

Data Processing Addendum

The Trafft Data Processing Addendum (“**DPA**”), that includes the Standard Contractual Clauses adopted by the European Commission attached hereto as Exhibit I, if applicable, as well as the Standard Contractual Clauses adopted by the Commissioner for information of public importance and personal data protection of the Republic of Serbia attached hereto as Exhibit II, if applicable, is incorporated into and is an integral part of our Terms of Use available at <https://trafft.com/terms-of-service/> (the “**Agreement**”).

We periodically update these terms. If you are an active Client, we will let you know when we do via an email or in-app notification.

The term of this DPA shall follow the term of the Agreement. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

“**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (and for the purposes of this DPA, means the Client).

“**Data Protection Law**” means: a) the Personal Data Protection Act; and/or b) the GDPR when Standard Contractual Clauses adopted by the European Commission apply.

The terms “process”, “processes” and “processed” will be construed accordingly.

“**Data Subject**” means the individual to whom Personal Data relates.

“**GDPR**” means the General Data Protection 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.

“**Instruction**” means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available). The parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools) constitute Client’s documented instructions regarding TMS’ processing of Client Data (“**Documented Instructions**”). TMS will process Client Data only in accordance with Documented Instructions.

“**Personal Data**” means any information relating to an identified or

Data Processing Addendum

identifiable individual where such information is contained within Client Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Personal Data Protection Act" means the Personal Data Protection Act of the Republic of Serbia ("*Official Gazette of the Republic of Serbia*", no. 87/2018);

"Processing" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

"Processor" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller (and for the purposes of this DPA, means TMS).

"Standard Contractual Clauses adopted by the European Commission" means the clauses attached hereto as Exhibit I pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Standard Contractual Clauses adopted by the Serbian Commissioner" means the clauses attached hereto as Exhibit II pursuant to the Decision on Standard Contractual Clauses ("*Official Gazette of the Republic of Serbia*", no. 5/2020).

"Sub-Processors Page" means TMS' Sub-Processors list available in Section 7 of the Privacy Policy available at <https://trafft.com/privacy-policy/>.

2. Details of the Processing

- (a) **Categories of Data Subjects.** Controller may submit Personal Data to the Service, the extent of which is determined and controlled by Controller in its sole discretion, and which may include, but is not limited to any personal data provided by any Employee, as well as any personal data provided to the Client by Customer for the purpose of providing Client's Services in accordance with Agreement.
- (b) **Types of Personal Data.** To the extent of which is determined and controlled by the Controller in its sole discretion and the extent to which Controller

Data Processing Addendum

decides to use functionalities of Trafft, we process Client Data such as scheduling on-site or virtual appointments, meetings & events with the Customers, managing staff and services, accepting payments, sending reminders to Customers and Employees.

- (c) **Subject-Matter and Nature of the Processing.** The subject-matter of Processing of Personal Data by Processor is the provision of the Services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement.
- (d) **Purpose of the Processing.** Personal Data will be Processed for purposes of providing the Services set out, as further instructed by Controller in its use of the Services, and otherwise agreed to in the Agreement.
- (e) **Duration of the Processing.** Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. Controller's Responsibility

Within the scope of the Agreement and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA is Client's complete and final instruction to TMS in relation to Personal Data and that additional instructions outside the scope of DPA would require prior written agreement between the parties. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions including via an email (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

4. Obligations of Processor

- (a) **Compliance with Instructions.** The parties acknowledge and agree that Client is the Controller of Personal Data and TMS is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable law, Processor will

Data Processing Addendum

- i. promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and
 - ii. cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new Instructions with which Processor is able to comply.
 - iii. If this provision is invoked, Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable Services until such time as the Controller issues new Instructions in regard to the Processing.
- (b) **Security.** Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Annex II to Exhibit I and Appendix 3 to Exhibit II. Such measures include, but are not limited to:
- i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems,
 - ii. the prevention of Personal Data Processing systems from being used without authorization,
 - iii. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization,
 - iv. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified,
 - v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems,
 - vi. ensuring that Personal Data is Processed solely in accordance with the Instructions,
 - vii. ensuring that Personal Data is protected against accidental destruction or loss.

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data by

- i. implementing and maintaining the security measures described under Annex II to Exhibit I and Appendix 3 to Exhibit II,
- ii. complying with the terms of Section 4.c. (Personal Data Breaches); and
- iii. providing the Controller with information in relation to the Processing in accordance with Section 6 (Audits).

Data Processing Addendum

- (c) **Personal Data Breaches.** Processor will notify the Controller without undue delay but within no more than 72 hours after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

Unsuccessful Security Incidents. Client agrees that an unsuccessful Security Incident is one that results in no unauthorized access to Client Data or to any of TMS' equipment or facilities storing Client Data, which include but does not limit to: pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

Notification(s) of Security Incidents, if any, will be delivered to one or more of Client's administrators by any means TMS selects, including via email. It is Client's sole responsibility to ensure Client's administrators maintain accurate contact information on the TMS management console and secure transmission at all times.

- (d) **Deletion or Retrieval of Personal Data.** Other than to the extent required to comply with Data Protection Law, following termination or expiration of the Agreement, Processor will delete or return all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller.

