Good Tape - Data Processing Agreement

Effective as of February 12th, 2025

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

CVR:

Name:

(the data controller)

and

CVR: 43724509

Name: Good Tape ApS

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

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

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of Good Tape, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

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

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

4. The data processor acts according to instructions

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

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in

Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

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

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

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

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

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

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

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

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

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

c. the right of access by the data subject

d. the right to rectification

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

f. the right to restriction of processing

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

h. the right to data portability

i. the right to object

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

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, Danish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would

result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

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

2. The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation [OPTION 1] to delete all personal data processed on behalf of the data controller and certify to the data controller that

it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

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

13. The parties' agreement on other terms

1. The parties may agree to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

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

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause

11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data controller

Name

Position

Date

Signature

On behalf of the data processor

Name Lasse Finderup

Position Chief Executive Officer

Date

Signature

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:
2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name: Lasse Finderup

Position: Chief Executive Officer

Telephone: +45 20 68 04 45

E-mail: yourfriends@goodtape.io

Name: Jakob Steinn

Position: Tech Lead

Telephone: +45 24 91 52 90

E-mail: steinn@goodtape.io

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Data processor will process Personal Data for the purpose of providing services in accordance with the Services Agreement.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Data processor and select sub-processors will process audio files in order to extract text transcriptions.

A.3. The processing includes the following types of personal data about data subjects:

- Audio and video recordings
- Transcribed text
- Metadata: such as file names, formats, duration, etc.
- Any information provided in the recording

A.4. Processing includes the following categories of data subject:

- Individuals whose voices are recorded in audio or video files.
- Users of the Good Tape platform.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Duration of performance of the Services. If data controller opts for it, the data will be securely retained in order for data controller to access it, during the term of the Agreement

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

Name	Company registration number & Address	Location of Processing	Description of Processing	Type of Processing
First Tier sub-processors				
Azure	256796 70 Sir John Rogerson's Quay, Dublin	European Union	In the event extraordinary scaling is needed; it processes transcriptions, and temporarily stores a copy of uploaded audio files while actively processing transcription, ensuring GDPR-compliant handling of personal data.	Access and temporary storage of uploaded audio files. Processing of transcriptions.
Google	368047 1st and 2nd Floor, Gordon House, Barrow Street, Dublin 4, Ireland	European Union	Processes transcriptions, and temporarily stores a copy of uploaded audio files while actively processing transcription,	Access and temporary storage of uploaded audio files. Processing of transcriptions.

			ensuring GDPR-compliant handling of personal data.	
Supabase	T20UF4683B San Francisco Bay Area, West Coast, Western US	European Union	We use Supabase to securely log in our users. We also use their cloud based secure databases.	Access to personal data limited to account and access management.
Scaleway	RCS PARIS B 433 115 904 8 rue de la ville l'Evêque – 75008 Paris, FRANCE	European Union	We use Scaleway to store your uploaded files, if you tell us to.	Processing and storage of audio files if requested.
MongoDB	0001441816 1633 Broadway, 38th Floor, New York, NY	European Union	We use MongoDB to efficiently manage and store your transcription editor state, ensuring high availability and performance.	Storage of transcription text and edits.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform, in writing, the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

- Transcription of recordings.

C.2. Security of processing

The level of security shall take into account:

- The data importer has implemented and maintains comprehensive technical and organizational safeguards, which contain those safeguards described below:
- Organizational management and dedicated staff responsible for the development, implementation and maintenance of the data processor's information security program.
- Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to data processor's organization, monitoring and maintaining compliance with the data processor's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
- Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable media (i.e. laptop computers).
- Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
- Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords.
- Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii)

manage, monitor and log movement of persons into and out of the data processor's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

- Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the data processor's possession.
- Change management procedures designed to test, approve and monitor all material changes to the data processor's technology and information assets.
- Incident management procedures designed to allow data processor to investigate, respond to, mitigate and notify of events related to the data processor's technology and information assets.
- Network security controls designed to protect systems from intrusion and limit the scope of any successful attack.
- Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
- Disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Good Tape ApS assists data controllers in fulfilling their GDPR obligations, particularly in responding to data subject rights requests, including access, rectification, erasure, data portability, and objection to processing. The company ensures compliance by processing personal data strictly according to the controller's instructions and facilitating requests related to automated decision-making. In the event of a data breach, Good Tape promptly notifies the data controller and provides necessary information for reporting to authorities within 72 hours when required. Additionally, Good Tape supports data controllers in consulting with the Danish Data Protection Agency when processing presents a high risk.

Beyond incident support, Good Tape provides transparency regarding its security measures and assists controllers in meeting their obligations under Article 32 of the GDPR. This includes sharing details of technical and organizational safeguards and implementing additional measures if deemed necessary by the controller.

