Personal Data Processing Clauses

1. Definitions

"Affiliate" means in relation to Customer, another entity that presently or in the future, directly or indirectly, whether by itself or through one or more intermediaries, controls, is controlled by, or is under common control with Customer; Where "control" means: (i) beneficial ownership of at least fifty percent (50%) of the voting securities of a corporation or other business organization with voting securities, by contract, as trustee or executor, or otherwise, or (ii) a fifty percent (50%) or greater share in the profits and/or capital of a partnership or other business organization without voting securities.

"Data controller" means the entity that executed the Service Agreement together with its affiliates (for so long as they remain Affiliates) which have signed Order Forms.

"Customer Data" means what is defined in the Service Agreement as "Customer Data" or "Your Data".

"Data Protection Law of Republic of Serbia" means Law on Personal Data Protection ("Official Gazette of RS" no 87/2018)

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United.

"Member State Law" means all laws and regulations, including laws and regulations of the Republic of Serbia, European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under this Clause as amended from time to time.

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations and Data Protection Law of Republic of Serbia), where for each (i) or (ii), such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"Data processor" means the Things Solver which Processes Personal Data on behalf of the Controller.

"Public Authority" means a government agency or law enforcement authority, including judicial authorities.

"Service Agreement" Subscription Agreement to which this Data Protection Agreement ("DPA) represents integral part.

"Sub-processor" means any Processor engaged by Things Solver

"THINGS SOLVER" means Things Solver d.o.o. Beograd, Milutina Milankovića 19, 11 000 Belgrade, Republic of Serbia.

2. Preamble

2.1. The Parties have entered into a Subscription Agreement for the provision of Services ("Service Agreement") to which this Data Protection Agreement ("DPA and or Agreement") represents integral part. In the course of providing the Services etc as defined in Service Agreement it may be necessary for the Things Solver to process certain data on behalf of Data controller.

2.2. These Contractual Clauses (the Clauses) set out the rights and obligations of the Data controller and the Data processor, when processing personal data on behalf of the Data controller.

2.3. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of GDPR add Article 45 of Data Protection Law of Republic of Serbia.

2.4. In the context of the provision of the Service Agreement, the Data processor will process personal data on behalf of the Data controller in accordance with the Clauses.

2.5. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.6. Three appendices are attached to the Clauses and form an integral part of the Clauses:

- Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
- Appendix B contains list of sub-processors authorized by the Data controller.
- Appendix C contains the minimum security measures to be implemented by the Data processor and how audits of the Data processor and any sub-processors are to be performed.

2.7. The Clauses along with appendices represents the integral part to the Service Agreement.

2.8. The Clauses shall not exempt the Data processor from obligations to which the Data processor is subject pursuant to GDPR, Data Protection Law of Republic of Serbia or other legislation.

3. The rights and obligations of the Data controller

3.1. The Data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR, the applicable EU or Member State data protection provisions, Data Protection Law of Republic of Serbia and the Clauses.

3.2. The Data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. The Data controller shall be responsible, among other, for ensuring that the processing of personal data, which the Data processor is instructed to perform, has a legal basis.

4. Instructions

4.1. The Data processor shall process personal data only on documented instructions from the Data controller, unless required to do so by Data Protection Law of Republic of Serbia or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2. The Data controller undertakes to issue instructions to the Processor regarding the processing of personal data in written form, as well as that it will be clear, precise and in all respects in accordance with the applicable regulations.

4.3. The Data processor shall immediately inform the Data controller if instructions given by the Data controller, in the opinion of the Data processor, contravene the Data Protection Law of Republic of Serbia, GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1. The Data processor is obliged to ensure that only persons who need access to personal data, in order to fulfill the obligations of the Data processor towards the Data controller, have access to such data.

5.2. The Data processor is obliged to ensure that the private individual who is authorized to perform personal data processing activities with the Data processor is obliged to keep the data confidential or that that person is subject to legal obligation to keep the data confidential. The need for persons to have access to personal data will be reviewed from time to time, and if it is established that a person has ceased to need access to such data, they will be denied access.

5.3. The Data processor shall at the request of the Data controller demonstrate that the concerned persons under the Data processor's authority are subject to the abovementioned confidentiality.

