID, Program-ID, Probabilistic-ID, Event-ID, Reference-ID, Deterministic-ID
Type of data delivery	☐ SFTP ☒ HTTPS (download link) ☒ Integration of the WBG application via the tracking script;
Return/deletion periods after completion of the order	☒ 3 months ☐ 6 weeks ☐ _____

Appendix 2: Persons authorised to instruct, data protection officers

1. Client's person authorised to issue instructions:

Contact person on the part of the Client:

- The contract signatory itself
- Corporate bodies of the Client and/or authorised representatives
- Other persons named to the Contractor

2. Contractor's person authorised to issue instructions

Contact person on the part of the Contractor:

Function currently:	Head of Affiliate & Account Management
Name:	Nichelle Büttner
Email:	NBuettner@webgains.de

as a substitute:

Name:	Hanna Eidenhardt
Email:	HEidenhardt@webgains.de

3. Data Protection Officer of the Contractor

Name: Dr. Stefan Drewes
Email: data-privacy@webgains.com; datenschutz@webgains.de
Telephone: +49 (0)228 / 90 24 80 70

☐ internal ☒ external

PART A

Appendix 3: Approved subcontractors

No.	Supplier/Service provider	Location	Purpose
1	Webgains Ltd, Third Floor, 21 Farringdon Road, London, EC1M 3HA	England	Management IT application, IT support
2	Amazon Web Services, Inc	Ireland and England	Hosting service
3	In addition pursuant to Clause 8 of Part A, included as subcontractor are the Webgains companies in the EU, provided the campaign is delivered throughout the EU	WBG locations in the EU (currently: France, Germany, England, Spain, Italy, The Netherlands)	Support for processing the EU-wide campaigns / management of the WBG platform
4	Neory GmbH	Germany	container tag solutions
5	Rollbar, Inc.	San Francisco, California, USA	Rollbar monitors application errors for Advertisers. While sending Rollbar error data, Advertisers may inadvertently include end user personal data. Consequently, a data processing agreement is agreed on.

*****

Appendix 4: IT security measures

For the specific data processing, a level of protection is guaranteed suitable for the risks to the rights and freedoms of the natural persons affected by the processing. For this purpose, the protection objectives of Art. 32 para. 1 GDPR, such as confidentiality, integrity and availability of the systems and services, as well as their resilience in regard to the type, scope, circumstances and purpose of the processing, are considered in such a way that the risk is mitigated by means of suitable technical and organisational measures.

The service provider has defined the security objectives, an IT security process and IT security management in its IT security concept to ensure the protection of Personal Data through appropriate technical and organisational measures. According to the specifications from the IT security concept, the risks associated with data processing were determined as well as a determination of the potential effects on the Data Subjects and the probability of occurrence. The determination of the technical measures to ensure data security takes place – as shown in the IT security concept – in consideration of the state of the art as well as the implementation costs.

The ongoing guarantee of the requirements resulting from statutory provisions, e.g. GDPR, is ensured by the "IT security management", where, in addition to the clear definitions and functions as well as tasks and responsibilities including, but not limited to, the implemented technical and organisational measures set forth below in this Appendix in accordance with Art. 32 GDPR, are implemented and continuously monitored and checked in the context of security checks.

The measures described below represent the selection of the technical and organisational measures ("TOM") to guarantee data security according to Art. 32 GDPR, suitable for the risk determined, taking into consideration the protection objectives according to the state of the art. The following protective level concept was used as a basis:

Protection level	Personal data	for example (for individual data; for cumulative data, if necessary, higher protection level attached!)	Severity of possible damage
A	have been made freely accessible by the Data Subject	telephone directory, freely accessible website, freely accessible social media	Minor
B	the improper handling of which does not lead to any particular adverse effects, but which were not made freely accessible by the person concerned	Restricted access public files, land register access, non-freely accessible social media; masked IBAN (the last six numbers blacked out), customer master data, date of birth, place of birth	Minor
C	The Data Subject could be impaired in his or her social status or in his or her economic circumstances ("reputation") by improper handling	income, tax data, administrative offences, passport data, IBAN (complete); contract data (delivery and order data)	Manageable
D	The Data Subject could be significantly impaired in his or her social status or in his or her economic	commitment to an institution criminality, official assessments, job references, health data,	Substantial

	circumstances (“existence”) by improper handling	liabilities, garnishments, data of special categories according to Art. 9 GDPR	
E	Their improper handling could impair the health, life or freedom of the Data Subject	Data about persons who can be a potential victim of a criminal act, witness protection program	Great
F	which are processed within the framework of remote maintenance/remote access	Special regulations that address the specific situation of remote maintenance/remote access.	

