Data Processing Agreement

Agreement on contract data processing on behalf according to Art. 28 General Data Protection Regulation (GDPR)

entered into by and between **Parking Customer**

- Controller - hereinafter referred to as **“Controller”**

and

Sedo GmbH

Im Mediapark 6B

50670 Cologne

- Processor - hereinafter referred to as **“Processor”**

- hereinafter referred to jointly as **“the Parties”** -

Preamble

This Agreement defines and sets out in detail the data protection obligations of the contracting Parties arising under this Agreement as described in the currently valid version of Processors' General Terms and Conditions for the Domain Parking Service (hereinafter referred to as "**GTC**" or "**Main Agreement**"). The Processor offers its customers (hereinafter referred to as "**Parking Customer**" or "**Controller"**) a domain trading platform on which the customers can monetize their domains, among other things. As part of this, personal data are processed by the Processor on behalf of the Controller to enable the Domain Parking Service. In view of the above, the present contract data processing agreement has to be concluded between the Parties in relation to the GTC in order to meet the requirements of the EU General Data Protection Regulation (hereinafter referred to as "**GDPR**").

Article 1 Definitions

(1) Meant by "**Parking Customer**" is a natural person or company registered at the Sedo platform and using the Sedo Parking Service based on the Sedo Domain Parking Terms and Conditions.
(2) Meant by **"personal data"** is information relating to an identified or identifiable natural person (person affected); deemed as being identifiable is a natural person who can be directly or indirectly identified, especially by way of being allocated an identifier such as a name, an identification number, location data, an online identifier or one or more particular features that are an expression of that person's physical, physiological, genetic, psychological, economic, cultural or social identity.
(3) Meant by **"processing"** is any process carried out with or without the help of automated procedures or any such series of processes in connection with personal data, such as collection, acquisition, organization, arrangement, storage, adjustment, modification, reading out, retrieval, use, disclosure through transmission, distribution or any other form of provision, matching, linking, restriction, deletion or destruction.
(4) Meant by "**the Controller**" is the natural or legal person, authority, institution or other body that makes the decision alone or together with others regarding the purposes and means of processing personal data ("Controller" within the meaning of Article 4 (7) of the GDPR and with interpretive consideration of Article 4 (7) of the [Data Protection Adaptation and Implementation Act] DSAnpUG EU/[Federal Data Protection Act] BDSG, as amended).
(5) Meant by the "**Processor**" is a natural or legal person, authority, institution or other body that processes personal data on behalf of the Controller.

Article 2 Subject matter and duration of the assignment

(1) The subject matter of this Agreement is the processing of personal data (hereinafter referred to as "Data") by the Processor for the Controller on its behalf and according to its instructions in connection with the Domain Parking Service in addition to the GTC.
(2) This Agreement shall enter into force on signature by both Parties and end as a rule with the termination of the underlying Main Agreement. The right to extraordinary termination remains unaffected.

Article 3 Provision of data by the Controller

(1) The Processor shall obtain access to the following data (through the Controller providing it with the data or enabling it to access the data) or the Controller shall allow the Processor to collect the following data:

a) Data types:

- IP address;
- Device ID;
- Cookie ID.

b) Group of persons affected:

- Internet users.

(2) The data shall be accessed or collected as follows:

As part of a normal internet connection, the Processor shall have access to the source IP as specified in an http header. The header is fed in by all proxies between the Contractor and the Processor.

Article 4 General remarks concerning the rights and obligations of the Controller

(1) The Controller shall inform the Processor without delay if the Controller detects errors or irregularities when inspecting the contract data processing or in any other way.

(2) When exercising its powers arising from this Agreement, the Controller shall respect the rights as well as the legal and other interests of the Processor.

Article 5 Dealing with the data and the Controller's right of instruction

(1) The Processor shall process the data exclusively within the context of the Agreement made and according to the Controller's instructions. It shall not use the data for any other purposes and, in particular, shall not be entitled to pass on the data it is provided with to any third parties. Copies and duplicates shall not be produced without the Controller's knowledge. This shall not apply to back-up copies for guaranteeing due and proper data processing.