5.4. Notwithstanding the previous provisions of this Article, the Data processors have the right to disclose any personal data at the request of a court or other state body or Public Authority in the exercise of their powers prescribed by Member State Law, with the obligation to immediately notify the Data controller, as well as to consult with the Data controller, to the extent to which it is possible, on the scope and form of data disclosure.

6. Security of processing

6.1. The Parties shall implement appropriate protection measures in order to achieve an appropriate level of security in relation to risk, in accordance with the level of technological achievements and costs of their application, nature, scope, circumstances and purpose of processing, as well as the probability of risk occurrence and risk level for rights and freedoms of private individuals as defined in Article 32 to the GDPR and/or Article 42 to the Data Protection Law of Republic of Serbia.

6.2. The Parties are obliged to separately assess the probability of occurrence of risk and the level of risk regarding the rights and freedoms of private individuals, as well as to determine appropriate protection measures to reduce the assessed risk, and the Data controller is bound to provide all information to the Data processor so that the Data processor would be able to fulfill this obligation of theirs.

6.3. Where necessary, the safety measures referred to in this Article of the Clause shall in particular include:

    6.3.1. pseudonymization and crypto protection of personal data;

    6.3.2. ensuring lasting confidentiality, integrity, availability and resilience of processing systems and services;

6.3.3. ensuring the re-availability and access to personal data in the event of physical or technical incidents as soon as possible;

6.3.4. conducting regular testing, evaluation and assessment of the effectiveness of technical, organizational and personnel security measures of processing.

6.4. When assessing the appropriate level of security referred to in paragraph 1 of this Article, special account shall be taken of the risks of processing, in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

6.5. The parties are obliged to take measures in order to ensure that any private individual authorized by the Data controller or Data processor to access personal data processes that data only upon the order of the Data controller or if required by Member State Law.

6.6. If subsequently - in the assessment of the Data controller - mitigation of the identified risks require further measures to be implemented by the Data processor, than those already implemented by the Data processor pursuant to Article 32 GDPR or Article 42 to the Data Protection Law of Republic of Serbia, the Data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1. The Data processor may entrust the processing to a sub-processor only if the Data controller authorizes them to do so on the basis of a general or special written authorization. If the processing is entrusted on the basis of a general authorization, the Data processor is obliged to inform the Data controller about the intended selection of the sub-processor, i.e. the replacement of the sub-processor, so that the Data controller has the opportunity to provide the opinion on such a change.

7.2. If the Data processor appoints a sub-processor to perform special processing operations on behalf of the Data controller, the Data processor is obliged to ensure that the same personal data protection obligations established by this Clauses apply to the sub-processor, based on a special agreement or other legally binding act concluded or adopted in written form, which includes electronic form, which in the relationship between the Data processor and sub-processor determines sufficient guarantees for the application of appropriate protection measures ensuring that the processing is performed in accordance with the member State Law and provisions of this Clause.

7.3. The Data processor is obliged to include in the agreement or other legally binding act concluded with the sub-contractor a provision which enables the Data controller to, in case of termination of the Data processor, for any reason, have the right to request the sub-contractor to destroy or return personal data that are the subject of that agreement or other legally binding act.

7.4. If it entrusts the processing to a sub-processor, the Data processor must be able to indicate that the sub-processor has been engaged in everything in accordance with the provisions of this article of the Clauses.

7.5. If the sub-processor does not fulfill its obligations regarding the protection of personal data, the Processor is responsible to the Controller for fulfilling the obligations of the sub-processor.

8. Transfer of data to third countries or international organizations

8.1. Any transfer of personal data to third countries or international organizations by the Data processor shall only occur on the basis of documented instructions from the Data controller and shall always take place in compliance with Chapter V GDPR or Chapter V Data Protection Law of Republic of Serbia.