The Parties have found that the processing of Personal Data regulated in this Order Processing Agreement is subject to the following protection requirement:

Protection level	**Check as appropriate**
A	☐
B	☐
C	☒
D	☐
E	☐
F	☐

The following catalogue of measures contains the agreed technical and organisational measures to guarantee the determined protection requirement of protection level C.

If a further need for protection has been established for individual data processing, the additional measures taken are documented to ensure the protection objectives in the respective process description:

I. Organisational specifications to ensure data security

The service provider maintains a procedure for regular review and evaluation of the effectiveness of the technical and organisational measures taken to ensure the security of data processing. This is also intended to ensure that the measures taken to ensure data security correspond to the state of the art. This is to be demonstrated to the Client at any time upon request.

II. Technical measures for ensuring data security

The Contractor shall take the following measures to ensure data security, compliance with which is ensured with appropriate controls within the framework of organisational measures:

Protection objective: Confidentiality

It must be ensured that no person – both employees and third parties – has unauthorised knowledge of Personal Data. Ensuring this protection objective requires measures for date entry and access control. Unauthorised device access should be prevented. In addition, the specifications for client separation are also listed here in order to ensure that data is assigned to a controller.

1. Entry control:

Control of the entry to the premises of data processing systems (DP system) by unauthorised persons. Entry control must prevent persons who are not authorised from being able to get near a DP system. The DP systems include, in addition to the central unit including the integrated drives, the connected peripheral units such as terminals, PCs, printers, plotter and tape units, etc. Also included are the end devices used for remote access.

Entry control to PCs within office spaces is ensured, e.g. by measures that are taken to prevent customers from getting near the PCs or being able to view the screen.

Measures to meet the protection objectives
Entry regulation for persons outside of the company; the implementation is carried out by the following points:
• Regulations for entry by external persons
• Logging of the arrival and departure of non-company persons
• Availability of central reception area (gatekeeper/reception)
• Issuance of visitors ID
• Presence of non-company personnel anywhere in the company building only in the presence of employees
• Return of access equipment after the authorisation has expired
Entry regulation for company personnel; the implementation is carried out by the following points:
• Determination of persons authorised to enter, including the scope of the authorisations, for physical access to relevant rooms/security areas
• Issuance of entry authorisation cards (e.g. chip card with logging)
• Logging of employees' arrival and departure
Determination of persons authorised to enter the computer/server room
Measures so that only authorised entry to the computer/server room occurs
Provision of lockable cabinets/rolling containers for employees
Key control if keys are used, (locked doors; issue keys only to authorised persons; storage and use of a general key)
Measures for object protection (e.g. protection of ducts and windows; area monitoring)
Secured entrance (e.g. locking system, ID reader)

Burglar resistance window

2. Access control:

The use of DP systems by unauthorised persons (unauthorised employees or external persons) should be prevented. The access control involves the question of identification and subsequent authentication. The access control also includes the goal that no external access (e.g. from the internet) can take place on DP systems (hacker protection).

Requirements
Authentication of users compared to the data processing system, e.g. identification by user name and password or 2-factor procedure
Regulations for password assignment
Personal password
At least 10 characters including special characters/numbers, upper case and lower case letters
Rights management
Logging of accesses
Assignment by user himself
Expiration after specified time
Access block after three failed attempts
No disclosure to third parties
Regulation for absence (leave, illness, etc.)
Blocking of the last 5 passwords used
Immediate blocking of authorisations when employees leave the company
Regular monitoring of the validity of authorisations (annually)
Securing of the workstations screen for absence and running system (password protection for screen savers after 5 min. to 15 min, depending on the risk of misuse)
Separation of internal networks against access from outside (firewall, encryption VPN)

3. Data access control:

The goal of data access control is that employees and authorised third parties can access data only within the framework of their access authorisation. In addition, it should be ensured that Personal Data cannot be read, copied, altered or removed (deleted) without authorisation when it is being handled. This applies to both to data stored in DP systems as well as for that which is on machine-readable data media or on paper.

