PERSONAL DATA PROCESSING AGREEMENT

between the following parties:

1.

Name: ....

Registration number / VAT ID:.....

Address: .....

Signed by: .....

Signature: .....

(hereinafter as **"Controller")**

and

2. Name: **Smartsupp.com, s.r.o.** Reg. no : 03668681, VAT ID : CZ 03668681

Address : Milady Horakove 13, 602 00 Brno, Czech Republic

Signed by: Petr Janosik Signature: .....

(hereinafter as **"Processor")**

The Controller and the Processor are collectively referred to as the "**Parties**" and individually as a "**Party**".

The Parties hereto make this Agreement on Data Processing with the following content:

1. DEFINITIONS

1.1 For the purpose of this Agreement:

1.1.1 **Agreement** means this agreement and all underlying appendices;

1.1.2 **Directive** means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) when this takes effect;

1.1.3 **Data subject** means the identified or identifiable natural person to whom Personal data relates;

1.1.4 **Personal data** means any information relating to an identified or identifiable natural person as defined in the Article 4 of the Directive, mainly any such information disclosed by the Controller to the Processor for purpose of Processing;

1.1.5 **Processing** or **Data processing** means any operation or set of operations which is performed on Personal data or on sets of Personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction as defined in the Article 4 of the Directive;

1.1.6 **Terms** means Terms of Service available on the Processor´s website www.smartsupp.com/terms to which the Controller has agreed by accessing or using the service for which the Controller has signed up;

1.1.7 **Primary Service** means non-exclusive SaaS (software as a service) licence provided by the Processor to the Controller as described in the Terms;

1.1.8 **Data Retention Period** means a time frame for how long are data of the Controller, including Personal data, stored by the Processor. Data Retention Period depends on the Primary Service purchased by the Controller as further described in the Terms.

1.1.9 **Instructions** means any documented instructions issued by the Controller to the Processor in alignment with Terms, this Agreement and the Directive as to the nature, scope and method of Data processing.

2. BACKGROUND AND PURPOSE

2.1 The Parties have agreed to the provision of the Terms, which governs the Controller's limited, non-exclusive and terminable right to the use of the Primary Service.

2.2 In this connection, the Processor processes Personal data on behalf of the Controller and by Controller's Instructions, and for that purpose the Parties have entered into this Agreement in accordance to the Article 28 of the Directive.

2.3 The purpose of this Agreement is to ensure that the co-operation of the Processor and the Controller in the field of Processing of Personal Data of Data subjects complies with the Directive.

3. APPOINTMENT AND INSTRUCTIONS

3.1 The Processor is authorised by the Controller to process Personal data disclosed to Processor by the Controller on behalf of the Controller on the terms and conditions set out in this Agreement.

3.2 The Processor may only process Personal data subject to the Instructions, including with regard to transfers of Personal data to a third country or an international organisation, unless required to

do so by Union or Member State law to which the processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 All Instructions shall comply with the Directive and any other applicable law and the Processor reserves the right to refuse any Instruction noncompliant with the Directive or any other applicable law or if such Instruction, in Processor's opinion, infringes the Directive or other Union or Member State data protection provisions. In such case Processor may postpone the execution of such and Instruction and shall immediately inform the Controller.

3.4 This Agreement, including appendices, constitutes the complete and final Instructions for the Processing of Personal Data for purpose an in scope as set in this Agreement and in connection with Primary Service.

3.5 Any change of any Instruction shall be done by written and by both Parties signed amendment to this Agreement only. Before any changes are made to the Instructions, the Parties shall to the widest possible extent discuss and, if possible agree on, the implementation of the changes, including time and costs of implementation.

3.6 The Processor may process Personal Data outside the scope of the Instructions in cases where required by EU law or national law to which the Processor is subject.

3.7 If Personal Data are processed outside the scope of the Instructions, the Processor shall notify the Controller of the reason. The notification must be made before processing is carried out and must include a reference to the legal requirements forming the basis of the processing.

