Agreement on Commissioned Data Processing between

_____

_____

_____

– hereinafter "Controller"–

and

snapADDY GmbH
Haugerkirchgasse 7
DE - 97070 Würzburg
– hereinafter "Processor"–

§ 1 Subject of the Agreement and Term

(1) The Processor performs services for the Controller as described in Appendix 1. Appendix 1 details the subject-matter, type and purpose of processing, the types of data and categories of data subjects in compliance with Art. 28 para. 2 GDPR.

(2) This Agreement shall – unless otherwise agreed – become effective after it has been signed by both parties and shall apply as long as the Processor processes personal data on behalf of the Controller.

§ 2 Instructions of the Controller

(1) The Controller is responsible for compliance with the relevant data protection provisions, in particular for the admissibility of the data processing and for safeguarding the data subjects' statutory rights, stipulated by the GDPR. Statutory or contractual liability provisions shall remain unaffected.

(2) The Processor processes the personal data disclosed by the Controller solely under the instructions of the Controller and within the scope of the agreed services/stipulations. Data must only be corrected, erased or blocked subject the Controller's instructions.

(3) Unless processing of certain personal data is required by law of the European Union or a Member State to which the Processor is subject, the Processor must only process data under the Controller's instruction. In such a case, the Processor shall inform the Controller of that legal requirement prior to processing, unless that law prohibits such information on important grounds of public interest.

(4) The Controller's instructions require no specific form. Verbal instructions must be documented by the Controller. Instructions must be given in writing or in text form, if the Processor requires it.

(5) If the Processor believes that an instruction given by the Controller infringes upon data protection laws, he must inform the Controller of this without undue delay.

§ 3 Technical and Organizational Measures

(1) The Processor undertakes to employ adequate technical and organizational security measures for the data processing and to document these measures in Appendix 3. These security measures should be appropriate to the risks involved with the specific personal data processing operations.

(2) The measures that have been taken can be adapted to future technical and organizational developments. The Processor may only carry out these adaptions, if they satisfy at least the previous level of security. Where no other regulations exist, the Processor must only inform the Controller of substantial changes.

(3) The Processor shall support in his sphere of responsibility the Controller to comply with all legal obligations as far as the technical and organizational measures are concerned. The Processer shall, upon request, cooperate in creating and maintaining the Controller's record of processing activities. The Processor shall cooperate with the creation of a data protection impact assessment and if necessary with prior consultations with supervisory authorities. Upon request, the Processor shall disclose the required information and documents to the Controller.

§ 4 Obligations of the Processor

(1) The Processor confirms that he is aware of the relevant data protection regulations. The Processor's internal operating procedures shall, in his sphere of responsibility, comply with the specific requirements of an effective data protection management.

(2) The Processor guarantees that he has implemented appropriate technical and organizational measures, in a way that the processing is in compliance with the requirements of data protection law and the rights of data subjects.

(3) The Processor warrants and undertakes that all employees involved in the personal data processing procedures are familiar with the relevant data protection regulations. The Processor assures that those employees are bound to maintain confidentiality or are subject to an adequate legal obligation of secrecy. The Processor shall monitor compliance with the applicable data protection regulations.

(4) The Processor may only access the Controller's personal data if it is necessary for the purposes of carrying out the data processing.

(5) Insofar as it is legally required, the Processor shall appoint a Data Protection Officer. The Processor's Data Protection Officer's contact details are to be shared with the Controller for the purposes of making direct contact.

(6) The Processer may only process personal data provided to him exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another contracting state to the Agreement on the European Economic Area. Processing personal data in a third country requires prior explicit approval by the Controller and must meet the relevant legal requirements.

(7) The Processor supports the Controller with appropriate technical and organizational measures to ensure that the Controller can fulfill his existing obligations to respond to requests for exercising the data subject's rights, e.g. information and disclosure to the data subject, correction or erasure of data, restriction of processing or the right to data transferability and opposition. The Processor will nominate a contact person who will support the Controller in the fulfillment of legal obligations to provide information in connection with the data processing and will share this person's contact details with the Controller without undue delay. The Processor shall support the Controller, insofar as the Controller is subject to information obligations in the event of a data breach. Information may only be given to data subjects or to third parties with the prior instruction of the Controller. If a data subject exercises his or her data subject's rights directly in respect to the Processor, the Processor shall forward this request to the Controller without undue delay.