5. Data Subject Requests

Processor will enable Controller to respond to requests from Data Subjects to exercise their rights under the applicable Data Protection Law in a manner consistent with the functionality of the Service. To the extent that Controller does not have the ability to address a Data Subject request, then upon Controller's request Processor shall provide reasonable assistance to the Controller to facilitate such Data Subject request to the extent able and only as required by applicable Data Protection Law. Controller shall reimburse Processor for the commercially reasonable costs arising from this assistance.

Data Processing Addendum

Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests.

6. Audits

Processor shall, in accordance with Data Protection Laws and in response to a reasonable written request by Controller, make available to Controller such information in Processor's possession or control related to Processor's compliance with the obligations of data processors under Data Protection Law in relation to its Processing of Personal Data.

Controller may, upon written request and at least 30 days' notice to Processor, during regular business hours and without interrupting Processor's business operations, conduct an inspection of Processor's business operations or have the same conducted by a qualified third party auditor subject to Processor's approval, which shall not be unreasonably withheld.

Processor shall, upon Controller's written request and on at least 30 days' notice to the Processor, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

TMS may at its discretion provide reasonable cooperation to Client in connection with any data protection impact assessment (at Client's expense) or consultations with supervisory authorities that may be required in accordance with applicable Data Protection Law.

7. Sub-Processors

- (a) **Appointment of Sub-Processors.** Controller acknowledges and agrees to (a) the engagement as sub-Processors of Processor's affiliated companies and the third parties listed on our Sub-Processors Page available at <https://trafft.com/privacy-policy/> and (b) that Processor and Processor's affiliated companies respectively may engage third-party sub-Processors in connection with the provision of the Service. For the avoidance of doubt, the above authorization constitutes Controller's general written authorization to

Data Processing Addendum

the sub-Processing by Processor for purposes of Clause 9 of the Standard Contractual Clauses adopted by the European Commission.

Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfill its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations.

Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this DPA and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.

The provisions of this Section 7 shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, TMS transfers any Personal Data to a sub-Processor located outside of the EEA, TMS shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

- (b) **Current Processor List and Notification or Objection to New Sub-Processors.** If the Processor intends to instruct sub-Processors other than the companies listed on the Sub-Processors Page, the Processor will notify the Controller by updating the Sub-Processors Page available at <https://trafft.com/privacy-policy/> and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 10 days after being notified. The objection must be based on reasonable grounds. If the Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party.

8. Data Transfers

Controller acknowledges and agrees that, in connection with the performance of the Services under the Agreement, Personal Data will be transferred to TMS in the Republic of Serbia. Processor may access and perform Processing of Personal Data on a global basis as necessary to provide the Service, in accordance with the Agreement.

The Standard Contractual Clauses adopted by the European Commission in Exhibit I will apply with respect to Personal Data transfer from EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Law).

Data Processing Addendum

The Standard Contractual Clauses adopted by the Serbian Commissioner in Exhibit II will apply with respect to Personal Data transfer from a country that does not provide an adequate level of protection for Personal Data (as described in Personal Data Protection Act).

To the extent that Controller or Processor are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently revoked, or held in a court of competent jurisdiction to be invalid, Controller and Processor agree to cooperate in good faith to pursue a suitable alternate mechanism that can lawfully support the transfer.

9. General Provisions

The parties are liable according to the general rules of applicable law, however, TMS is liable according to the scope set out in the Agreement.

Client agrees to indemnify and hold TMS harmless from any and all demands, losses, liability, claims or expenses (including attorneys' fees) made against TMS by any third party due to or arising out of or in connection with the Client's breach of any obligation of the Data Protection Law, provided TMS could not have been reasonably aware that Client's actions constitute breach of the Data Protection Law.

In case of any conflict, this DPA shall take precedence over the regulations of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses adopted by the European Commission in Exhibit I hereof, the Standard Contractual Clauses adopted by the European Commission shall prevail, provided however: (a) Controller may exercise its right of audit under clause 8.9(c) and (d) of the Standard Contractual Clauses adopted by the European Commission, and subject to the requirements of section 6 of this DPA; and (b) Processor may appoint sub-Processors as set out, and subject to the requirements of, section 4 and section 7 of this DPA.

In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses adopted by the Serbian Commissioner in Exhibit II hereof, the Standard Contractual Clauses adopted by the Serbian Commissioner shall prevail, provided however: (a) Controller may exercise its right of audit under Article 11 of the Standard Contractual Clauses adopted by the Serbian Commissioner, and subject to the requirements of section 6 of this DPA; and (b) Processor may appoint sub-Processors as set out, and subject to the requirements of, section 4 and section 7 of this DPA.

Data Processing Addendum

This DPA replaces all previously signed DPAs, previous written or oral correspondence, offers or proposals exchanged between the Parties. Unless otherwise specifically prescribed in this DPA, the DPA may be amended only in writing in the form of a separate Annex or DPA to be signed by both Parties. No action, conduct or behavior of any of the Parties during the term of the contractual relationship can be interpreted as a waiver of this provision or as a proposal to amend this provision.

10 Parties to this DPA

This DPA is an amendment to and forms part of the Agreement. Controller and TMS that are each a party to the Agreement are also each a party to this DPA.