Good Tape implements robust technical and organizational measures to support data controllers in protecting personal data. All data is securely stored in EU-based data centers, with AES-256 encryption for data at rest and TLS 1.2/1.3 for data in transit. Access control measures, including multi-factor authentication (MFA) and role-based access control (RBAC), restrict unauthorized access. Additionally, continuous security monitoring, audit logs, firewalls, and malware protection ensure the integrity and confidentiality of data processing activities.

Organizationally, Good Tape trains employees in GDPR compliance, enforces confidentiality agreements, and maintains a structured incident response plan. The company also provides ongoing security assessments, compliance documentation, and support for responding to data subject requests. Regular backups in multiple EU-based locations ensure data redundancy and business continuity.

C.4. Storage period/erasure procedures

Data processor shall delete all the Personal Data on data processor's systems on data controller's request and after the end of the provision of Services, and shall delete existing copies unless continued storage of the Personal Data is required by (i) applicable laws of the European Union or its Member States, with respect to Personal Data subject to European Data Protection Laws or (ii) Applicable Data Protection Laws, with respect to all other Personal Data. Data processor will comply with such instruction as soon as reasonably practicable after such expiration or termination, unless Applicable Data Protection Laws require storage. Data controller may choose to request a copy of such Personal Data from data processor for an additional charge by requesting it in writing at least 30 days prior to expiration or termination of the Agreement. Upon the parties' agreement to such charge pursuant to a work order or other amendment to the Agreement, data processor will provide such copy of such Personal Data before it is deleted in accordance with this clause.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- Njalsgade 21G, 3rd floor, 2300 Copenhagen, Denmark
- Any location in which the sub-processors listed in appendix B conduct business

C.6. Instruction on the transfer of personal data to third countries

The data controller hereby instructs and authorizes that data processor to transfer personal data to the sub-processors listed in appendix B to the extent necessary to provide the data processors services to the data controller, provided that the data processor enters into a contract with the sub-processor based on module three of the EU Standard Contractual Clauses for the transfer of personal data to third countries, and implements any supplementary measures deemed necessary to provide the data subjects with a level of protection that is essentially equivalent to the level of protection within EU.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall make available to the data controller any information that is necessary to document the data processor' compliance with these clauses. This includes allowing the data controller to carry out audits.

Data processor will contribute to such audits by providing data controller or data controller's Supervisory Authority with the information and assistance that data processor considers appropriate in the circumstances and reasonably necessary to conduct the audit.

To request an audit, data controller must submit a proposed audit plan to data processor at least two weeks in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit.

Data processor will review the proposed audit plan and provide data controller with any concerns or questions (for example, any request for information that could compromise data processor security, privacy, employment or other relevant policies).

Data processor will work cooperatively with data controller to agree on a final audit plan.

Nothing in this Section 9 shall require the data processor to breach any duties of confidentiality.

If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, or similar audit report performed by a qualified third party auditor within twelve (12) months of data controller's audit request and data processor has confirmed there have been no known material changes in the controls audited since

the date of such report, data controller agrees to accept such report in lieu of requesting an audit of such controls or measures.

The audit must be conducted during regular business hours, subject to the agreed final audit plan and data processor’s safety, security or other relevant policies, and may not unreasonably interfere with data processor business activities.

Each Party shall bear its own costs related to the inspection or audit.

Appendix D The parties' terms of agreement on other subjects

D.1. Definitions

"Transcription Data" shall mean any content, in writing or audio (or any other media), provided by the data controller through the Services, including but not limited to Personal Data.

"Process", "Processing" or "Processed" shall mean any operation or set of operations, as defined in the Applicable Privacy Law, performed upon Personal Data whether or not by automatic means, including collecting, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data.

"***Security Breach***" means a breach of data processor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in data processor's possession, custody or control. Security Breaches do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

"***Services***" shall mean the services as described in the Agreement or any related order form or statement of work.

D.2. Data controller obligations

1. **Data controller's Security Responsibilities**. Data controller agrees that, without limitation of data processor's obligations under Section 4 (Security of Personal Data), data controller is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices data controller uses to access the Services; (c) securing data controller's systems and devices that data processor uses to provide the Services; and (d) backing up Personal Data.

2. **Prohibited Data**. Data controller represents and warrants that no special categories of personal data as defined in Article 9 of the GDPR, including but not limited to data revealing racial or ethnic origin, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, or data concerning health or biometric identifiers, nor any personal data relating to criminal convictions or offenses as defined in Article 10 of the GDPR, shall be submitted to the data processor for processing under this Agreement, unless explicitly agreed by concluding this Agreement and only where the data controller has established a lawful basis for such

processing in compliance with applicable data protection laws. Furthermore, data controller warrants that no data processed through the Services will contain personal data of children under the age thresholds specified by applicable Member State law without verifiable parental consent, in accordance with Article 8 of the GDPR. Data controller further agrees that the Services shall not be utilized to process, transmit, or store content of a pornographic, violent, threatening, abusive, harassing, defamatory, or otherwise unlawful nature, or any content that could reasonably be expected to endanger or compromise the safety, security, or well-being of any natural person.