§ 5 Authority to Conclude a Subprocessing Agreement

(1) The Processor may only assign Subprocessors, after informing the Controller of every intended change in relation to the addition of or replacement of a Subprocessor in writing, whereby the Controller has the opportunity to veto the intended change within 2 weeks. The controller may only veto with good cause. If the objection cannot be remedied, the contracting partners have a special right of termination according to the general regulations of the relevant contract.

(2) A relationship shall be regarded as that of a Subprocessor when the Processor commissions other Processors in part or in whole for services agreed upon in this contract. Ancillary services that are provided to and on behalf of the Processor by third party service providers and that are determined to support the Processor to execute the assignment services, shall not be regarded as Subprocessors within the meaning of this Agreement. Such services may include, for example, provision of telecommunication services or facility management. However, the Processor is obliged to guarantee the protection and the security of the Controller's data in respect to third party service providers, and to ensure appropriate and legally compliant contractual agreements and supervisory measures are in place.

(3) A Subprocessor may only have access to the data once the Processor has ensured, by means of a written contract, that the regulations of this contract are also binding against the Subprocessor, and in particular adequate guarantees are provided that appropriate technical and organizational measures are carried out in a way so that the processing is compliant with data protection regulations.

(4) The commissioning of Subprocessors listed in Appendix 2 of this Agreement at the time of signature are deemed to be approved, provided that the requirements of § 5 Para. 3 of this Agreement are implemented.

§ 6 Controller's Right of Inspection

The Processor agrees that the Controller or a person authorized by him shall be entitled to monitor compliance with the data protection provisions and the contractual agreements to the extent necessary, in particular by gathering information and requests for relevant documents, the inspection of data-processing programs or accessing the working rooms of the Processor during the designated office hours after prior notice. Proof of proper data processing can also be provided by appropriate and valid certificates for IT security (e.g. IT-Grundschutz, ISO 27001), provided that the specific subject of certification applies to the commissioned data processing in the specific case. However, presenting a relevant certificate does not replace the Processor's duty to document the safety measures within the meaning of § 3 of this Agreement.

§ 7 Obligation to Report Data Protection Violations by the Processor

The Processor shall notify the Controller without undue delay about any disruption in operation which implicates menace to personal data provided by the Controller, as well as of any suspicion of data protection infringements concerning personal data provided by the Controller. The same applies if the Processor discovers that his security measures do not satisfy legal requirements. The Processor is aware that the Controller is obligated to document all breaches of the security of personal data and, where necessary, to inform the supervisory authority and/or the data subjects. If such breaches of the security of personal data occurred, the Processor will assist the Controller in complying with its reporting obligations. The Processor will report breaches to the Controller without undue delay and will provide, at a minimum, the following information:

a) A description of the nature of the breach, the categories and approximate number of data subjects and personal data records concerned,

b) Name and contact details of a contact person for further information,

c) A description of the likely consequences of the breach, and

d) A description of the measures taken for the remedy or mitigation of the breach.

§ 8 Termination of the Agreement

(1) On termination or expiration of this Agreement the Processor shall return or erase all personal data, provided there is no statutory duty to preserve records for retention periods set by law. Other personal data on backup systems will be deleted within 3 month.

(2) The Controller can terminate the contractual relationship without notice if the Processor gravely violates this Agreement or the legal provisions of data protection and the Controller can therefore not reasonably be expected to continue the data processing until the expiry of the notice period or the agreed termination of Agreement.

§ 9 Liability

The liability of the Processor for breaches of this contract shall be determined in accordance with the statutory provisions. In addition, the Controller shall indemnify the Processor against claims for damages by affected parties, unless the breach of duty giving rise to liability is attributable to the Processor.

§ 10 Final Provisions

(1) In case any of the Controller's property rights are at risk in the office premises of the Processor due to measures taken by third parties (e.g. through seizures or confiscation), insolvency proceedings or any other events, the Processor shall promptly inform the Controller hereof. The Processor waives the right of lien in respect to storage media and datasets.