Data Processing Addendum

	EXHIBIT I				
	STANDARD CONTRACTUAL CLAUSES ADOPTED BY THE EUROPEAN COMMISSION				
	SECTION I				
	Clause 1				
	Purpose and scope				
(a)	The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.				
(b)	<p>The Parties:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%; text-align: center;">(i)</td> <td>the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and</td> </tr> <tr> <td style="text-align: center;">(ii)</td> <td>the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')</td> </tr> </table> <p>have agreed to these standard contractual clauses (hereinafter: 'Clauses').</p>	(i)	the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each ' data exporter '), and	(ii)	the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ' data importer ')
(i)	the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each ' data exporter '), and				
(ii)	the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ' data importer ')				
(c)	These Clauses apply with respect to the transfer of personal data as specified in Annex I.B .				
(d)	The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.				
	Clause 2				
	Effect and invariability of the Clauses				
(a)	These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and				

Data Processing Addendum

	<p>Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.</p>																
(b)	<p>These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.</p>																
	Clause 3																
	Third-party beneficiaries																
(a)	<p>Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:</p>																
	<table border="1"> <tr> <td>(i)</td> <td>Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;</td> </tr> <tr> <td>(ii)</td> <td>Clause 8.1(b), 8.9(a), (c), (d) and (e);</td> </tr> <tr> <td>(iii)</td> <td>Clause 9(a), (c), (d) and (e);</td> </tr> <tr> <td>(iv)</td> <td>Clause 12(a), (d) and (f);</td> </tr> <tr> <td>(v)</td> <td>Clause 13;</td> </tr> <tr> <td>(vi)</td> <td>Clause 15.1(c), (d) and (e);</td> </tr> <tr> <td>(vii)</td> <td>Clause 16(e);</td> </tr> <tr> <td>(viii)</td> <td>Clause 18(a) and (b).</td> </tr> </table>	(i)	Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;	(ii)	Clause 8.1(b), 8.9(a), (c), (d) and (e);	(iii)	Clause 9(a), (c), (d) and (e);	(iv)	Clause 12(a), (d) and (f);	(v)	Clause 13;	(vi)	Clause 15.1(c), (d) and (e);	(vii)	Clause 16(e);	(viii)	Clause 18(a) and (b).
(i)	Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;																
(ii)	Clause 8.1(b), 8.9(a), (c), (d) and (e);																
(iii)	Clause 9(a), (c), (d) and (e);																
(iv)	Clause 12(a), (d) and (f);																
(v)	Clause 13;																
(vi)	Clause 15.1(c), (d) and (e);																
(vii)	Clause 16(e);																
(viii)	Clause 18(a) and (b).																
(b)	<p>Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.</p>																
	Clause 4																
	Interpretation																
(a)	<p>Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.</p>																

Data Processing Addendum

(b)	These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c)	These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.
	Clause 5
	Hierarchy
	In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.
	Clause 6
	Description of the transfer(s)
	The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.
	Clause 7
	Docking clause
(a)	An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b)	Once it has completed the Appendix and signed Annex I.A. , the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c)	The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.
	SECTION II – OBLIGATIONS OF THE PARTIES
	Clause 8

Data Processing Addendum

Data protection safeguards	
	The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.
8.1	Instructions
(a)	The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b)	The data importer shall immediately inform the data exporter if it is unable to follow those instructions.
8.2	Purpose limitation
	The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B , unless on further instructions from the data exporter.
8.3	Transparency
	On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.
8.4	Accuracy

Data Processing Addendum

	<p>If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.</p>
8.5	Duration of processing and erasure or return of data
	<p>Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).</p>
8.6	Security of processing
(a)	<p>The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data</p>

Data Processing Addendum

	importer shall at least implement the technical and organisational measures specified in Annex II . The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
(b)	The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
(c)	In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
(d)	The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.
8.7	Sensitive data
	Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences

Data Processing Addendum

	(hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.								
8.8	Onward transfers								
	The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:								
	<table border="1"> <tr> <td>(i)</td> <td>the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;</td> </tr> <tr> <td>(ii)</td> <td>the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;</td> </tr> <tr> <td>(iii)</td> <td>the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or</td> </tr> <tr> <td>(iv)</td> <td>the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.</td> </tr> </table>	(i)	the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;	(ii)	the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;	(iii)	the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or	(iv)	the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
(i)	the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;								
(ii)	the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;								
(iii)	the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or								
(iv)	the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.								
	Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.								
8.9	Documentation and compliance								
(a)	The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.								
(b)	The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.								
(c)	The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and								

Data Processing Addendum

	contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
(d)	The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e)	The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.
Clause 9	
Use of sub-processors	
(a)	The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
(b)	Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
(c)	The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or

Data Processing Addendum

	other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d)	The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e)	The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
	Clause 10
	Data subject rights
(a)	The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
(b)	The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
(c)	In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.
	Clause 11
	Redress
(a)	The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Data Processing Addendum

(b)	In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.				
(c)	Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to: <table border="1" style="width: 100%; margin-top: 5px;"> <tr> <td style="width: 5%; vertical-align: top;">(i)</td> <td>lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;</td> </tr> <tr> <td style="vertical-align: top;">(ii)</td> <td>refer the dispute to the competent courts within the meaning of Clause 18.</td> </tr> </table>	(i)	lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;	(ii)	refer the dispute to the competent courts within the meaning of Clause 18.
(i)	lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;				
(ii)	refer the dispute to the competent courts within the meaning of Clause 18.				
(d)	The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.				
(e)	The data importer shall abide by a decision that is binding under the applicable EU or Member State law.				
(f)	The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.				
Clause 12					
Liability					
(a)	Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.				
(b)	The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.				