Requirements
Creation of a user profile, i.e. determination of access rights with regard to processed Personal Data
Differentiated permissions for reading, modifying or deleting data
Assignment of authorisations to employees and vicarious agents according to the minimal principle; access to applications and system components is only permitted if this access is required for the specific activity.
Creation and implementation of an authorisation concept • Setting up administration rights
Management of access rights by system administrator
Encryption of all devices (smartphone, notebook, etc.)
Transmission encryption for email
Screensaver
Separation of test and production operation
Configuration of the EDP devices used so that all services and components that are not required to fulfil their services are deactivated. Annual review of the proper configuration

Assignment of authorisations must be documented comprehensively and an approval step must be included.
Data protection-compliant disposal of no longer required data media according to the respective state of the art in compliance with the respectively valid standards (DIN 66399: 2012) or commissioning a service provider specialised in disposal of data media who will destroy the data storage devices with the same or higher level of security. The data storage media intended for disposal must be protected against unauthorised access during storage and transport with suitable measures.
Data protection-compliant disposal of waste paper (for example, incorrect printing of work lists, letters, etc.) by means of a file shredder, which has a security level P-4 defined according to DIN 66399:2012 or commissioning a service provider specialising in file destruction who will destroy the documents with the same or a higher level of security.
Exclusion of private internet use for employees who have access to data from the customer at the same time.
Exclusion of private use of the business email account for employees who simultaneously process data from the Client.

4. Separation control:

According to the separation requirement, data collected for different purposes must be processed separately (also: requirement of non-linkability). This is intended to ensure that the intended purpose of the Personal Data is implemented through organisational and technical measures. The separation requirement is particularly important in the context of order processing, if, for example, data of several clients is stored on a system. If the separation requirement cannot be achieved by technical measures such as access control software, separate storage is necessary.

Requirements
Authorisation concept with determination of access rights
Multi-client database

Protection objective: Integrity

It must be ensured that information technology processes and systems continuously meet the set specifications so that the data to be processed with them remains intact, complete and up to date. Information must be correct and complete in terms of content, originate from the creator and may only be changed by authorised persons. This protection goal requires measures to ensure the integrity of data when being transmitted. It should also be ensured that changes to data are also attributable to the initiator (input control).

5. Transmission control:

This includes all variants of the transfer of personal data by means of data storage devices or communication networks. The transmission control should prevent data from being used without authorisation while being transmitted (read, copied, changed, or removed/deleted). The term transfer includes both the transfer to third parties and the transfer within the framework of order processing between the client and contractor and to the data subject.

Requirements
Documentation of data recipients, transport/transmission routes, the persons authorised to transmit data and the data to be transmitted
Authenticated and sufficiently encrypted transmission of data prior to transmission with unsecured transmission paths

6. Input control:

The input control is intended to document who is responsible for (un)permitted or erroneous data entry. The goal is the auditability of the input of personal data into the DP system, which also includes non-networked individual workstations, such as PCs. The data entry to be checked includes the first-time storage as well as the change and deletion (removal) of data.

Requirements
Management of audit-proof (written, comprehensible) access authorisations
Logging of input, changes or deletion of personal data
Regulation of access authorisations to created protocol data
Use of check sums

Protection objective: Availability and resilience

It must be possible to quickly restore the availability of personal data and access to it in the event of a physical or technical incident For this purpose, the protection of data against accidental destruction or loss must be guaranteed. Possible hazards are, for example, water damage, lightning strike, power failure, fire, sabotage or theft. The protection objective of the resilience should achieve a certain stability with regard to failures of, and attacks on, the systems. Since this requirement also has special relevance in outsourcing services (hosting data), the requirements for an order control are also listed here.

7. Availability control:

The following measures in the area of availability control exist in order to prevent accidental loss or destruction of data and to ensure a rapid restoration of the availability of the Personal Data in the event of a physical or technical incident.

Requirements
Formalised release procedure for new DP procedures and in case of significant changes in old procedures
Uninterruptible power supply (UPS)
Automatic fire and smoke alarm systems
CO2 fire extinguishing device in/in front of server room
Securing data inventories
• Creation of an inventory protection concept
• Storage of backup copies in a safe place (outsourcing)
• Creation of backup copies according to the generation principle in suitable time intervals
• Restart concept for the reconstruction of data inventories
• Test runs in the reconstruction of data inventories
Redundancy of hardware and software as well as infrastructure

8. Order control:

Guarantee of processing according to instructions. The Contractor must comply with the instructions given to it, while the Client must ensure that its instructions are clear and unambiguous and are followed.

Requirements
Control of compliance with data security provisions by Contractor
Reporting if there are violations or there is suspicion that the data security guidelines are insufficient
Obligation of employees of the Contractor to ensure data protection-relevant requirements
Issuing instructions to employees with regard to the intended use of data as well as the scope of data that is required and should be used for the execution of the order.

9. Procedure for regular review

Continuous guarantee of compliance with data protection specifications and IT security. The Contractor must regularly review and document that the contractually owed specifications are complied with.

Requirements
Introduction of a system for accountability and IT security governance (in the required scope)
Incident Response Management
Regulations for controlling processes for changing procedures
Reporting security incidents that are detected in ongoing operation
Monitoring of the effectiveness of the implemented measures at least once a year
Safe and sufficient default setting for the servers by which a secured restart of the server system can be carried out in the planned time

*****

PART A

Appendix 5: Confirmation of compliance with data security

Confirmation

for the implementation of data security requirements by the Processor

The Contractor hereby confirms that it has implemented the data security requirements specified by the Client in Appendix 4 before the start of data processing and has also verified this in the context of a review.