(2) Any and all modifications, amendments and supplements to this Agreement must be in writing, and, following the 25.05.2018, can also be made in an electronic format.

(3) Should a provision of this Agreement become unenforceable, that shall not affect the validity or enforceability of any other provision of this Agreement.

_____	_____
Place, Date	Controller
Würzburg, 20.01.2020	
Place, Date	Processor

Appendix 1: List of Contracted Services and contact details of the data protection officers

Subject-matter of the Processing	The Controller uses the Software snapADDY CardScanner, snapADDY Grabber or snapADDY VisitReport for quick research, capture, completion and validation of addresses and contact information from various publicly available sources or business cards or for the registration of visit reports at fairs, events or at customer visits or conversations.
Nature and Purpose of the Processing	Electronic collection of data via PC or mobile devices (e.g. of business cards or of other sources), transmission of the data to CRM-systems or other processing systems, updating or validating existing data in processing systems.
Type of Personal Data	Last Names, First Names, Email addresses, Telephone numbers, Streets, House numbers, Postcodes, Places, Company, Compandy address (partly from business cards or other publicly available sources)
Categories of Data Subjects	Customers, suppliers, trade fair visitors, business partners, interested parties, applicants, employees of the client and the like

Name and contact details of the controller`s data protection officer (if designated)	
Name and contact details of the processor`s data protection officer (if designated)	datenschutz süd GmbH Dr. iur. Christian Borchers, Volljurist Geschäftsführer Telefon: +49 (0) 931 304 976 0 office@datenschutz-sued.de Wörthstraße 15 DE-97082 Würzburg

Appendix 2: List of Deployed Subprocessors including the Processing Sites

Subprocessor (Name, legal status, place of business)	**Processing site**	**Type of service**
Amazon Web Services Inc. 410 TerryAvenue North Seattle, WA 98109-5210 USA	AWS Region Frankfurt, Deutschland (eu-central-1)	Data center for server hosting
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland	europe-west3-Region, Frankfurt	Cloud services e.g. text recognition (OCR)

Appendix3: Technical and organisational measures pursuant to Art. 32 DSGVO

In the course of obtaining this information, the Contractor shall provide the Customer with the following information on the technical and organisational measures set up:

Confidentiality [Art. 32 para. 1 lit. b DSGVO]

a) Entry Control

Measures to deny unauthorized persons access to the server systems used to process or use personal data:

The data centers are staffed 24/7. Access to the security areas is protected by an electronic access control system with logging.
The output of keys for the office locking system for the employees is centrally managed, monitored and documented. The access areas are secured by video surveillance. Visitors must identify themselves at the reception and will only be guided to their contact persons in the respective areas if accompanied.

b) Access Control

Measures to prevent the use of data processing systems by unauthorized persons:

The data processing systems are protected in particular by anti-virus software, firewall systems (software) and proxy servers. The administration of the security software is regularly ensured and is carried out only by authorized personnel. The authorization of the personnel is ensured by assigned user rights or user profiles. These profiles can be used to log on to the respective IT systems using two-factor authentication. This is done using a username and password (at least 8 digits, 1 lowercase letter, 1 uppercase letter, 1 number) and a 6-digit one-time code, which is sent to the user's smartphone via an app or via SMS.
Access to data processing systems is via secure connections (e.g. SSL certificates). The electronic data traffic between client and contractor is secured by encryption technology.

c) Access Control

Measures which guarantee that those authorized to use a data processing system only access data subject to their access authorization and that personal data cannot be processed, used and stored without authorization, read, copied, changed or removed:

The assignment of rights is implemented according to the authorization concept and administration is the responsibility of the system administrators. The concept and the rights granted are subjected to an annual self-assessment and the procedure is monitored.

In principle, the number of administrators is limited to the "most necessary". To ensure that only authorized persons have access to data, data carriers and data are encrypted and access is regulated via user rights. Access to systems and applications is password-protected by two-factor authentication and depends on user rights - each employee can only access the functions necessary to perform his or her tasks within the scope of his or her area of responsibility. Illegal access to systems or data integrity via vulnerabilities in programs is prevented by regular monitoring of the infrastructure and immediate resolution of problems found. Both external and internal accesses are recognized and their effects minimized.
Customer data on the servers of the hosting service provider are stored AES256-encrypted and are therefore not readable by the hosting service itself.

d) Pseudonymization

Pseudonymization (Art. 32 para. 1 lit. a, Art. 25 para. 1 DSGVO) guarantees that identification features of personal data, insofar as this is necessary to protect the data subjects or is required from the point of view of data protection law, are replaced by identifiers for certain or identifiable persons and can therefore not be assigned to the data subject without additional information.