3.8 Notification should not be made if such notification would be contrary to EU law or national law.

3.9 By this Agreement Controller thereby appoints Processor to process Personal data disclosed to him by the Controller on behalf of the Controller in scope as is necessary to provide Primary Service or otherwise subsequently agreed to by the Parties in writing.

4. DURATION

4.1 The Agreement applies until either (a) termination of the Agreement(s) on provision of the Primary Service or (b) termination of this Agreement.

4.2 Regardless of the termination of the Processor Agreement, clause 13 of the agreement regarding confidentiality as well as clauses 9, 10 and 11 will remain in force after termination of the Processor Agreement.

5. DATA PROCESSING

5.1 The Processor shall process Personal Data on behalf of the Controller solely for the purpose of providing Primary Service within the scope and for the purpose specified in Appendix 1 of this Agreement.

5.2 Subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects are specified in Appendix 1 of this Agreement.

5.3 Personal Data of EU Data subjects processed on behalf of the Controller by the Processor will be processed exclusively within European Union. Only exception is processing of Personal Data by

Mandrill specified in Appendix 3 point 1.3, where the Personal Data are processed in the USA under EU-US Privacy Shield.

5.4 All Personal Data processed on behalf of the Controller by the Processor will be processed under appropriate technical and organisational security measures as specified in the Article 6.1. of this Agreement.

5.5 If a Data subject applies directly to the Processor to request the access, rectification, restriction, erasure or portability of Data Subject's Personal Data, or if Data Subject objects to the Processing, or its right not to be subject to an automated individual decision making, the Processor shall forward such request to the Controller immediately.

5.6 The Processor shall not rectify, erase or restrict any Personal data processed on behalf of the Controller without documented Instruction of the Controller or unless Data Retention Period expires. The Processor shall not rectify, erase or restrict any Personal data processed on behalf of the Controller even if such Instruction is given in case any Union or Member State law requires storage of the such Personal data.

5.7 The Processor shall not use any Personal data disclosed by the Controller for the Processing under this Agreement for any other purpose than specified in Appendix 1.

5.8 The Processor shall not disclose such Personal data to third parties, except sub-processors authorized by the Controller, specified in appendix 3 of this Agreement.

5.9 The Processor shall not make any copies or duplicate Personal data disclosed to him by the Controller without authorization of the Controller, except such copies or duplicates are part of backups described in the Terms or are required by the the Directive or other Union or Member State law (i.e. statutory retention rules).

5.10 The Processor shall upon end of provision of Primary Service, completion of contractual work as laid down in the Terms and this Agreement, or when requested by the Controller (mainly by the Instruction) delete all Personal data and delete existing copies unless Union or Member State law requires storage of the personal data.

5.11 The Processor shall not transfer Personal Data to third countries or international organisations unless specifically stated in this Agreement.

5.12 The Processor has appointed Data Protection Officer (hereinafter as "DPO"), who shall perform duties in compliance with the Directive. The DPO can be contacted at dpo@smartsupp.com.

6. PROCESSOR'S OBLIGATIONS

6.1 Technical and organisational security measures

6.1.1 The Processor is responsible for implementing necessary technical and organisational measures to ensure an appropriate security level. The measures must be implemented with due regard to the current state of the art, costs of implementation and the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity to the rights and freedoms of natural persons. The Processor shall take the category of Personal data described in appendix 1 into consideration in the determination of such measures.

6.1.2 Processor has implemented the technical and organisational security measures as specified in appendix 2 to this Agreement.

6.1.3 The Processor shall implement the suitable technical and organisational measures in such a manner that the processing by the Processor of Personal data meets the requirements of the applicable Personal data regulation.