Data Processing Addendum

(c)	Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d)	The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e)	Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f)	The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g)	The data importer may not invoke the conduct of a sub-processor to avoid its own liability.
Clause 13	
Supervision	
(a)	Where the data exporter is established in an EU Member State: Germany The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
(b)	The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply

Data Processing Addendum

	with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.						
	SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES						
	Clause 14						
	Local laws and practices affecting compliance with the Clauses						
(a)	The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.						
(b)	The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%; text-align: center;">(i)</td> <td>the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;</td> </tr> <tr> <td style="text-align: center;">(ii)</td> <td>the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;</td> </tr> <tr> <td style="text-align: center;">(iii)</td> <td>any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.</td> </tr> </table>	(i)	the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;	(ii)	the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;	(iii)	any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
(i)	the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;						
(ii)	the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;						
(iii)	any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.						

Data Processing Addendum

(c)	The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d)	The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e)	The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f)	Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.
Clause 15	
Obligations of the data importer in case of access by public authorities	
15.1	Notification
(a)	The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

Data Processing Addendum

	<p>(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or</p> <p>(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.</p>
(b)	If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c)	Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d)	The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e)	Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.
15.2	Review of legality and data minimisation
(a)	The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after

Data Processing Addendum


	careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).		
(b)	The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.		
(c)	The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.		
SECTION IV – FINAL PROVISIONS			
Clause 16			
Non-compliance with the Clauses and termination			
(a)	The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.		
(b)	In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).		
(c)	The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where: <table border="1" style="margin-left: 20px;"> <tr> <td>(i)</td> <td>the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these</td> </tr> </table>	(i)	the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these
(i)	the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these		

Data Processing Addendum


	<p>Clauses is not restored within a reasonable time and in any event within one month of suspension;</p>
(ii)	<p>the data importer is in substantial or persistent breach of these Clauses; or</p>
(iii)	<p>the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.</p>
	<p>In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.</p>
(d)	<p>Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.</p>
(e)	<p>Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.</p>
	Clause 17
	Governing law
	<p>These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The</p>

Data Processing Addendum

	Parties agree that this shall be the law of the Federal Republic of Germany.
	Clause 18
	Choice of forum and jurisdiction
(a)	Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b)	The Parties agree that those shall be the courts of the Member State in which the data exporter is established.
(c)	A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d)	The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX	
ANNEX I	
A. LIST OF PARTIES	
Data exporter(s):	
1.	Name: Privatpraxis für Psychotherapie
	Address: 25712 Burg (Dithmarschen), Bürger Feld 6
	Contact person's name, position and contact details: Wolfgang Hack praxis@psychotherapie-hack.de, +49 4825 9033951
	Activities relevant to the data transferred under these Clauses:
	Signature and date:  <u>03.01.2025.</u>
	Role (controller/processor): controller

Data Processing Addendum

	Data importer(s):	
2.	Name:	TOUCH ME SOFT D.O.O. BEOGRAD – NOVI BEOGRAD
	Address:	Velisava Vulovića 18, Belgrade, Republic of Serbia
	Contact person's name, position and contact details:	Alexander Gilmanov, Managing Director
	Activities relevant to the data transferred under these Clauses:	
	Signature and date:	 03.01.2025.
	Role (controller/processor):	processor
B. DESCRIPTION OF TRANSFER		
A	Categories of data subjects whose personal data is transferred	
	Categories of data subjects set out under Section 2(a) of the Data Processing Agreement to which the Clauses are attached.	
B	Categories of personal data transferred	
	Categories of personal data set out under Section 2(b) of the Data Processing Agreement to which the Clauses are attached.	
C	Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	

Data Processing Addendum

	The parties do not anticipate the transfer of special categories of data. The Client shall NOT disclose to the TMS any Personal data falling into a special category of Personal data as specified in the GDPR. Also, the Client shall not use the Service in a way that would demand or motivate Data Subjects to provide such Personal data.
D	The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
	The data is transferred on a continuous basis.
E	Nature of the processing
	Nature of the processing set out under Section 2(c) of the Data Processing Agreement to which the Clauses are attached.
F	Purpose(s) of the data transfer and further processing
	Purposes of the processing set out under Section 2(d) of the Data Processing Agreement to which the Clauses are attached.
G	The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
	The period set out under Section 2(e) of the Data Processing Agreement to which the Clauses are attached.
H	For transfers to sub-processors, also specify subject matter, nature and duration of the processing
	The subject matter, nature and duration of the processing by the sub-processor is set out on data importer's Sub-Processors Page available at https://trafft.com/privacy-policy/ .
	C. COMPETENT SUPERVISORY AUTHORITY
	Competent supervisory authority is established in an EU Member State, Germany.

Data Processing Addendum

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

TMS currently observes the security practices described in this Annex II. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, TMS may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

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

A. **Access control to premises**

- *Premises in which technical equipment is stored are protected in a most appropriate manner to prevent unauthorized access to the computers.*
- *Keys of premises in which technical equipment is stored can be used only in accordance with protection plans and should never be left in the door lock.*
- *In absence of employees, protected premises are locked and can never be left without supervision of Processor's employees.*
- *Special categories of personal data, in terms of Law on Personal Data Protection, are kept exclusively inside of premises protected in accordance with special measures.*
- *Employees (such as hygiene personnel, security etc.) can enter the protected premises outside working hours only in the case that access to personal data is disabled (locked closets and desks, computers turned off and other hardware devices etc.).*