Part B

JOINT CONTROLLER AGREEMENT

Preamble

The use of the WBG platform for affiliate marketing requires a division of labour between the WBG and the Publisher and Advertiser to the extent described below ("**cooperation** ") as well as data protection in accordance with Art. 26 GDPR between Publishers and Advertiser (see Part D JOINT CONTROLLER AGREEMENT). For this purpose, the Parties shall grant each other access to specific Personal Data or collect and process it during the collaboration.

This Agreement is concluded between the Advertiser and WBG. In addition, the Advertiser and commissioned Publisher agree to an additional JOINT CONTROLLER AGREEMENT (in accordance with Part C) for the collaboration relevant to data protection law. This Agreement is also concluded in cases where Advertisers use certain Publishers for the placement of displays/advertising.

In this Part B, the Parties shall specify the scope of the Collaboration, mutual obligations of the Parties and their respective roles and responsibilities in regard to compliance with the respective data protection obligations.

1. Scope of Collaboration

As part of the collaboration, the Controllers will act as Joint Controller. The roles of the Controller and the associated tasks are specified in more detail in Appendix 1. If one party is solely responsible for a data processing operation, this party will implement all relevant data protection provisions on its own responsibility. However, such data processing procedures are not subject to this Agreement.

Joint data processing and the type of Personal Data collected and processed within the framework of collaboration are specified in Appendix 1.

2. Obligations of the Controller, Processors

2.1 The Controller carries out the processing of Personal Data in accordance with the relevant provisions of the applicable data protection laws. Both Parties and the Publisher are jointly responsible externally for compliance with the applicable data protection laws with regard to joint data processing. In the internal relationship, the scope of the responsibility for compliance with the applicable data protection laws arises from Appendix 1 where the Parties have been assigned individual data processing procedures.

2.2 The Controllers use the Personal Data within the framework of this Collaboration for the purposes as described in Appendix 1. For further data processing beyond the joint responsibility, each Controller is solely accountable and must comply with the data protection law requirements independently.

Should the Parties process Personal Data for purposes other than those described herein, the Parties shall inform each other in the appropriate scope, provided this is mandatory by law.

2.3 The Data Controllers ensure that all persons who are involved in the processing of Personal Data are required and/or will be required to maintain confidentiality and will process personal data on instruction of the controller only.

2.4 Personal Data must be correct and, if necessary, up-to-date. The collection and processing of Personal Data must be restricted appropriately and considerably to the purpose as well as to the extent necessary for the purposes of transmission and further processing.

2.5 The Controller will only process Personal Data in accordance with the contract with the aid of Processors if an order processing agreement corresponding to the statutory requirements is concluded with the

respective Processors. The Controller shall only disclose Personal Data to third parties to the extent this is actually required for fulfilling the obligations resulting from the Collaboration or is otherwise legally permissible and proper and the other Party is informed of the other recipients of the Personal Data.

3. Technical and organisational measures

Taking into account the state of the art, the implementation costs and the type, scope, circumstances, and the purposes of processing, as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons, the Controllers shall take appropriate technical and organisational measures to ensure an appropriate level of protection; these measures include, depending on individual case, the following:

- pseudonymisation and encryption of Personal Data;
- the ability to ensure, over the long-term, the confidentiality, integrity, availability and resilience of the systems and services in connection with processing;
- the ability to rapidly restore the availability of Personal Data and access to it upon the occurrence of a physical or technical incident;
- a procedure for regular review, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing.

4. Responsibility for compliance with data protection laws and rights of Data Subjects

4.1 As a rule, the Controller who has initially collected the Personal Data or has a direct contractual relationship with the Data Subjects is a central contact point for the Data Subjects. This is usually the Advertiser who is directly in contact with the customer and has collected its data for the conclusion of the contract.

4.2 Data Subjects are entitled to various rights with regard to the Personal Data processed by the Controller. The Controllers agree to fulfil their respective obligations in accordance with the provisions of the applicable data protection laws.

4.3 Data Subjects must be provided with information about the processing according to Art. 13 and 14 GDPR. The Parties agree that Publisher issues the information obligations vis-a-vis the Data Subjects for the data processing described in Part C, Appendix 1. Furthermore, it is the responsibility of the Advertiser to provide all necessary information on the data processing activities listed in Part B Appendix 1 to the Data Subjects in a suitable manner in accordance with the procedure described below.