6.1.4 Should the Processor implement any new technical or organizational security measures in the meaning of this Article, especially in connection with improvement and development of the Primary Service, technical progress and development of technical and organizational security measures, changes in the organization of the Processor, changes in any applicable law etc., the specification in the appendix 2 will be updated if necessary. Any change in the technical or organizational security measures must not reduce the level of technical or organizational security measures as specified at the date of signature of this Agreement.

6.1.5 The Parties agree that the provided safeguards and all technical and organisational measures to ensure an appropriate security level of Personal data as specified in appendix 2 are adequate at the date of conclusion of this Agreement.

6.2 **Employee conditions**

6.2.1 The Processor shall ensure that employees who process Personal Data for the Processor have undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

6.2.2 The Processor shall ensure that access to the Personal data is limited to those employees for whom it is necessary to process Personal data in order to meet the Processor´s obligations to the Controller under the Terms.

6.2.3 The Processor shall ensure that employees processing Personal Data for the Processor only process such data in accordance with the Instructions.

6.3 **Documentation for compliance with obligations**

6.3.1 Upon written request, the Processor shall document to the Controller that the Processor:

a) meets its obligations under this Agreement and the Instructions.

b) meets the provisions of the Directive, in respect of the Personal data processed on behalf of the Controller.

6.3.2 The Processor's documentation must be provided within reasonable time.

6.4 **Records of processing activities**

6.4.1 The Processor shall maintain a record of the processing of Personal data.

6.4.2 The record must include the following information:

a) Categories of processing carried out on behalf of the Controller.

b) Processors' employees who process the Personal data.

c) If relevant, Sub-Processors who process the Personal data.

d) A general description of technical and organisational measures in connection with the processing.

e) If relevant, specification of third countries or international organisations to which the personal data are transferred as well as documentation for appropriate safeguards.

f) Contact details of the Processor's and Sub-Processor's contact person or Data processing adviser (if appointed).

6.4.3 Upon request, the Processor shall make the records available to the Controller or any relevant supervisory authority within reasonable time.

6.5 **Security breach**

6.5.1 The Processor shall notify the Controller of any Personal data breach, which may potentially lead to accidental or unlawful destruction, alteration, unauthorised disclosure of, or access to, Personal data processed by the Processor for the Controller (hereinafter as "Security Breach").

6.5.2 Security Breaches must be reported to the Controller without undue delay.

6.5.3 The Processor shall maintain a record of all Security Breaches. The record must as a minimum document the following:

a) the actual circumstances of the Security Breach;

b) the effects of the Security Breach; and

c) the remedial measures taken.

6.5.4 Upon written request, the record must be made available to the Controller or the supervisory authorities.

6.6 **Audits and Inspections**

6.6.1 The Processor allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

6.6.2 Any audit or inspection by the Controller or auditor mandated by the Controller may be carried out by prior consultation with the Processor. In such consultation duration, scope, subject and date and time of the respective audit or inspection must be mutually agreed.

6.6.3 The right of audit or inspection stipulated in this Agreement does not extent to any facilities operated by sub-processors, sub-contractors or any third party, even if used in connection with providing Primary Service or Data Processing.

6.6.4 Any audit or inspection by the Controller or auditor mandated by the Controller may be carried out only to verify compliance of the Data Processing carried out by the Processor with this Agreement, the Directive or other applicable law.

6.6.5 All information and documents disclosed by the Processor to the Controller in connection with audit or inspection are part of Processor’s trade secret and are subject to the confidentiality as stipulated in clause 13, if not stipulated otherwise. Such information and documents may be disclosed only to the authorized supervisory authority.

6.7 **Assistance**

6.7.1 The Processor shall to the necessary and reasonable extent assist the Controller in the performance of its obligations in the processing of the Personal Data covered by this Agreement, including in connection with:

a) responses to Data subjects on exercise of their rights, especially data subject's rights laid down in Chapter III of the Directive;

b) ensuring compliance with the obligations of the Controller pursuant to Articles 32 to 36 of the Directive taking into account the nature of processing and the information available to the Processor;

c) Security Breaches;

d) impact assessments;

e) prior consultation of the supervisory authorities,

6.7.2 In this connection, the Processor shall obtain the information to be included in a notification to the supervisory authority provided that the Processor is best suited to do so.