(2) The Controller may, in individual cases, clearly define the specific contract data processing by means of instructions. The right to issue instructions shall be subject to the decision whether processing will take place and what data are to be processed by the Processor. The decision concerning the means of processing shall be taken solely by the Controller, though there shall be a contractual obligation to carry out the processing by particular means or in a certain

manner only after prior agreement between the parties, which also includes the corresponding consideration on the part of the Controller. The right to issue instructions shall not extend to the technical and organizational measures to be taken by the Processor. The limitations of this right are generally to be found in the provisions contained in this agreement.

(3) The Controller shall inform the Processor of instructions for the contract data processing in text form at least and also document the issuing of the same. The Controller shall direct its instructions to the Processor's management or a person expressly designated by such management as the recipient of instructions. Entitled to issue instructions are the Controller's management as well as any of the Controller's employees expressly authorized for this purpose.

(4) The Processor shall inform the Controller if any instruction given by the Controller infringes the applicable data protection law in the view of the Processor. The Processor shall be entitled to suspend the implementation of a disputed instruction until the Controller has reviewed such disputed instruction and confirmed the same to the Processor as an instruction to actually be carried out. This confirmation shall only be effective when it has been communicated in text form at the very least and the issue of it has also been documented by the Controller.

Article 6 Technical-organizational measures

(1) The Processor shall document the implementation of the required technical and organizational measures set out prior to the contract being awarded before the commencement of processing, especially with regard to the specific execution of the assignment and submit this to the Controller for inspection.

(2) The Processor shall provide the security pursuant to Article 28 (3) (c) and Article 32 of the GDPR, particularly in conjunction with Article 5 (1), (2) of the GDPR. In overall terms, the measures to be taken are those of data security and guaranteeing a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, extent and purposes of the processing have to be taken into consideration in this regard, as must the differing likelihood of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR [detail in **Annex 1**].

(3) The technical and organizational measures are subject to technical progress and further development. In this regard, the Processor shall be permitted to implement adequate alternative measures. The security level of the specified measures must be complied with. Significant changes must be documented.

Article 7 Correction, restriction and deletion of data

(1) The Processor may not correct, delete or limit the processing of the data processed on behalf of the Controller in an arbitrary manner

(2) Where included in the scope of services, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly according to the Controller's documented instructions.

Article 8 Quality assurance and other obligations of the Processor

In addition to complying with the provisions of this commission, the Processor also has statutory obligations in accordance with Articles 28 - 33 of the GDPR, guaranteeing compliance with the following guidelines and provisions in particular:

a) Written appointment of a data protection officer, who shall perform his/her work in accordance with Articles 38 and 39 of the GDPR.
The data protection officer can be contacted at any time electronically via dataprotection@sedo.de.

b) Observance of confidentiality pursuant to Articles 28 (3) (2) (b), 29, 32 (4) of the GDPR. When carrying out the work, the Processor shall only deploy staff who are committed to maintaining confidentiality and have been familiarized with the relevant data protection provisions. The Processor and any person with access to personal data who is under the authority of the Processor may only process such data in accordance with the instructions given by the Controller, including the competences granted in this agreement, unless they are obliged to perform such processing by law.

c) The Controller and the Processor shall, on request, work together with the supervisory authority in the performance of its duties.

d) Inform the Controller without delay with regard to control procedures and measures undertaken by the supervisory authority, insofar as these relate to the assignment. This shall also apply where the Processor is under investigation by a competent authority as part of administrative infringement or criminal proceedings in relation to the processing of personal data during a processing assignment.

e) Insofar as the Controller is subjected to inspection by the supervisory authority, to administrative infringement or criminal proceedings, to a liability claim by an affected person or a third party, or to any other claim relating to the contract data processing by the Processor, the Processor shall assist the Controller to the best of its ability and possibilities.

f) The Processor shall regularly monitor the internal processes as well as the technical and organizational measures in order to guarantee that the processing in its area of responsibility is carried out in accordance with the requirements of the data protection law in force and safeguard the protection of the affected person's rights.