4.4 The Controllers support each other in the fulfilment of corresponding contractual and/or other statutory obligations and provide the necessary information on the relevant data processing activities in order to meet these requirements. WBG shall provide the Advertiser with separate data protection notices that will provide its end customers with information on the data processing activities carried out by WBG in the course of the use of Affiliate Marketing Services. Notwithstanding the provision of the above-mentioned data protection notices, the Advertiser remains responsible for complying with all legal obligations that it must meet, in particular, obligations to inform.

4.5 Data Subjects are entitled under the statutory requirements to the right to request information on the processing of their Personal Data. In addition, the Data Subjects affected by the Collaboration can demand that the Controller correct, delete or restrict access to their data. In the cases regulated by law, the persons affected by the cooperation can object to the processing of their personal data by the person responsible at any time for reasons that arise from their particular situation.

The Parties agree that it is basically the responsibility of the Advertiser to answer appropriate enquiries from Data Subjects. It remains the central point of contact for the Data Subjects.

The Controller shall also clarify that the Data Subjects of the processing can assert their respective rights arising from or in connection with the processing of the Personal Data against each Controller. Art. 82 GDPR remains unaffected.

The Controller will take all necessary and appropriate steps to fulfil corresponding enquiries and claims in the name of the other Controller and to collaborate accordingly in this context. In each case, the Controllers must support each other appropriately.

4.6 Reporting obligations according to Art. 33 and 34 GDPR are fulfilled by the Controller where the reportable incident occurred. The Parties shall immediately inform each other in the event of a reportable incident with regard to the processing covered by the contract. The respective other Party shall support the Controller with the reporting obligation in the best possible way in clarifying the facts and in taking appropriate measures to protect the Data Subjects. The decision on the necessity, content and scope of the measures to be taken shall be made by the Controller with the reporting obligation.

4.7 In addition, the Advertiser is responsible for providing information to the Data Subject about the essential contents of the regulations according to PART B, if, and to the extent, that the Data Subject requests this and it is absolutely required under applicable law. In the event that the Data Subjects request appropriate information, the Controller will pass on this section of PART B to the Data Subject after prior coordination.

4.8 Each Controller shall maintain a directory of processing activities independently. The Controllers shall provide each other with the information required for maintaining a corresponding directory of processing activities.

4.9 The Controllers shall support each other in the appropriate scope, if necessary, in the creation of a data protection impact assessment and, if appropriate and insofar as legally permissible with the prior consultation with Supervisory Authorities. At the request of the other Controller, the other Controller must provide the required information and documents to the requesting party.

4.10 Each Controller shall bear its own costs incurred in the context of fulfilling the obligation in accordance with this PART B. The provisions of the General Terms and Conditions for the use of Affiliate Marketing Services remain unaffected by this.

5. Liability

The Controllers are liable to each other in accordance with the statutory provisions.

6. Conflict regulation

The regulations in the General Terms and Conditions concerning the use of Affiliate Marketing Services is superseded by this regulation to the extent that this Agreement provides for special regulations. Otherwise, the subsidiary applicability of the provisions for the use of the Affiliate Marketing Services remains.

PART B

APPENDIX 1: Roles, tasks and scope of the Collaboration between Advertiser and WBG

WBG provides an Affiliate Marketing Platform and concludes separate Agreements ("GTC") for its use with Advertiser and Publisher, respectively. The task of WBG is to enable the settlement of the sales brokered via the platform. The Publisher initiates this data processing by publishing advertisements provided by the Advertiser with a corresponding tracking code. This is done by forwarding the interested party to a landing page specified in advance by the Advertiser.

The data relevant for the invoicing of the Publisher's services is transmitted to the Advertiser based on contractual agreement to WBG, so that WBG can fulfil its contractual obligations. In addition, WBG proposes to the Advertiser suitable Publishers for the services/products offered by the Advertiser. For this purpose, WBG proposes Publishers according to the specifications of the Advertiser from WBG's data stock, which is presumably especially suitable for the marketing activities of the Advertiser. WBG also creates an overview for the Publisher of the items offered by the Advertisers via the platform with statements to what extent these products were sold. In this way the publisher can select the products / advertising materials that interest it.