8.2. In case transfers to third countries or international organizations, which the Data processor has not been instructed to perform by the Data controller, is required under EU or Member State law to which the Data processor is subject, the Data processor shall inform the Data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3. Without documented instructions from the Data controller, the Data processor therefore cannot within the framework of the Clauses:

    8.3.1. transfer personal data to a Data controller or a Data processor in a third country or in an international organization

    8.3.2. transfer the processing of personal data to a sub-processor in a third country

    8.3.3. have the personal data processed in by the Data processor in a third country

8.4. If, in the performance of the Services, Personal Data that is subject to the GDPR or any other Member State Law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of Europe, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the member State Law and Regulations of Europe:

8.5. The EU Controller-to-Processor Transfer Clauses. Where Data controller is a controller and a data exporter of Personal Data and Data processor is a processor and data importer in respect of that Personal Data, then the Parties shall comply with the EU Controller-to-Processor Transfer Clauses. For Data controllers in Republic of Serbia Standard contractual clauses issued by Commissioner authority ("Official Gazette of RS" no 05/2020) are to be applied on and/or

8.6. The EU Processor-to-Processor Transfer Clauses. Where Data controller is a Processor acting on behalf of a controller and a data exporter of Personal Data and Data processor is a processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of the EU Processor-to-Processor Transfer Clauses.

9. Assistance to the Data controller

9.1 Taking into account the nature of the processing, the Data processor shall assist the Data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of the Data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR or Chapter III Data Protection Law of Republic of Serbia.ž

9.2 This entails that the Data processor shall, insofar as this is possible, assist the Data controller in the Data controller's compliance with:

    a) the right to be informed when collecting personal data from the data subject

    b) the right to be informed when personal data have not been obtained from the data subject

    c) the right of access by the data subject

    d) the right to rectification

    e) the right to erasure ('the right to be forgotten')

    f) the right to restriction of processing

    g) notification obligation regarding rectification or erasure of personal data or restriction of processing

    h) the right to data portability

    i) the right to object

    j) the right not to be subject to a decision based solely on automated processing, including profiling.

9.3 If the data subject submits to the Data processor a request for exercising a right prescribed by applicable regulations, and for whose actions the Data controller is responsible, the Data processor is not authorized to act upon such request of that person, but is obliged to immediately inform the Data controller and forward such a request to them, as well as to inform the person who submitted the request that it has been forwarded to the Data controller.

9.4 In case of termination of the Data controller, the Data processor is obliged to act upon the requests of the data subject, unless there is a legal successor of the Data controller, which assumes the rights and obligations of the Data controller from this Clauses.

10. Notification of personal data breach

10.1 In case of any personal data breach, the Data processor shall, without undue delay after having become aware of it, notify the Data controller of the personal data breach.

10.2 The Data processor's notification to the Data controller shall, if possible, take place within 48 hours after the Data processor has become aware of the personal data breach to enable the Data controller to comply with the Data controller's obligation to notify the personal data breach to the competent supervisory authority.

10.3 The Data processor shall submit to the Data controller a notice of personal data violation containing the following data:
   a) date and time of the data security violation (if known, or as assessed);
   b) description of the nature of personal data violation, the type of data and the approximate number of persons to whom that data type relate, as well as the approximate number of personal data whose security has been violated;
   c) name and contact details of the Personal Data Protection Officer or information on other manner in which information on the violation can be obtained
   d) description of possible consequences of the violation;
   e) description of the measures taken or proposed by the Processor in connection with the violation, including measures taken to mitigate the harmful consequences.
   f) other data of importance for notification of data violation.

10.4 If all this information cannot be provided at the same time, the Data processor shall, without undue delay, progressively provide the Data controller with the available information, which must be documented.

11. Erasure and return of data

11.1 After the completion of the agreed processing operations, the Data processor is obliged, based on the decision of the Data controller, to delete or return to the Data controller all personal data and delete all copies of these data, unless the law prescribes the obligation to keep the data.

11.2 The Data processor must be able to present to the Data controller the fulfillment of its obligation from the previous paragraph of this article.

11.3 If the Data controller does not take over the personal data within 15 days from the date of termination of the Service Agreement or does not provide the Data processor with a decision to delete the personal data in accordance with the provisions of paragraph 11.1. the Data processor shall erase the personal data and at the request of the Data controller, it will submit the appropriate proof/statement of the deletion.