Article 9 Subcontracting

(1) The Processor shall be allowed to have its services provided by third parties and to engage sub-processors.

(2) Meant by subcontracting within the meaning of this provision are those services directly relating to the provision of the principal service. This does not include ancillary services availed of by the Processor, e.g. in the form of telecommunication services, postal/transport services, maintenance and user services or the disposal of data carriers, as well as other measures to ensure confidentiality, availability, integrity and capacity of the hardware and software of data processing systems.

Article 10 Monitoring/supervision rights on the part of the Controller

(1) The Controller shall have the right to carry out inspections in consultation with the Processor or have these conducted by inspectors to be designated in individual cases. It shall have the right to convince itself that this agreement is being complied with by the Processor in the latter's business establishment by way of spot checks which shall, as a rule, be announced in good time beforehand.

(2) The Processor shall ensure that the Controller is able to convince itself that the Processor is meeting its obligations pursuant to Article 28 of the GDPR. The Processor undertakes to provide the Controller with the necessary information on request and, in particular, furnish proof of the implementation of the relevant technical and organizational measures.

Article 11 Notification in the event of infringements by the Processor

(1) The Processor shall provide the Controller with support and assistance with regard to complying with the obligations under Articles 32 -36 of the GDPR concerning the security of personal data, reporting of data breaches, data protection impact assessments and prior consultations. This shall include, among other things:

a) ensuring an adequate level of protection through technical and organizational measures that take account of the circumstances and purposes of the processing as well as the predicted likelihood and severity of any possible infringement of

rights through security breaches and facilitate the immediate detection of relevant violation incidents;

b) the obligation to report violations of personal data to the Controller without delay;
c) the obligation to support and assist the Controller vis-à-vis the affected person within the context of its obligation to provide information and provide the Controller with all relevant information in this regard without delay;
d) support the Controller in its data protection impact assessment;
e) support the Controller within the framework of prior consultations with the supervisory authority.

(2) The Processor shall be able to claim any remuneration for support provided that is not included in the description of services or cannot be ascribed to wrongdoing on the part of the Processor.

Article 12 Deletion and return of personal data

(1) No copies or duplicates of the data shall be made without the knowledge of the Controller. This does not include back-up copies where these are required to guarantee due and proper data processing, as well as data that are needed with regard to complying with statutory retention requirements.

(2) On completion of the work agreed under the contract or earlier at the request of the Controller - on termination of the Main Agreement at the latest –, the Processor shall hand over all documents coming into its possession, as well as processing and usage results produced and those data files relating to the contractual relationship to the Controller or destroy the same according to data protection requirements following prior approval. The same applies to test and waste material. The deletion log shall be submitted on request.

(3) Documentation serving as proof of due and proper data processing in accordance with the assignment shall be kept by the Processor after termination of the contract in accordance with the relevant retention periods. The Processor can relieve itself of this obligation by handing such documentation over to the Controller at the end of the contract.

Article 13 Miscellaneous

(1) Should any provision contained in this agreement prove to be ineffective, this shall not affect the validity of the remaining provisions. In the event of a provision proving to be ineffective, the Parties shall replace such provision with a new one coming closest to the intention of the Parties.

(2) Any changes, modifications or amendments to this agreement as well as collateral agreements must be in writing. This also applies to the waiving of this clause requiring the written form itself.

(3) The court responsible of the location of the Processor's registered office shall have sole jurisdiction for all disputes arising from and in relation to this agreement, subject to any exclusively statutory jurisdiction.

(4) German law applies.

Cologne, 27.06.2019 Sedo GmbH _____ Matthias Conrad, CEO _____ Barbara Stolz, CFO	Place, Date: Controller: Name: Company: Address: E-Mail: Login Name: Name, Position:

Annex 1: technical and organizational measures

I. Confidentiality (Art. 32 (1) (b) GDPR)

1. Physical access control

Physical access control is intended to prevent unauthorised persons from gaining access to the information processing systems of Sedo GmbH (hereinafter referred to as “Sedo”). The data centre used by Sedo guarantees a high level of protection through modern security technology and extensive property and data protection measures. Access to the data centre is restricted to a limited group of authorised employees.

