CUSTOMER DATA PROTECTION AGREEMENT

This Customer Data Protection Agreement (the "Agreement") is entered into between DocRaptor, LLC, an Indiana limited liability company ("DocRaptor") on behalf of itself and its Affiliates, and the Customer (as defined below), effective as of [Current Date].

RECITALS

A. Customer uses one or more Services provided by DocRaptor. As part of using the Services, Customer may provide Personal Data controlled by Customer for processing by DocRaptor.

B. Customer requires that DocRaptor process Personal Data in compliance with applicable Data Protection Laws, including the GDPR and relevant laws governing international data transfers, and DocRaptor agrees to do so in accordance with the terms of this Agreement.

NOW, THEREFORE, for good and valuable consideration, the parties agree as follows:

AGREEMENT

1. Definitions

1.1 *Affiliate*: Any entity that directly or indirectly controls, is controlled by, or is under common control with a party. "Control" means ownership or control of more than 50% of the voting interests or the right to receive more than 50% of profits.

1.2 *Customer*: The customer using the Services and signing this Agreement.

1.3 *Data Protection Laws*: All applicable data protection and privacy laws and regulations, including GDPR, the UK Data Protection Act 2018, and any other laws governing the processing of Personal Data.

1.4 *GDPR*: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data.

1.5 Standard Contractual Clauses (SCCs): The latest version of the standard contractual clauses for data transfers adopted by the European Commission (currently the version adopted on June 4, 2021), which are incorporated herein by reference.

1.6 *U.S. Data Privacy Framework*: The framework established to facilitate compliant data transfers between the EU and the U.S., replacing the Privacy Shield.

1.7 *Technical and Organizational Measures (TOMs)*: Measures implemented to ensure security and compliance with applicable Data Protection Laws (see Appendix I).

2. Data Processing

2.1 *Scope of Processing*: DocRaptor will process Personal Data only as necessary to provide Services, as specified in the Customer's instructions, and in compliance with this Agreement and applicable Data Protection Laws. For purposes of GDPR, DocRaptor is the data importer, Customer, is the data exporter, and processing activities consist of conversion of HTML to PDF and related API services.

- 1. *Data Transfers*:
    1. Transfers of Personal Data outside the EEA, UK, or Switzerland will be governed by the SCCs or the U.S. Data Privacy Framework, as applicable.
    2. DocRaptor ensures an adequate level of protection in accordance with Data Protection Laws.
  2. *Data Subject Requests*: DocRaptor will cooperate with Customer to address requests from data subjects under GDPR or other applicable laws (e.g., access, rectification, deletion).

3. *Sub-processors*: DocRaptor may engage Sub-processors, provided that: (a) Sub-processors agree to obligations no less stringent than those in this Agreement, and (b) DocRaptor remains fully liable for any breach caused by Sub-processors.

4. *Data Breaches*: In the event of a Security Incident, DocRaptor shall notify Customer within 24 hours of becoming aware of the breach, and 9rovide details, including the nature of the breach, affected data, and mitigation measures.

5. *Data Retention*: Personal Data will be retained by DocRaptor only as long as necessary to provide Services. Upon termination or expiration, Personal Data will be deleted or returned within 30 days, unless required by law.

3. Security Measures

- 1. *TOM's*: DocRaptor will implement TOMs, including, (a) encryption of Personal Data in transit and at rest, (b) regular vulnerability assessments and penetration testing, (c) access control policies to limit access to authorized personnel.

2. *Compliance with Security Standards*: DocRaptor adheres to SOC 2 and/or ISO 27001 standards.

4. Audits

4.1 *Audits*: Customer may contact DocRaptor to request an audit of the architecture, systems and procedures relevant to the protection of Personal Data. Customer shall reimburse the DocRaptor for any time expended by the DocRaptor or its Subcontractors for any such audit at the DocRaptor's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such audit, Customer and DocRaptor shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by the DocRaptor, or its Subcontractors. Customer shall promptly notify DocRaptor with information regarding any non-compliance discovered during the course of an audit.

5. Governing Law

5.1 *Governing Law*. This Agreement will be governed by the laws of the Member State where the data exporter is established for matters related to GDPR. For all other matters, the laws of the State of Indiana, USA, shall apply.

6. Term and Termination

6.1 *Term*. This Agreement remains effective as long as DocRaptor processes Personal Data for the Customer.

6.2 *Effect of Termination*. Upon termination, DocRaptor will cease processing Personal Data, and return or delete all Personal Data within 30 days.

7. Modifications

7.1 *Modifications*. DocRaptor reserves the right to update this Agreement to reflect changes in Data Protection Laws or SCCs. Customers will be notified 30 days in advance.

IN WITNESS WHEREOF, the parties have executed this Agreement.

DocRaptor LLC:

By: 

Name: Matthew W Gordon

Title: VP, SaaS Division

CUSTOMER:

By:

Name:

Title:

Appendix I: Security Measures

In fulfilling its obligations hereunder, DocRaptor has in place and operates in accordance with security policies and standards which comply with the following (and in the case of conflict the highest standard shall prevail):

- 1. the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or an internationally recognised company engaged in the same type of activity under the same or similar circumstances;
2. the policies and standards that the data exporter applies to its own information and documentation;
3. the data importer's security policies and standards;
4. SOC 2 and/or equivalent standards