In detail, the tasks are distributed as part of Joint Controller as follows:

Procedure	**Purpose / scope**	**Roles and tasks**	**Processing of / access to data categories / Data Subjects**
Transmission of data by Advertiser to WBG for the creation of invoices for Publishers / Advertiser and to store data for the fulfilment of tax and commercial retention obligations;	Provision of data on the sales brokered via the platform by Publishers for the creation of invoices against Advertiser/Publisher and fulfilment of tax and commercial obligations by WBG.	Advertiser: Transmission of data to WBG WBG: Processing of the data provided for the purposes specified.	Data Subject: Customer of the Advertiser who has concluded a contract due to the Publisher's brokerage: The following data is affected: • Contact details of the Advertiser, • Contact data of the agency (if available) • Advertiser ID • Agency ID • Program ID • Invoice data • Contract data • Publisher ID
Analysis of transaction data for the management and development of the platform as well as for misuse and fraud control	Use of data to detect misuse/fraud and – in anonymised form – for • Capacity planning, • Process optimisation • Creation of reports about the use of the platform and • Development of the platform.	WBG: Coordination of the data to be transmitted to WBG for the stated purposes (evaluation of the specified data). Advertiser: Transmission of data to WBG.	Data Subject: Customer of the Advertiser who has concluded a contract due to the Publisher's brokerage: The following data is affected: • Advertiser ID • Agency ID • Publisher ID • Program – ID • Program details (fee, override, commission) • Invoice data • Transaction data and transaction status • Timestamp
Reporting for Publisher	Preparation of reports for Publisher to verify sales and optimise own marketing activities	WBG: Coordination of the data to be transmitted to WBG for these purposes (creation of reports based on the data). Advertiser: Transmission of data to WBG.	Data Subject: Customer of the Advertiser who has concluded a contract due to the Publisher's brokerage: The following data is affected: • Invoice data • Voucher code • Transaction data and transaction status • Timestamp • Type of device used by the user • Device browser used • Number of clicks on advertisement • URL accessed by the user

Provision of recommendations for Advertiser with regard to potentially suitable Publishers	Selection of potentially suitable Publishers based on the items or services sold/offered by the Advertiser. Provision of an overview of the Publishers determined for the Advertiser.	WBG: Selection of the Publishers based on internal data and provision of reports/proposals to the Advertiser Advertiser: Coordination with WBG regarding criteria for selection of the Publishers and provision of the data	Data Subject: Publisher The following data is affected: • Publisher ID • Campaign ID • Item • Number of brokered items • Date of sale
Provision of recommendations for Publishers with regard to potentially suitable products	Display platform for Publishers which contain the products offered by the Advertiser via the WBG platform. This advertisement also contains statements regarding the extent to which these products have been sold. In this way the publisher can select the products / advertising materials that interest it.	Advertiser: Coordination with WBG regarding the selection of the Publishers and provision of the data Advertiser: Coordination with WBG regarding anonymisation of data for the creation of statistics	Data Subject: Customers of the Advertiser The following data is used: • Item • Date of sale • Number of product purchased

*****

Part C

JOINT CONTROLLER AGREEMENT
between

Advertiser and **Publisher**

Preamble

The use of the WBG platform for Affiliate Marketing requires a work-related collaboration of WBG with Publisher and Advertiser as well as a collaboration between Publisher and Advertiser relevant to the data protection law according to Art. 26 GDPR. The provisions of Part C JOINT CONTROLLER AGREEMENT apply to this collaboration of the Advertiser and Publisher. The Advertiser and Publisher shall grant each other access to specific Personal Data or collect and process them during the collaboration. This Agreement is also concluded in cases where Advertisers use certain Publishers for the placement of displays/advertising.

In **Appendix 1/1a** to this Agreement, the Parties specify the scope of the collaboration, mutual obligations of the Parties and their respective roles and responsibilities in regard to compliance with the respective data protection obligations.

1. Scope of Collaboration

As part of the collaboration, the Controllers will act as Joint Controller. The roles of the Controller and the associated tasks are specified in more detail in Appendix 1/1a. If one party is solely responsible for a data processing operation, this party will implement all relevant data protection provisions on its own responsibility. However, such data processing procedures are not subject to this Agreement.

Joint data processing and the type of Personal Data collected and processed within the framework of collaboration are specified in Appendix 1/1a.

2. Obligations of the Controller, Processors

2.1 The Controller carries out the processing of Personal Data in accordance with the relevant provisions of the applicable data protection laws. Both Parties and the Publisher are jointly responsible externally for compliance with the applicable data protection laws with regard to joint data processing. In the internal relationship, the scope of the responsibility for compliance with the applicable data protection laws arises from Appendix 1/1a where the Parties have been assigned individual data processing procedures.

2.2 The Controllers use the Personal Data within the framework of this Collaboration for the purposes as described in Appendix 1/1a. For further data processing beyond the joint responsibility, each Controller is solely accountable and must comply with the data protection law requirements independently.

Should the Parties process Personal Data for purposes other than those described herein, the Parties shall inform each other in the appropriate scope, provided this is mandatory by law.

2.3 The Data Controllers ensure that all persons who are involved in the processing of Personal Data are required and/or will be required to maintain confidentiality and will process personal data on instruction of the controller only.