6.7.3 The Processor is entitled to payment for time spent and materials consumed for assistance pursuant to clause 6.7.

6.7.4 Appropriate technical and organisational measures implemented by the Processor in order to assist the Controller with the fulfilment of his obligation to respond to requests for exercising the data subject's rights (right of access by the data subject, right to rectification, right to erasure, right to restriction of processing, right to data portability, Right to object and automated individual decision-making) laid down in Articles 15 to 22 of the Directive are specified in appendix 2 of this Agreement.

7. CONTROLLER'S OBLIGATIONS

7.1 Lawfulness of processing

7.1.1 The Controller shall ensure and guarantees that during the whole duration of this Agreement:

7.1.1.1 all Personal Data disclosed by the Controller to the Processor for Processing anyhow related to the Primary Service were collected by legal and legitimate manners according to the Directive, or any other applicable law;

7.1.1.2 consent of the Data Subject is given for Processing of the respective Personal data by the Processor, such consent is given freely and in accordance to the Article 7 of the Directive and that the consent is valid for the whole time of Processing and was not withdrawn by the Data subject;

7.1.1.3 other conditions of lawful processing according to the Article 6 of the Directive apply if consent of the Data Subject was not given;

7.1.1.4 no Personal data falling into special category of Personal data as specified in the Article 9 of the Directive were disclosed to the Processor.

7.1.2 In case any condition stipulated in the clause 7.1.1. is not met at any time of the Data Processing by the Processor or during the duration of this Agreement, Controller must

notify the Processor in the most expedient time possible under the circumstances and without reasonable delay and, where feasible, not later that 72 hours after having become aware of such deficiency. Controller also must exclude such Personal Data from Processing by himself (mainly by erasing such Personal Data from the Controllers Primary Service) and if not possible provide to Processor all necessary assistance to except such Personal Data from Processing.

7.2 **Employee conditions and third parties**

7.2.1 The Controller shall ensure that employees who process Personal data and have access to the Primary Service on behalf of the Controller undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

7.2.2 The Controller shall ensure that any third party having access to the Primary Service on behalf of the Controller undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

7.2.3 The Controller is fully liable to the Processor for the performance of any employee or third party to whom access to Primary Service is given by the Controller.

7.3 **Documentation for compliance with obligations**

7.3.1 Upon written request, the Controller shall document to the Processor that:

a) Controller meets its obligations under this Agreement and the Terms;

b) Controller meets the provisions of the Directive or other applicable law, in respect of the Personal Data disclosed to Processor;

c) Data Subject's consent is valid and was given for Processing of the respective Personal Data by the Processor**,** such consent was given freely and in accordance to the Article 7 of the Directive.

7.3.2 The Controller 's documentation must be provided within reasonable time.

7.4 **Security breach**

7.4.1 The Controller shall notify the Processor of any Security Breach as stipulated in clause 6.5.1.

7.4.2 Security Breaches must be reported to the Processor without undue delay.

7.4.3 The Controller shall maintain a record of all Security Breaches. The record must as a minimum document the following:

d) the actual circumstances of the Security Breach;

e) the effects of the Security Breach; and

f) the remedial measures taken.

7.4.4 Upon written request, the record must be made available to the Processor or the supervisory authorities.

7.5 **Assistance**

7.5.1 The Controller shall to the necessary and reasonable extent assist the Processor in the performance of its obligations in the processing of the Personal Data covered by this Agreement, including in connection with:

a) responses to data subjects on exercise of their rights, especially data subject's rights laid down in Chapter III of the Directive;

b) Security Breaches;

c) impact assessments;

d) prior consultation of the supervisory authorities,

7.5.2 In this connection, the Controller shall obtain the information to be included in a notification to the supervisory authority provided that the Controller is best suited to do so.

