knipp

AGREEMENT FOR THE
DATA PROCESSING IN ACCORDANCE WITH ARTICLE 28 GENERAL DATA PROTECTION REGULATION (GDPR)
FOR REGISTRAR SERVICES

Customer: _____ Person: _____

_____ E-Mail: _____

Address: _____ Phone: _____

_____ Fax: _____

_____ Effective Date: _____

Customer No: _____

This contract is based on the model contract of *The German Association for Data Protection and Data Security e.V. (GDD)* and is adopted where needed.

This Agreement is made at the Effective Date specified above (the *Effective Date*) between the Customer specified above (henceforth called *Customer*) and Knipp Medien und Kommunikation GmbH (henceforth called *Knipp,* the Supplier), with offices located at Martin-Schmeisser-Weg 9, Technologiepark, Dortmund, Germany, acting on behalf of itself and its Affiliates.

1. DEFINITIONS

1.1 **Controller** means in this context the Customer.

1.2 **Processor** means Knipp as the Supplier of the services.

2. SUBJECT MATTER AND DURATION OF THE CONTRACT

2.1 **Subject Matter** of the Contract is defined and equal to the Service Agreement with Customer and its respective Amendments.

2.2 **The Duration** of this Contract corresponds to the duration of the Service Agreement and its respective Amendments.

3. SPECIFICATION OF THE CONTRACT DETAILS

3.1 The **Nature and Purpose** of Processing of personal data by the Supplier for the Customer are precisely defined in the Service Agreement. The undertaking of the contractually agreed Processing of personal data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of personal data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Customer and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. The adequate level of protection in these areas has been decided by the European Commission (Article 45 Paragraph 3 GDPR).

3.2 The **Type of Personal Data** includes the following, mainly compiled to contact handles:

(a) Person master data, versioned,
(b) Communication data (such as Phone, Email), versioned,
(c) Domain names,
(d) Auth codes,
(e) Links to each other.

3.3 The **Categories of Data Subjects** are registrants and administrators of domain names.

4. TECHNICAL AND ORGANIZATIONAL MEASURES

4.1 **Documentation.** Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of the Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Customer for inspection. Upon acceptance by the Customer, the documented measures become the foundation of the contract. Insofar as the inspection by the Customer shows the need for amendments, such amendments shall be implemented by mutual agreement.

4.2 **Security.** The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix A]

4.3 **The Technical and Organizational Measures** are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

5. RECTIFICATION, RESTRICTION AND ERASURE OF DATA

5.1 **Changes.** The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Customer, but only on documented instructions from the Customer.

Insofar as a Data Subject contacts the Supplier directly con-

cerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Customer.

5.2 **Erasure Policy.** Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Customer without undue delay.

6. QUALITY ASSURANCE AND OTHER DUTIES OF THE SUPPLIER

6.1 **Data Protection Officer.** In addition to complying with the rules set out in this Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular to have an appointed Data Protection Officer, who performs his duties in compliance with Articles 38 and 39 GDPR.

6.2 **Confidentiality** in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work.

6.3 Implementation of and compliance with all **Technical and Organizational Measures** necessary for this Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR. [Details in Appendix A]

6.4 **Cooperation.** The Customer and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

6.5 **Inspections.** The Customer shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

6.6 **Supervisory Authority.** Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Contract data processing by the Supplier, the Supplier shall make every effort to support the Customer.

6.7 **Permanent Monitoring.** The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

6.8 **Verifiability** of the Technical and Organizational Measures conducted by the Customer as part of the Customer's supervisory powers referred to in item 8 of this contract.

7. SUBCONTRACTING

7.1 **Subcontracting** for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Customers data, even in the case of outsourced ancillary services.

7.2 **Commision.** The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Customer. The consent is granted, of course, if the subcontractor is a registry or a reseller of a registry that provides exactly the registration service for a specific top-level domain.

8. SUPERVISORY POWERS OF THE CUSTOMER

8.1 **Inspections.** The Customer has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

8.2 **Verification.** The Supplier shall ensure that the Customer is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Customer the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

8.3 **Evidence** of such measures, which concern not only the specific Contract, may be provided by

(a) Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;

(b) Certification according to an approved certification procedure in accordance with Article 42 GDPR;

(c) Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor);

(d) A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI) or ISO/IEC 27001).

8.4 **Remuneration.** The Supplier may claim remuneration for enabling Client inspections.

9. COMMUNICATION IN THE CASE OF INFRINGEMENTS BY THE SUPPLIER

9.1 **Assistance.** The Supplier shall assist the Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

(a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

(b) The obligation to report a personal data breach immediately to the Customer.

(c) The duty to assist the Customer with regard to the Customer's obligation to provide information to the Data Subject concerned and to immediately provide the Customer with all relevant information in this regard.

(d) Supporting the Customer with its data protection impact assessment.

(e) Supporting the Customer with regard to prior consultation of the supervisory authority.

9.2 **Compensation.** The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

10. AUTHORITY OF THE CLIENT TO ISSUE INSTRUCTIONS

10.1 **Confirmation.** The Customer shall immediately confirm oral instructions (at the minimum in text form).

10.2 **Violation.** The Supplier shall inform the Customer immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Customer confirms or changes them.

11. DELETION AND RETURN OF PERSONAL DATA

11.1 **Copies or duplicates of the data** shall never be created without the knowledge of the Customer, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

11.2 **Hand Over / Destruction.** After conclusion of the contracted work, or earlier upon request by the Customer, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Customer or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

11.3 **Contract Duration.** Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Customer at the end of the contract duration to relieve the Supplier of this contractual obligation.

In Witness Whereof, each of the Parties hereto has caused the Agreement to be executed by its duly authorized representative.

Knipp Medien und Kommunikation GmbH		**Company Name**	
Print Name:	_____	Print Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____
Signature:	_____	Signature:	_____

knipp

Appendix A

TECHNICAL AND ORGANIZATIONAL MEASURES

A.1 CONFIDENTIALITY (Article 32 Paragraph 1 Point b GDPR)

A.1.1 *Physical Access Control*
No unauthorised access to Data Processing Facilities, ensured by keys, electronic door openers, facility security services and entrance security staff, alarm systems, CCTV Systems.
A.1.2 *Electronic Access Control*
No unauthorised use of the Data Processing and Data Storage Systems, ensured by passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data storage media.
A.1.3 *Internal Access Control*
No unauthorised Reading, Copying, Changes or Deletions of Data within the system, ensured by rights authorisation concept, need-based rights of access, logging of system access events.
A.1.4 *Isolation Control*
The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing.
A.1.5 *Pseudonymisation* (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.

A.2 INTEGRITY (Article 32 Paragraph 1 Point b GDPR)

A.2.1 *Data Transfer Control*
No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
A.2.2 *Data Entry Control*
Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

A.3 AVAILABILITY AND RESILIENCE (Article 32 Paragraph 1 Point b GDPR)

A.3.1 *Availability Control*
Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning.
A.3.2 *Rapid Recovery* (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR).

A.4 PROCEDURES FOR REGULAR TESTING, ASSESSMENT AND EVALUATION (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

A.4.1 *Data Protection Management;*
A.4.2 *Incident Response Management;*
A.4.3 *Data Protection by Design* and Default (Article 25 Paragraph 2 GDPR);
A.4.4 *Order or Contract Control*
No third party data processing as per Article 28 GDPR without corresponding instructions from the Customer, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.