B. **Access control to use the Service**

- *Access to data via software installed on Processor's computers is allowed only by entering the password on the system of authorization and identification of a person, program, and data. Based on the entered passwords, it is possible to determine the time when personal data was entered, the identity of person who made the entry and other relevant information related to personal data entries.*
- *If the system detects the inactivity of the logged user, automatic time-out of the user terminal will occur, so the user will be required to re-enter the password on the system of authorization and identification of a person, program, and data.*

Data Processing Addendum

- *Passwords must comply with requirements regarding minimum length, use of special characters, etc.*

C. **Access control to Personal Data**

- *Processor uses the appropriate firewall and encryption technologies to protect the gateways and pipelines through which the data travels.*
- *Processor monitors the completeness and correctness of the transfer of data via SFTP or SSL (end-to-end check).*
- *Passwords and procedures related to personal data entries and administration of computers are kept in a locked folder protected from unauthorized access and are used only in exceptional and/or urgent circumstances. Each opening and/or use of the content of locked folder is being documented. After each opening or use of the content of locked folder, the new password is set.*
- *Automated password protected screen-lock is set after more than 15 minutes of inactivity.*

D. **Organization control**

- *Processor organizes annual training of employees on data protection and privacy matters.*
- *Processor enters into separate non-disclosure agreements with every employee who has or may have access to personal data.*
- *Employees responsible for receipt and record of postal items are obliged to deliver received items directly to the individual to whom the item is addressed, i.e. the sector to which it is addressed.*
- *Clear desk principle.*
- *Access rights hierarchy to areas and electronic storage locations.*

E. **Availability control**

- *In case that computer systems fail or need to be restarted or any other exceptional circumstance occurs, personal data is being backed-up on appropriate data transmission media and/or appropriate telecommunication channels. Back-up copies must be kept under lock, protected from fire, flood and electromagnetic interferences in regular climate conditions.*
- *Security events are monitored, notification and alert process is set up on all servers, networks, databases containing personal data;*
- *Security Incident Response Process is defined;*

F. The Processor is using servers and cloud infrastructure of Amazon Web Services as well as Google LLC to store Personal Data.

G. 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

Data Processing Addendum

c)Information about GDPR compliance of Amazon Web Services:
aws.amazon.com/compliance/gdpr-center

Information about security of Google LLC:

a)Information about security of Google LLC:
<https://safety.google/security-privacy/>

b)Information about physical security of Google LLC data centers:
<https://www.google.com/about/datacenters/data-security/>

c)Information about GDPR compliance of Google LLC:
<https://cloud.google.com/privacy/gdpr>

Information about security of Hetzner Online GmbH:

a)Information about security of Google LLC:
<https://www.hetzner.com/assets/Uploads/Sicherheit-en.pdf>

b)Information about physical security of Hetzner Online GmbH data centers:
<https://www.hetzner.com/assets/Uploads/Sicherheit-en.pdf>

c)Information about GDPR compliance of Hetzner Online GmbH:
<https://www.hetzner.com/legal/privacy-policy>

- H. The Controller can manage and delete any Personal data in his account used to access the Service. This allows the Controller to meet his obligations regarding requests of Data subjects for Personal data information or deletion.

Data Processing Addendum

EXHIBIT II

STANDARD CONTRACTUAL CLAUSES ADOPTED BY THE SERBIAN COMMISSIONER ("SCC")

Article 1

This SCC shall regulate the legal relationship between the contracting Parties regarding the processing of Personal Data entrusted to the Data Processor – TMS on behalf of the Data Controller – the Client.

The subject matter of the processing, nature and purpose of the processing, categories of Personal Data and Data Subjects to be processed shall be defined in **Appendix 1** to this Agreement, which shall form an integral part thereof.

For anything not regulated by this SCC, the Contracting Parties shall regulate independently, unless the latter is contrary to this SCC, i.e., if that act does not diminish the protection of Personal Data or the rights of the Data Subject.

Article 2

Defined terms:

- 1) "**Personal Data**", "**Data Subject**", "**processing**", "**Data Controller**", "**Data Processor**", as well as "**Personal Data breach**" shall have the same meaning as prescribed in the Personal Data Protection Act ("*Official Gazette of the RS*", no. 87/18);
- 2) "**Sub-processor**" shall mean another Data Processor who has been entrusted by the Data Processor with certain processing operations on behalf of the Data Controller;
- 3) "**security measures**" shall mean the appropriate technical, organizational and personnel-related measures designed to ensure the effective application of the principles of Personal Data protection as well as the protection of the rights and freedoms of the Data Subject;
- 4) "**the Law**" shall mean the Personal Data Protection Act ("*Official Gazette of the RS*", no. 87/18) and the bylaws adopted in accordance with the Personal Data Protection Act;
- 5) "**the applicable legislation**" shall mean the relevant legislation of the Republic of Serbia.

Obligations of the Data Controller

Data Processing Addendum

Article 3

The Data Controller shall be obliged to carry out the processing operations of Personal Data in accordance with the Law, as well as to apply all data protection measures and ensure the exercise of the rights and freedoms of the Data Subject.

The Data Controller undertakes to issue instructions to the Data Processor regarding the processing of Personal Data in writing, as well as to provide clear, precise and instructions that are in accordance with the applicable legislation.

Obligations of the Data Processor

Article 4

The Data Processor shall be obliged to process Personal Data only upon the written instructions of the Data Controller, including the instructions regarding the transfer of Personal Data to third countries or international organizations, unless the Data Processor is legally obliged to process the Personal Data. In such case, the Data Processor is obliged to notify the Data Controller of that legal obligation before the commencement of processing, unless it is in public interest to prohibit the disclosure of such information by the Law.