12. Audit and inspection

12.1 The Data processor shall make available to the Data controller all information necessary to demonstrate compliance with the obligations laid down in GPPR and/or Member State Law and the Clauses and allow for and contribute to audits, including inspections, conducted by the Data controller or another auditor mandated by the Data controller.

12.2 The Processor shall enable the Data controller (at its request) to supervise the resources used for the processing of personal data, in relation to the processing activities prescribed by this Clauses and in accordance with the audit conditions defined in the Service Agreement.

12.3 The Data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data controller's and Data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data processor's physical facilities on presentation of appropriate identification.

13. Liability

13.1 In the event that it did not act in accordance with the obligations prescribed by the applicable law directly related to it or that it acted outside the instructions or contrary to the instructions of the Data controller, issued in accordance with the law, the Data processor is obliged to compensate the Data controller for damages in accordance with limitations of damage compensation defined by the Service Agreement so that the total amount of damages under the Service Agreement and this Agreement may not exceed the limits defined in the Service Agreement.

13.2 Notwithstanding the limit defined in the previous paragraph, the Data processor shall be liable for all damages paid by the Data controller to private individuals based on a final court decision, provided that the damage occurred due to the fact that the Data processor did not act in accordance with the applicable law directly related to the Data processor or it acted outside the instructions or contrary to the instructions of the Data controller, issued in accordance with applicable law.

13.3 The Data controller is obliged to immediately, without delay, inform the Data processor about the request of private individuals for compensation for damage for which the Data processor may be responsible. The Data controller and the Data processor are obliged to jointly take all available legal measures in order to defend themselves against the requests of private individuals and are liable for damages due to failure to act in accordance with the obligations defined in this paragraph.

14. Commencement and termination

14.1 The Clauses shall become effective on the date of the Data controllers first access to the service under Service Agreement and shall be concluded for the period of processing and the execution of the Service Agreement.

14.2 The conditions of termination, the notice period, as well as the consequences in case of termination defined by the Service Agreement shall apply to these Clauses

14.3 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data controller pursuant, the Clauses may be terminated by written notice by either party.

15. Data processor contact point

15.1 The Data controller may contact Data processor using the following contact:
- for Data processor: dpo@thingsolver.com

16. Final provision

16.1 The Parties agree that the relevant provisions of Service Agreement shall apply to all matters not defined in these Clauses.

Appendix A - Information about the processing

The subject of processing (fill in):

Processing of personal data using the Solver Al Suite software in order to perform the services defined in the Service Agreement.

The nature and purpose of processing (fill in):

Collecting, recording, classifying, grouping, i.e. structuring, storing, adapting and using data, automated or non-automated with the use of special software for the implementation of the Data controller's online sales program.

Types of data subjects (fill in):

Clients of Data controller

Types of personal data (fill in)

as specified at: https://docs.thingsolver.com/data-models/overview.html

Location of processing:

- Belgrade – Republic of Serbia and Frankfurt - Federal Republic of Germany

Special types of personal data (fill in if applicable):

- Not applicable

Appendix B - Authorized sub-processors

- INFOBIP SERBIA d.o.o - channels infrastructure services (SMS, Viber, WhatsApp, Email, Push Notifications)
- Amazon Web Services EMEA S.a r.l. – hosting services and channels infrastructure services (SMS, Email, Push Notifications)

Appendix C: Security measures

1)   technical measures:
Configured HTTP traffic between the server and end users to use SSL encryption (HTTPS) of data during communication. Adequate protection of user authentication and authorization is provided during access. Precise and careful definition of data structure, privileges and rights granted to users.

2)   organizational measures:
The Rulebook on the Protection of Personal Data at the Processor regulates the internal procedure and organization that ensures the protection of personal data processed by the Processor, personal data protection measures, access to personal data, rights, obligations and responsibilities in connection with data processing, and other issues of importance and which represent the legal obligations of the Processor related to the processing of personal data based on the authorization of the Controller.

3)   personnel measures:
The Rulebook on the organization and systematization of work at the Processor, and the employment contracts with the employees of the Processor, clearly define which employees have access to personal data, as well as their obligations and responsibilities related to the processing of personal data when performing work tasks for the Processor, including the obligation to keep data confidential and the prohibition of using data outside the purpose for which the Processor processes it.