2.4 Personal Data must be correct and, if necessary, up-to-date. The collection and processing of Personal Data must be restricted appropriately and considerably to the purpose as well as to the extent necessary for the purposes of transmission and further processing.

2.5 The Controller will only process Personal Data in accordance with the contract with the aid of Processors if an order processing agreement corresponding to the statutory requirements is concluded with the respective Processors. The Controller shall only disclose Personal Data to third parties to the extent this is actually required for fulfilling the obligations resulting from the Collaboration or is otherwise legally permissible and proper and the other Party is informed of the other recipients of the Personal Data.

3. Technical and organisational measures

Taking into account the state of the art, the implementation costs and the type, scope, circumstances, and the purposes of processing, as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons, the Controllers shall take appropriate technical and organisational measures to ensure an appropriate level of protection; these measures include, depending on individual case, the following:

- pseudonymisation and encryption of Personal Data;
- the ability to ensure, over the long-term, the confidentiality, integrity, availability and resilience of the systems and services in connection with processing;
- the ability to rapidly restore the availability of Personal Data and access to it upon the occurrence of a physical or technical incident;
- a procedure for regular review, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing.

4. Responsibility for compliance with data protection laws and rights of Data Subjects

4.1 As a rule, the Controller who has initially collected the Personal Data or has a direct contractual relationship with the Data Subjects is a central contact point for the Data Subjects. This is usually the Advertiser who is directly in contact with the customer and has collected its data for the conclusion of the contract.

4.2 Data Subjects are entitled to various rights with regard to the Personal Data processed by the Controller. The Controllers agree to fulfil their respective obligations in accordance with the provisions of the applicable data protection laws.

4.3 Data Subjects must be provided with information about the processing according to Art. 13 and 14 GDPR. The Parties agree that Publisher issues the information obligations vis-à-vis the Data Subjects for the data processing described in Part C, Appendix 1/1a. Furthermore, it is the responsibility of the Advertiser to provide all necessary information on the data processing activities listed in Part B Appendix 1 to the Data Subjects in a suitable manner in accordance with the procedure described below.

4.4 The Controllers support each other in the fulfilment of corresponding contractual and/or other statutory obligations and provide the necessary information on the relevant data processing activities in order to meet these requirements. WBG shall provide the Advertiser with separate data protection notices that will provide its end customers with information on the data processing activities carried out by WBG in the course of the use of Affiliate Marketing Services. Notwithstanding the provision of the above-mentioned data protection notices, the Advertiser remains responsible for complying with all legal obligations that it must meet, in particular, obligations to inform.

4.5 Data Subjects are entitled under the statutory requirements to the right to request information about the processing of their Personal Data. In addition, the Data Subjects affected by the Collaboration can demand that the Controller correct, delete or restrict access to their data. In the cases regulated by law, the persons affected by the cooperation can object to the processing of their personal data by the person responsible at any time for reasons that arise from their particular situation.

The Parties agree that it is basically the responsibility of the Advertiser to answer appropriate enquiries from Data Subjects. It remains the central point of contact for the Data Subjects.

The Controller shall also clarify that the Data Subjects of the processing can assert their respective rights arising from or in connection with the processing of the Personal Data against each Controller. Art. 82 GDPR remains unaffected.

The Controller will take all necessary and appropriate steps to fulfil corresponding enquiries and claims in the name of the other Controller and to collaborate accordingly in this context. In each case, the Controllers must support each other appropriately.

4.6 Reporting obligations according to Art. 33 and 34 GDPR are fulfilled by the Controller where the reportable incident occurred. The Parties shall immediately inform each other in the event of a reportable incident with regard to the processing covered by the contract. The respective other Party shall support the Controller with the reporting obligation in the best possible way in clarifying the facts and in taking appropriate measures to protect the Data Subjects. The decision on the necessity, content and scope of the measures to be taken shall be made by the Controller with the reporting obligation.

4.7 In addition, the Advertiser is responsible for providing information to the Data Subject about the essential contents of the regulations according to PART B, if, and to the extent, that the Data Subject requests this and it is absolutely required under applicable law. In the event that the Data Subjects request appropriate information, the Controller will pass on this section of PART B to the Data Subject after prior coordination.

4.8 Each Controller shall maintain a directory of processing activities independently. The Controllers shall provide each other with the information required for maintaining a corresponding directory of processing activities.

4.9 The Controllers shall support each other in the appropriate scope, if necessary, in the creation of a data protection impact assessment and, if appropriate and insofar as legally permissible with the prior consultation with Supervisory Authorities. At the request of the other Controller, the other Controller must provide the required information and documents to the requesting party.