1.1 Organisational measures

1.1.1 Access to the data centre

The data centre is operated by InterNetX GmbH (hereinafter referred to as “InterNetX”) and is subject to their security standards. These include:

- Access for Sedo or InterNetX employees only, in accordance with the current access list
- Access for authorised visitors. Authorisation is based on the existing access list for authorised employees.

2. Equipment access control

Equipment access control is intended to prevent intrusion by unauthorised persons into Sedo's information processing systems. For this purpose, technical and organisational measures have been implemented with regard to user identification and authentication.

2.1 Organisational measures

2.1.1 User and permission processes

Users who are to acquire rights to a system for the performance of their tasks must request those permissions via a formal user and permission process. User IDs and permissions are managed by the user and permission administration system. At a technical level, authorisation for issuing and removing access rights is granted via a ticketing system in which the procedure is documented. User permissions are blocked in the administration system as soon as the user leaves the company or if permissions are used without authorisation. Obsolete access rights are also deleted in the course of system diagnostics. On a technical level, each authorised user is restricted to a single user ID on the target system.

2.2 Technical measures

2.2.1 Authentication process

Access permissions are configured with as much granularity as possible, so that people only have access to what they need for their job function and for the performance of their tasks. The equipment access control processes apply to all Sedo employees.

All systems are protected by two-stage authentication processes (e.g. user ID and password) to prevent unauthorised access. If passwords are used as part of the authentication process, they must comply with the internal password policies for employees and systems. Passwords that do not meet the standards laid down in the policies are not allowed. The systems are automatically locked after a certain period of inactivity. In addition, accounts are automatically deactivated if their passwords are not changed. Three incorrect password entries result in automatic locking of the account to guard against brute force attacks.

Remote access to internal systems is only possible using authentication. Access to internal systems is granted only to devices owned and administered by Sedo.

3. Data access control

Data access control is intended to prevent unauthorised activities in Sedo's information processing systems by implementing measures for monitoring and logging access.

3.1 Assigning permissions

The systems have been configured so that regular access with administrative rights is restricted to authorised internal employees from secure network segments. Needs-based permission concepts were developed for this purpose, to define, monitor and log access rights. Permissions are always assigned according to the need-to-know principle. Depending on their authorisations, differentiated permissions are set up for users, subdivided according to roles and profiles. Other system authorisations require the setting of permissions in accordance with the user and permissions process that has been implemented.

3.2 Changes

Access rights can only be modified by system administrators once they have received approval from an employee's supervisor.

3.3 Removal

Removal of user permissions (e.g. after an employee has left the company) occurs promptly, or at the latest within one working day. Access rights are also deleted in the course of system diagnostics. In this way, obsolete access rights are cleaned up. User permissions are blocked in the administration system as soon as the user leaves the company, or if permissions are no longer required or are used without authorisation. Obsolete access rights, e.g. those that have been inactive over a longer period of time, are deleted in the course of system diagnostics.

4. Separability control

Separability control measures taken by Sedo include the separation of test and routine programs, separation using access rules, and file separation.

For example, all production systems must be operated separately from development and test systems. On a technical level, this is achieved by segmenting networks by means of an activated firewall policy. Test data must not be used in production environments.

II. Integrity (Art. 32 (1) (b) GDPR)

1. Transport control

Within the scope of transport control, measures are defined for the transport, transmission and transfer of personal data, and for their subsequent verification.

1.1 Organisational measures

1.1.1 Training in data secrecy

All Sedo employees are bound by data and business secrecy. These topics are also covered at regular intervals, in order to raise awareness.

1.1.2 Classification of information

All information must be classified according to its protection requirements. If information is confidential, it requires special handling. Confidential business information may be transferred via secure communication channels only (e.g. encrypted e-mails).

1.2 Technical measures

1.2.1 Access and transport protection

As a matter of principle, only authorised users may access systems that process personal data. Data is transferred exclusively by the system itself to authorised recipients via secure channels using strong encryption.