Consequently, data can no longer be attributed to a specific data subject without additional information. This additional information must be kept separately and be subject to appropriate technical and organizational measures.

Customer data on the servers of the hosting service provider are stored AES256-encrypted and are therefore not readable by the hosting service itself.

Integrity [Art. 32 para. 1 lit. b DSGVO]

e) Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers and that it is possible to check and establish to which points personal data is to be transmitted by data transmission devices:

The electronic data exchange is monitored by security systems, where all data is transmitted SSL-encrypted (TLS 1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES_128_GCM (cipher)). Unauthorized removal of data carriers in the data center is restricted by security areas and access control. Guidelines have been issued for the respective areas to prevent unauthorized removal of data carriers. Discarded data carriers will be destroyed according to specifications.
In addition, an authorization concept is used to assign rights to enter, change and delete data on the servers. All employees are contractually bound to data secrecy.

f) Input Control

Measures to ensure that it can be subsequently verified whether and by whom personal data have been entered, modified or removed in data processing systems:

The restrictive assignment of rights by individual users restricts the entry, modification or removal of personal data in data processing systems. Every entry, modification and removal of data is recorded.

Availability [Art. 32 Par. 1 lit. b DSGVO]

g) Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss:

To limit accidental destruction or loss during job-related data processing, a backup & recovery concept was created, implemented and the recovery was regularly tested. The data backups are stored in a secure, outsourced location. An uninterruptible power supply (UPS) is used to ensure regular and safe operation of the systems even in the event of faults in the power grid. The server room is secured by various monitoring and alarm systems, in particular devices for monitoring temperature and humidity as well as fire and smoke detection systems.

Control measures [Art. 32 para. 1 lit. d, Art. 25 para. 1 DSGVO]

h) Order Control

Measures to ensure that personal data processed on behalf of the contracting authority can only be processed in accordance with the contracting authority's instructions:

The Processor shall process the data submitted in accordance with the contract concluded and shall comply with the statutory provisions and requirements defined by contract within the framework of the instructions of the Controller. This contractually excludes the disclosure of data to unauthorized third parties and defines the framework of instructions. The mandatory contents of § 28 DSGVO are also taken into account in the determination. The Processor shall allow the client to inspect the documentation of the "technical/organizational measures" in advance or, if necessary, to inspect the data processing equipment on site. A possible examination of the Processor as well as his activities

carried out in the context of data processing is thereby made possible and supported by the Processor.

i) Separation requirement

Measures to ensure that data collected for different purposes can be processed separately:

The separation requirement is ensured by logical client separation on the software side. Test environments are managed independently of the production system - customer data is not transferred to these test systems.

j) Data security management

Procedures to ensure regular review, analysis and evaluation of the effectiveness of technical and organizational measures:

The security measures described are regularly reviewed, analyzed and evaluated and adapted to the technical standard in order to ensure the effectiveness of the technical and organizational measures.

k) Privacy-friendly presetting

Measures to prevent unauthorized or unlawful data processing by presetting data processing for a specific purpose. The amount of data collected, the scope of processing, the storage period and accessibility must be taken into account. In particular, measures must be taken to prevent personal data from being made available automatically (without human intervention) to an indefinite number of natural persons:

By default settings and warnings within the products, the user is instructed on how to use them in compliance with data protection regulations. In addition, the access possibilities are personalized and password-protected.

l) Risk management

Procedures for determining the risk to the rights and freedoms of natural persons and needs-based analysis of the appropriate level of protection, taking into account the state of the art, implementation costs, the nature, scope, circumstances and purposes of processing and the different likelihoods and severity of the risk.

The risks to the rights and freedoms of natural persons are continuously examined and evaluated and the level of protection is adjusted accordingly if necessary.

Status: January 2020