The Data Processor shall be obliged to notify the Data Controller without any undue delay if they believe that the received written instructions are not in accordance with the Law and/or other applicable legislation, or provisions of this SCC, and in the event of any uncertainty regarding which actions are to be taken, the Data Processor is obliged to seek the opinion of the Data Controller.

The procedure and decision-making on further action in the situations referred to in the preceding paragraph of this Article, as well as the consequences in the event of a potentially unlawful instruction shall be specified in **Appendix 2** to this SCC and shall form an integral part thereof.

The Data Processor shall be obliged to ensure that only individuals who need access to the Personal Data to ensure compliance with the obligations of the Data Processor towards the Data Controller shall have access to such data.

The Data Processor shall be obliged to ensure that an individual authorized to process Personal Data with the Data Processor is obliged to keep the confidentiality of the data or that that individual is subject to a legal obligation of keeping the confidentiality of the data.

The need for individuals to have access to Personal Data shall be revised from time to time, and if it is determined that a particular person has ceased to have access to that data, they will be denied access.

Data Processing Addendum

The Data Processor is obliged to assist the Data Controller in fulfilling the obligations prescribed by the Law.

The Data Processor must be able to present to the Data Controller the fulfillment of their obligations prescribed by this SCC.

If the Data Processor violates the provisions of this SCC, determining the purpose and manner of processing Personal Data, the Data Processor shall be considered as the Data Controller in relation to that processing.

The obligations of the Data Processor under this SCC shall not diminish their obligations under the Law or other applicable regulation.

Safeguards of Personal Data Processing

Article 5

The Contracting Parties shall be obliged to implement the appropriate safeguards to achieve an adequate level of security concerning the risk, in accordance with the level of technological advances and the cost of their implementation, the nature, extent, circumstances and purpose of processing, as well as the likelihood of occurrence of risk and the level of risk for rights and freedoms of natural persons.

The Contracting Parties shall be obliged to individually assess the likelihood and level of risk occurrence regarding the rights and freedoms of natural persons and determine the appropriate safeguards to reduce the estimated risk, while the Data Controller shall be obliged to provide all the information to the Data Processor to enable him to fulfill this obligation.

Where appropriate, the safeguards referred to in this Article shall include the following, in particular:

- 1) pseudonymization and encryption of Personal Data;
- 2) ensuring the continued confidentiality, integrity, availability and resilience of processing systems and services;
- 3) ensuring the re-availability and access to Personal Data in the event of physical or technical incidents without any undue delay;
- 4) the implementation of regular testing, evaluation and assessment of the effectiveness of technical, organizational and personnel security measures of processing.

While assessing the appropriate level of security referred to in paragraph 1 of this Article, a special attention shall be paid to the risks of processing, in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data that has been transferred, stored or processed in another way.

In the event when, during processing, it is found that additional safeguards are required compared to those already agreed upon, the Contracting Parties shall subsequently enter such safeguards into

Data Processing Addendum

Appendix 3 to this Agreement, which shall form an integral part thereof.

The Contracting Parties shall be obliged to take measures to ensure that any natural person authorized to access Personal Data on behalf of the Data Controller or Data Processor, only processes such Personal Data at the request of the Data Controller or if required by the Law.

Notwithstanding the preceding provisions of this Agreement, the Data Processor shall be entitled to disclose any Personal Data at the request of a court or other state body, in the exercise of their powers prescribed by the applicable legislation, with the obligation to notify the Data Controller without any undue delay, as well as to consult the Data Controller to the extent possible on the scope and form of disclosing the data.

Notification of a Personal Data breach

Article 6

The Data Processor shall be obliged to inform the Data Controller without undue delay of a Personal Data breach which may cause a risk to the rights and freedoms of natural persons, as well as to assist the Data Controller in fulfilling his obligations prescribed by the Law.

The notification referred to in paragraph 1 of this Article must contain at least the following information:

- 1) description of the nature of the breach of the Personal Data, including the categories of Personal Data and the approximate number of Data Subjects of that type, as well as the approximate number of the Personal Data items affected by the Personal Data breach;
- 2) description of the possible consequences of the Personal Data breach;
- 3) description of the measures taken or proposed by the Data Processor concerning the breach, including the measures taken to mitigate the adverse effects.

The Data Processor shall be obliged to provide, at the request of the Data Controller, all information, required documentation and necessary assistance in order to eliminate or mitigate the possible consequences of Personal Data breach.

In the event of a Personal Data breach, the Data Controller may suspend the transfer of Personal Data to the Data Processor.

The deadline, content, and manner of notifying the Data Controller of a Personal Data breach on behalf of the Data Processor shall be defined in **Appendix 4** to this SCC, which shall form an integral part hereof.

Data Processing Addendum

Data Protection Impact Assessment

Article 7

Taking into consideration the nature of the processing and available information, the Data Processor shall be obliged to assist the Data Controller in fulfilling their obligation regarding the assessment of the impact of the anticipated processing operations on the protection of Personal Data and the obligation to seek the opinion of the Commissioner for Information of Public Importance and Personal Data Protection before commencing with the processing operations.

Subcontracting a Sub-processor

Article 8

The Data Processor shall not subcontract any of its processing operations to a Sub-processor without the prior written general or special authorization on behalf of the Data Controller. If the processing is performed under a general authorization, the Data Processor shall be obliged to inform the Data Controller of the planned choice of the Sub-processor, i.e., his replacement, in order for the Data Controller to be able to submit a declaration on such change.