Access protection for systems with sensitive information is implemented at several levels: At file system, operating system and network levels. The protection mechanisms allow only specially authorised administrators to access each respective level.

To prevent data loss, all work-related data must be stored on servers. These data are regularly backed up in accordance with the defined backup concepts, in order to eliminate data loss as far as possible.

2. Input control

To ensure the traceability and documentation of data administration and maintenance, measures are implemented for subsequent verification of whether and by whom data have been input, changed or erased.

2.1 Logging

Compliance with the access control rules listed above forms the basis for input control of systems that process personal data. As a basic principle, the roles and rights concept distinguishes between system users, process users and personalised users. Sedo's systems log which users have made changes.

III. Availability and resilience (Art. 32 (1) (b) GDPR)

1. Availability control

All services of Sedo and its subsidiaries are highly sensitive in terms of their availability and must be protected against accidental destruction or loss. In this context, data backup and retention measures are implemented.

1.1 Organisational measures

1.1.1 Backup processes

All data are backed up at regular intervals, and backups are documented in a different location from the system being backed up. Backups do not leave Sedo's data centre, however. The access controls mentioned above are implemented for the protection of archives and backups. Access to the backup software is restricted to dedicated backup administrators. The frequency of data backups depends on

the criticality of the information and can be adapted to specific requirements. Functionality testing of data backups is partly automated and partly carried out at random by the system administrators responsible.

Recovery processes for various systems are tested at random.

The escalation channels required for emergencies and incidents have been operationally tested.

1.2 Technical measures

1.2.1 Firewall

Sedo's networks and systems are protected against hacker attacks by means of a firewall which is regularly maintained and kept up-to-date by authorised system administrators. The firewall rules are designed to allow only required services and to block all network traffic by default. All internet connections are protected by at least one firewall.

1.2.2 High availability and power supply

The requirement of high availability results in a network infrastructure designed for redundancy and fault-tolerance in almost all areas. Power is supplied by multiple, redundant power supplies. The data centre is equipped with an uninterruptible power supply.

1.2.3 Fire protection

The secure areas of InterNetX's data centre are protected against fire by a pressurised gas extinguishing system. In the event of a fire, the gas suppresses oxygen in the room, thereby depriving the fire of oxygen at the source. The servers are not affected by the extinguishing process and can continue to operate normally.

2. Rapid recovery (Art. 32 (1) (c) GDPR)

The recoverability of Sedo’s systems is determined by that of both the data and the systems themselves.

The data are protected by backups which can be used for automatic recovery (see Backup).

The systems are installed and configured automatically for easy and repeatable installation and recovery.

IV. A process for regular testing, assessment and evaluation (Art. 32 (1) (b) GDPR)

1. Data protection management

All Sedo employees are bound by data and business secrecy and are made sufficiently aware of data protection. The Data Protection Officer is responsible for ensuring compliance with legal data protection requirements. The Data Protection Officer carries our regular inspections, in the course of which he or she issues regular instructions to promote problem awareness. There are also occasional spot checks for compliance with data protection and data security measures.

2. Incident response management

Through employee training in data protection regulations, employees involved in data processing are instructed in how to handle any data protection requests. Due to the flat company hierarchy, any requests concerning data protection are immediately forwarded to the Data Protection Officer and, depending on the content, also to executive management and the CTO. All data protection requests are processed promptly.

3. Privacy by design (Art. 25 (2) GDPR)

In developing its services, Sedo respects the principle of privacy by design. All product managers have had training in this. In addition, a data protection reference document has been created for employees, which also addresses this topic and explicitly informs employees about it. This document is given to employees along with the Privacy Statement.

Sedo products are set up by default so that Sedo collects the necessary data to provide its contractual services. No further compulsory personal data will be collected.

4. Processing control

All instructions from the customer for handling personal data are documented and stored in a central location for the use of employees involved in data processing. Data processing is always based on a processing agreement agreed between the parties, where necessary in conjunction with the main contract. The supplier shall process data only within the scope of the agreement entered into. The purpose, type and scope of data processing shall be based solely on the customer's instructions. Any processing deviating from those instructions shall require notification from the customer.