4.10 Each Controller shall bear its own costs incurred in the context of fulfilling the obligation in accordance with this Agreement. The provisions of the General Terms and Conditions between the respective Parties and Webgains GmbH and the supplemental regulations for the use of Affiliate Marketing Services remain unaffected by this.

5. Liability

The Controllers are liable to each other in accordance with the statutory provisions.

6. Conflict regulation

The regulations in the General Terms and Conditions concerning the use of Affiliate Marketing Services to WBG is superseded by this regulation to the extent that this Agreement provides for special regulations. Otherwise, the subsidiary applicability of the provisions for the use of the Affiliate Marketing Services remains.

*****

Part C

<u>APPENDIX 1</u>: Roles, tasks and scope of collaboration between Advertiser and Publisher, provided it is commissioned by the Advertiser for the brokerage

WBG provides an Affiliate Marketing Platform and concludes separate Agreements ("GTC") for its use with Advertiser and Publisher. The task of WBG is to enable the settlement of the sales brokered via the platform. The Publisher initiates this data processing by publishing advertisements provided by the Advertiser via the Affiliate Marketing Platform with a corresponding tracking code. This is done by forwarding the interested party to a landing page specified in advance by the Advertiser.

The merchant transmits the data relevant for billing the publisher's services to WBG on the basis of a separate contractual agreement so that WBG can meet its contractual obligations. In addition, WBG proposes to the Advertiser suitable Publishers for the services/products offered by the Advertiser. For this purpose, WBG proposes Publishers according to the specifications of the Advertiser from WBG's data stock, which is presumably especially suitable for the marketing activities of the Advertiser.

In detail, the tasks are distributed as part of Joint Controller between the Advertiser and Publisher as follows:

Procedure	**Purpose / scope**	**Roles and tasks**	**Processing of / access to data categories / Data Subjects**
Forwarding of the user by Publisher after clicking on an advertisement of the Advertiser on the landing page linked in the advertising material	The Publisher uses the advertisements of the Advertiser furnished with a tracking code for advertising purposes ("Display"). After clicking on the display, the user is forwarded to the intended landing page	<u>Publisher:</u> Integration of the pixelated advertising material (ad) within the framework of own marketing measures and forwarding of the request after the click on advertising material to access the Advertiser's landing page <u>Advertiser:</u> Provision ad with script	Data Subjects: potential customers of advertiser The following data are affected: • IP address, • Referrer, • Browser type, • Call time (timestamp), • Program ID • Publisher ID • Probable ID • Event ID • Value • Reference ID

<u>APPENDIX 1a</u>: Roles, tasks and scope of cooperation between Advertiser and Publisher when booking the Post View Tracking service.

This APPENDIX 1a is in addition to APPENDIX 1: Roles, Responsibilities and Scope of Cooperation between Advertiser and Publisher of Part B - Joint Controller Agreement between Publisher and Advertiser.

WBG provides an affiliate marketing platform and concludes separate agreements ("GTC") for its use with Advertiser and Publisher respectively. The use of the WBG platform for affiliate marketing requires a cooperation based on the division of tasks between WBG, the Publisher and the Advertiser to the extent described below, as well as a cooperation between Publisher and Advertiser relevant under data protection law pursuant to Art. 26 GDPR.

In detail, the tasks within the framework of joint controllership are distributed as follows:

Procedure	**Purpose / Scope**	**Roles and tasks**	**Processing of / access to categories of data/ Data subjects**
Provision of tracking code for evaluation of user behaviour on the publisher's website	Creating the technical requirements for tracking / per order	<u>Advertiser</u>: WBG creates and transfers tracking code as contractor of the advertiser <u>Publisher</u>: recipient of the Tracking Code	Technical preparatory actions that do not include data processing
Activation of tracking code after delivery of the ad	Creating the technical requirements for tracking / per order	<u>Advertiser</u>: Initiation <u>Publisher</u>: Integration of Tracking Code into ad	Technical preparatory actions that do not include data processing
Collection of user data on the publisher's website after delivery of the ad	Measurement of success and effectiveness of an ad / after user-consent in each case	<u>Advertiser</u>: Principal for tracking activity <u>Publisher</u>: Client for tracking activity	Website visitors and interested parties of the advertiser who are shown ads on the publisher's website / User data • Click-ID • Programm-ID • Campaign-ID • Time stamp
Transfer of user data to advertisers	Measurement of success and effectiveness of an ad / after user-consent in each case	<u>Advertiser</u>: recipient of user data <u>Publisher</u>: Transmitter of user data	Website visitors and interested parties of the advertiser who are shown ads on the publisher's website / User data: • Click-ID • Programm-ID • Campaign-ID • Time stamp

*****