8. SUB-PROCESSORS

8.1 The Processor may only use a third party ("Sub-Processor") for the processing of Personal data for the Controller provided that it is specified in Appendix 3 of this Agreement.

8.2 The Processor and the Sub-Processor(s) have concluded a written agreement imposing the same data protection obligations on the Sub-Processor as those of the Processor (including in pursuance of this Agreement) as referred to in paragraph 3 of the Directive regarding Data processing, ensuring protection of processed Personal data and compliance with the Directive, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Directive. Sub-processor also acts only under the Instructions of the Controller as stated in this Agreement.

8.3 The Processor reserves right to change or add Sub-Processors. The Processor shall notify the Controller of any such event. The notification shall be done at least 30 days prior to the event. If the Controller doesn't agree to the new Sub-Processor, he has the right to terminate the Primary Service immediately and is entitled to a refund for the remaining paid period of the Primary Service.

8.4 All communication with the Sub-Processor is handled by the Processor, unless otherwise specifically agreed.

8.5 The Processor is directly responsible for the Sub-Processor's processing of Personal Data in the same manner as had the processing been carried out by the Processor.

9. FEES AND COSTS

9.1 The Parties are only entitled to payment for the performance of the Primary Service in accordance with Terms, unless otherwise stipulated in this Agreement.

10. BREACH

10.1 The regulation of breach in the Terms on delivery of the Primary Service also applies to this Agreement as were this Agreement an integral part thereof. If this is not considered in the Terms on delivery of the Primary Service, the general remedies for breach laid down in applicable law will apply to this Agreement.

11. LIABILITY AND LIMITATION OF LIABILITY

11.1 The Parties are liable according to the general rules of applicable law, however, Smartsupp.com, s.r.o. is liable according to the scope set out in the Terms.

12. FORCE MAJEURE

12.1 The Processor cannot be held liable for situations normally referred to as force majeure, including, but not limited to, war, riots, terrorism, insurrection, strike, fire and natural disasters.

12.2 Force majeure may only be asserted for the number of working days for which the force majeure situation lasts.

13. CONFIDENTIALITY

13.1 Information regarding the content of this Agreement, the underlying Primary Service or the other Party's business which is either, in connection with the disclosure to the receiving Party, designated as confidential information, or which, by its nature or otherwise, should be considered as confidential, must be treated as confidential and subject to at least the same degree of care and discretion as the Party's own confidential information. Data, including Personal data, are always confidential information.

13.2 However, the duty of confidentiality does not apply to information, which is or becomes publicly available without this being the result of a breach of a Party's duty of confidentiality, or information, which is already in the possession of the receiving Party without any similar duty of confidentiality or information, which is developed independently by the receiving Party.

14. TERMINATION

14.1 Termination for cause or breach

14.1.1 The Agreement may only be terminated according to the provisions on termination in the Terms or this Agreement.

14.1.2 Termination of this Agreement is subject to – and allows for – simultaneous termination of the parts of the Terms that concern Personal Data processing pursuant to the Agreement.

14.2 Effects of termination

14.3 The Processor's authority to process Personal Data on behalf of the Controller lapses on termination of the Agreement for whatever reason.

14.4 The Processor may continue to process Personal Data for up to three months after the termination of this Agreement to the extent that this is necessary to take the required statutory measures. The Processing by the Processor during this period is assumed to comply with the Instructions.

14.5 The Processor is obliged to delete all Personal Data disclosed by the Controller until 3 months from the termination of the Agreement. The Controller may request adequate information for such deletion.

14.6 The Processor never processes any Personal Data, which the Controller doesn't have himself, as all Personal Data are always passed to the Processor from the Controller.