The deadline within which the Data Controller is entitled to submit a declaration on the selection or replacement of the Sub-processor, as well as on the list of Sub-processors approved by the Data Controller, whether or not the Data Processor is authorized to entrust them with processing based on the general or specific written authorization by the Data Controller, shall be defined in **Appendix 5** to this Agreement, which shall form an integral part thereof.

If the Data Processor designates a Sub-processor to perform special processing operations on behalf of the Data Controller, he shall ensure that the same Personal Data protection obligations set out in this SCC apply to the Sub-processor, under a separate agreement or other legally binding documents concluded or adopted in writing, including electronically, which establishes sufficient guarantees for the implementation of the appropriate security measures in the relationship between the Data Processor and the Sub-processor that ensure that processing is carried out in accordance with the Law, the applicable regulations and provisions of this SCC.

The Data Processor shall be obliged to provide a provision in the agreement or another legally binding document to be concluded with the Sub-processor that the Data Controller is entitled, for any reason, to require the Sub-processor to destroy or return the Personal Data of the Data Subject that is subject of that agreement or another legally binding document.

Data Processing Addendum

If the Data Processor entrusts the processing to a Sub-processor, the Data Processor must be able to demonstrate that the Sub-processor shall be subcontracted in everything in accordance with the provisions of this Article of the SCC.

The Data Processor shall be obliged to provide the Data Controller with a copy of the agreement or other legally binding document concluded with the Sub-processor immediately upon the conclusion of the agreement or the adoption of another legally binding document. The Data Processor is entitled not to provide the data that does not concern the processing of Personal Data from the agreement or another legally binding document to the Data Controller.

In the event the Sub-processor fails to fulfill his obligations regarding the protection of Personal Data, the Data Processor shall be liable for fulfilling the obligations of the Sub-processor.

Rights of Data Subjects

Article 9

Considering the nature of the processing, the Data Processor shall be obliged to assist the Data Controller, to the best of his ability, in fulfilling the obligations of the Data Controller in relation to the requirements for the exercise of the Data Subject's legally prescribed rights envisaged.

If the Data Subject submits a request to exercise a right prescribed by the applicable legislation to the Data Processor, for which the Data Controller is responsible, the Data Processor is not authorized to act upon such request of the Data Subject, but is obliged to inform the Data Controller without any undue delay and to forward such request, as well as to inform the Data Subject, who submitted the request, that it has been forwarded to the Data Controller.

In the event the Data Controller ceased to exist in law, the Data Processor is obliged to act upon the requests of the Data Subject, unless any successor entity has assumed the entire legal rights and obligations of the Data Controller from this SCC.

Transfer of Personal Data to Third Countries or International Organizations

Article 10

The transfer of Personal Data to a third country, part of its territory or one or more sectors of certain activities in that country or to an international organization shall be carried out in accordance with the provisions of the applicable legislation, while ensuring an adequate level of protection of Personal Data, the attainability of all rights and effective legal protection of the Data Subjects.

Data Processing Addendum

The Data Processor may transfer Personal Data to a third country, part of its territory, or one or more sectors of certain activities in that country or to an international organization only upon the written instructions of the Data Controller.

The instructions of the Data Controller for the transfer of Personal Data to a third country, part of its territory, or one or more sectors of certain activities in that country or to an international organization, as well as the list of third countries to which the transfer of data is authorized, if applicable, shall be indicated in **Appendix 6** to this SCC and shall form an integral part thereof.

Monitoring the Data Processor's Compliance with Obligations

Article 11

The Data Processor is obliged to submit to the Data Controller all information necessary to demonstrate fulfillment of the obligations of the Data Processor prescribed by the applicable regulations and this SCC, as well as information that enables and contributes to the monitoring of the Data Processor's work, which shall be carried out by the Data Processor or another authorized person.

The Data Controller is obliged to inform the Data Processor on the detected omissions in writing, which includes e-mail, as well as to leave the Data Processor an appropriate deadline for its elimination.

Until the Data Processor eliminates the detected omissions in the implementation of the obligations referred to in paragraph 1 of this Article, the Data Controller may suspend the transfer of Personal Data to the Data Processor.

The manner of exercising monitoring of the Data Processor's compliance with his obligations referred to in paragraph 1 of this Article on behalf of the Data Controller or an authorized person, as well as the deadline and the manner of elimination of any omissions by the Data Processor has been specified in **Appendix 7**, which shall form an integral part of the SCC.

Duration of the Processing

Article 12

This SCC shall begin to apply as of the day of execution and shall be concluded for the duration of the period for which Agreement is concluded or, in the case of termination of Agreement, until the date of termination of Agreement.

Obligation of the Data Processor After the Termination of Personal Data-Processing Services

Data Processing Addendum

Article 13

Upon completion of the contracted data-processing services, the Data Processor is obliged, on the basis of the decision of the Data Controller, to delete or return all Personal Data and delete all copies of this data to the Data Controller, unless the obligation to keep the data is otherwise prescribed by the Law.

The Data Processor must be able to present the fulfillment of his obligation from the preceding paragraph of this Article to the Data Controller.

The terms of termination of the SCC, the notice period, as well as the consequences of termination and liability in case of default, may be specified by the Contracting Parties in **Appendix 8**, which shall form an integral part of this SCC.