15. FINAL PROVISIONS

15.1 The regulation of dispute resolution specified in the Terms, including governing law and venue, also applies to this Agreement as were this Agreement an integral part thereof.

15.2 Natural person concluding and accepting this Agreement on Processor's website www.smartsupp.com (hereinafter as “Natural Person”) hereby declares that he or she acts on behalf of the Controller and is legally authorized to act on behalf of the Controller in the matter of this Agreement. If such legal authorization of the Natural Person will be found as invalid then this Agreement is binding for the Natural Person and Natural Person is fully responsible to fulfill all obligations stated in this Agreement.

15.3 The Parties affirmatively declare that actions of the Parties made under the conditions agreed in this Agreement create the rights and duties for the Parties leading to creation of the legal relations between the Parties as assumed by the Agreement. The Parties also declare that all rights and duties and the agreed matters are considered definite adequately and capable to call the legal effects and impacts assumed by this Agreement. Provisions under the preceding phrases are valid even if actions of the Parties do not meet all prerequisites assumed by the binding legal regulations. In this case the Parties shall agree and meet such prerequisite without undue delay.

15.4 The rights and duties following from or connected to this Agreement may not be ceded or transferred anyhow by any Party without the prior written approval of the other Party.

15.5 Communication of the Parties concerning the Agreement (incl. Security Breach notification) shall be led through following email addresses

a) Processor : dpo@smartsupp.com

b) Controller : email address used to sign up for the Primary Service

15.6 Smartsupp.com, s.r.o. reserves the right to change or update this Agreement without further notice. By continuing to access or use Primary Service after those revisions become effective, you agree to be bound by the revised Agreement. If you do not agree to the new Agreement, please stop using the Primary Service. The latest version of this Agreement, which is legally in effect, can always be found at www.smartsupp.com/dpa.

APPENDIX 1

NATURE, SCOPE, DURATION AND PURPOSE OF PERSONAL DATA PROCESSING

1. NATURE, SCOPE, DURATION AND PURPOSE OF PERSONAL DATA PROCESSING

1.1 **Nature of processing**: Personal data are processed in an automated way via a script of the Processor that the Controller inserts into his website(s). The script loads a chat box on Controller's website(s) where the script is inserted. The chat box is part of the Primary Service. Visitors of the Controller's website(s) may enter personal data in the chat box when they need to contact the Controller for customer support. Additional personal data of visitors may also be tracked in the background by the script itself. The Controller can import additional Personal data for processing via API of the Processor or by using integrations with 3rd party services as part of the Primary Service.

1.2 **Scope of processing:** Depending on how the Controller is using the Primary Service, particularly following types of Personal data may be processed in connection with the delivery of the Primary Service:

a) browsed pages on the Controller's website and referring URL

b) date and time of visits to the Controller's website

c) technical information as screen resolution, operating system, browser type and device type

d) geolocation data (country and city)

e) IP address

f) first name and/or last name

g) email address

h) phone number

i) Additional types of Personal Data depend on Controller's use of the Primary Service

1.3 The Controller shall NOT disclose to the Processor any Personal data falling into special category of Personal data as specified in the Article 9 of the Directive. Also the Controller shall not use the Primary Service in a way that would demand or motivate Data Subjects to provide such Personal data. Example of such data types:

a) information about race and/or religious beliefs

b) information about sexual behavior and/or sexual preferences

c) sensitive medical information and/or information about health and illnesses

d) sensitive information as passwords, credit card numbers etc.

1.4 **The categories of processing** of registered identified or identifiable natural persons covered by this Agreement:

a) visitors of Controller's website(s) where the Primary Service is used

1.5 **Duration of processing:** All processed Personal data are automatically deleted according Data Retention Period based on the purchased Primary Service.

1.6 **Purpose of the processing** is for the Controller to:

a) provide and improve customer service to his website visitors

b) gather feedback from visitors about his products or services

c) improve user experience on his website

2. OPTIONS TO LIMIT PERSONAL DATA PROCESSING AND IMPROVE PRIVACY OF USERS

2.1 As part of the Primary Service, the Processor offers the Controller following options to limit processing of Personal data and to improve privacy of Data Subjects. All options are accessible in Controller's account on www.smartsupp.com, which is part of the Primary Service.

a) Processor gives notice to visitors of Controller's website about Personal Data processing in the chat box and allows the Controller to link the notice to the Controller's website where the Controller shall provide visitors with necessary legal information about Personal Data processing via the Primary Service.

b) Processor allows the Controller to set Data Retention Period - period for how long are data about visitors saved by the Processor

c) Processor allows the Controller to disable tracking of IP addresses of visitors. Tracking of IP addresses is disabled by default and the Controller needs to explicitly enable it.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1.1 The Processor implemented following technical security measures to maximize protection of Personal data:

a) SSL/TLS encryption (secure sockets layer / transport layer security) for all data transfers in all parts of the Primary Service

b) Processor's website and web software runs on secured https protocol

c) Processor offers the Controller multiple options to limit processing of Personal data and improve privacy of Data subjects, described in point 2.1 in Appendix 1.

d) All employees of the Processor with access to Personal data have signed a confidentiality agreement with the Processor

e) the Processor appointed a Data Protection Officer to ensure that Personal data are protected. The DPO can be contacted at dpo@smartsupp.com.

1.2 The Processor is using servers and cloud infrastructure of VShosting and Amazon Web Services to store Personal Data (see Appendix 3 - Sub-processors).

1.3 Information about security of Amazon Web Services:

a) Information about security of Amazon Web Services

aws.amazon.com/security

b) Information about physical security of Amazon AWS data centers:

aws.amazon.com/compliance/data-center/controls

c) Information about GDPR compliance of Amazon Web Services:

aws.amazon.com/compliance/gdpr-center

1.4 Information about security of VShosting:

a) Information about security of VShosting data center:

www.vshosting.eu/datacenter-serverpark

b) Information about certifications of VShosting:

www.vshosting.eu/certifications

1.5 The Controller can manage and delete any Personal data in his account used to access the Primary Service at www.smartsupp.com. This allows the Controller to meet his obligations regarding requests of Data subjects for Personal data information or deletion.

APPENDIX 3

SUB-PROCESSORS

1. SUB-PROCESSORS

1.1 The Controller hereby approves that the Processor uses following Sub-Processors to process Personal data:

a) Amazon Web Services EMEA SARL, 5 rue Plaetis, L-2338 Luxembourg

b) VShosting s.r.o., VAT ID CZ61505455, Sodomkova 1579/5, 102 00 Prague, Czech Republic

c) CDN77, operated by DataCamp Limited, 207 Regent Street, London, Great Britain

d) Mandrill (part of Mailchimp), operated by The Rocket Science Group LLC, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA

1.2 The Processor is using CDN77 as content delivery network. CDN77 is processing solely IP addresses of data subjects and storing them for 2 days. CDN77 is a back-end service used in the Processor's infrastructure and is used solely for optimization of transfer and loading of data necessary for operation of the Primary Service.

1.3 The Processor is using Mandrill for delivery of transactional emails such as offline emails and chat transcripts sent to/from Data Subjects. For these purposes Mandrill is processing email addresses of data subjects and stores them for 30 days (90 days if the emails bounce, meaning there is technical issue with delivering the email). Mandrill also stores contents of the transactional emails being sent. Mandrill is a back-end service used in the Processor's infrastructure and is used solely for optimization of sending transactional emails necessary for operation of the Primary Service. Mandrill is processing Personal Data in the USA under EU-US Privacy Shield.

1.4 The Controller accepts that the Processor uses standard Microsoft and Google software (e.g. MS Office and Google Docs) and that due to this, Google and Microsoft may process Personal data on behalf of the Controller.