Applicable Law

Article 14

Standard Contractual Clauses shall be interpreted and applied in accordance with the legislation of the Republic of Serbia.

Dispute Resolution

Article 15

All disputes arising out of or in connection with the present contract shall be finally settled by arbitration organized in accordance with the Rules of the Belgrade Arbitration Center (the Belgrade Rules) and judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction thereof. The seat of arbitration shall be in Belgrade.

Data Processing Addendum

APPENDIX 1

This Appendix forms an integral part of the SCC and must be completed and signed by the Contracting Parties.

Subject Matter, Nature and Purpose of Processing

Subject-Matter and Nature of the Processing. Subject-Matter and Nature of the Processing set out under Section 2(c) of the Data Processing Agreement to which the SCC are attached.

Purpose of the Processing. Purposes of the processing set out under Section 2(d) of the Data Processing Agreement to which the SCC are attached.

Categories of Data Subjects

Categories of data subjects set out under Section 2(a) of the Data Processing Agreement to which the SCC are attached.

Categories of Personal Data

Categories of personal data set out under Section 2(b) of the Data Processing Agreement to which the SCC are attached.

Special Categories of Personal Data

The parties do not anticipate the transfer of special categories of Personal Data. Data Controller shall NOT disclose to the Data Processor any Personal Data falling into a special category of Personal Data as specified in the Law.

APPENDIX 2

This Appendix forms an integral part of the SCC and must be completed and signed by the Contracting Parties.

The procedure, decision-making on further action in situations where the Data Processor considers that the written instruction received from the Data Controller is not in accordance with the applicable regulations and/or the Law and/or the provisions of the Standard Contractual Clauses and the consequences in the case of an unlawful instruction:

Data Processing Addendum

as set out under Section 4(a) of the Data Processing Agreement to which the SCC are attached.

APPENDIX 3

This Appendix forms an integral part of the SCC and must be completed and signed by the Contracting Parties.

Security measures described under Annex II to Exhibit 1 of Data Processing Agreement to which the SCC are attached.

Subsequently entered security measures:

Description of the security measures:

1) Technical measures:

2) Organizational measures:

3) Personnel-related measures:

APPENDIX 4

This Appendix forms an integral part of the SCC and must be completed and signed by the Contracting Parties.

Data Processing Addendum

The deadline within which the Data Processor is obliged to notify the Data Controller of the Personal Data breach shall be 72 hours after it becomes aware of any Personal Data breach affecting any Personal Data (in letters: seventy-two hours).

The content and method of Notification of the Data Controller about the Personal Data breach by the Data Processor according to the Standard Contractual Clauses (please specify):

At the Data Controller's request, Data Processor will promptly provide the Data Controller with all reasonable assistance necessary to enable the Data Controller to notify relevant Personal Data breaches to competent authorities and/or affected Data Subjects, if Data Controller is required to do so under the Law, as set out under Section 5 of the Data Processing Agreement to which the SCC are attached.

APPENDIX 5

This Appendix forms an integral part of the SCC and must be completed and signed by the contracting parties if the processing has been entrusted to Sub-processors.

If the processing is performed under a general authorization, the deadline within which the Data Controller is entitled to assert his choice, i.e., replace the approved Sub-processor, shall be 48 hours (forty-eight hours).

In the event the Data Controller does not respond within the stipulated deadline, it shall be considered that he has agreed to the list of Sub-processors.

List of the approved Sub-processors:

The list of approved Sub-processor is available in Section 6 of the Privacy Policy available at <https://trafft.com/privacy-policy/>.

APPENDIX 6

Data Processing Addendum

This Appendix forms an integral part of the SCC and must be completed and signed by the Contracting Parties, in the event that Personal Data is exported from the Republic of Serbia. If the Personal Data is not being exported from the Republic of Serbia (besides to the country where the Data Processor is established), this Appendix shall not form a mandatory part of the SCC.

The instruction of the Data Controller for the transfer of Personal Data to a third country, to a part of its territory or one or more sectors of certain activities in that country or to an international organization:

The Data Processor shall specifically inform the Data Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the Data Controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Data Processor shall provide the Data Controller with the information necessary to enable the data exporter to exercise its right to object.

Where the Data Processor engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Processor under these SCC, including in terms of third-party beneficiary rights for data subjects. The Data Processor shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these SCC.

List of third countries to which the Personal Data transfer has been authorized:

The list of third countries to which the Personal Data transfer has been authorized is available in Section 6 of the Privacy Policy available at <https://trafft.com/privacy-policy/>.

APPENDIX 7

This Appendix forms an integral part of the SCC and must be completed and signed by the Contracting Parties.

The manner in which the Data Controller conducts monitoring over the Data Processor regarding the fulfillment of his obligations:

Data Processing Addendum

set out under Section 6 of the Data Processing Agreement to which the SCC are attached.

APPENDIX 8

This Appendix shall form an integral part of the SCC.

Termination conditions, notice period and the consequences in the event of termination:

The term of this SCC shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

The Contracting Parties agree that on the termination of the provision of data-processing services, the Data Processor and the Sub-processor shall, at the choice of the Data Controller, return all the Personal Data transferred and the copies thereof to the Data Controller or shall destroy all the Personal Data and certify to the Data Controller that it has done so, unless legislation imposed upon the Data Processor prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the Data Processor warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

The Data Processor and the Sub-processor warrant that upon request of the Data Controller and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in this SCC.