Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Master Terms of Service Agreement available at the Terms of Service ("Agreement"), entered into by and between Data Processor and Data Controller, in accordance with the personal data processed using Clearout's Services as outlined in the applicable Agreement. The main goal of this DPA is to demonstrate agreement between the two parties in terms of the processing of Personal Data in compliance with the requirements of Data Protection Legislation as provided below.

If the Data Controller signing this DPA is a party to the Agreement, this DPA forms part of the Agreement.
In such a case, Clearout that is a party to the Agreement becomes a party to this DPA.

In the course of providing the Services to Data Controller pursuant to the Agreement, Data Processor may Process Personal Data on behalf of Data Controller and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

1. Definitions

Data Processor or Clearout: Clearout, 2035 Sunset Lake Road Suite B-2, 19702, Newark, Delaware.

Data Controller: a person or company that controls the personal data processed using Clearout's Service

Service or Services: all content, services, and products available at, or through the Website, including, but not limited to, verifying email addresses using Clearout's Website or API.

API: Automated application programming interface to connect Clearout's Services with other websites, servers or applications.

Data Processing: processing of data on behalf of the Data Controller.

Data Protection Law: EU Directive 95/46/EC, as transposed into domestic legislation of each Member

2018) by the GDPR and laws implementing, replacing or supplementing the GDPR.

GDPR: The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).

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

Personal Data: means any data which relates to an identified or identifiable natural person ("Data Subject")

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

Sub-processor: means any person (including any third party, but excluding Clearout employees) appointed by or on behalf of Clearout to process data in connection with the Agreement.

2. Data Processing

2.1. Data Subjects

Data Subjects include the information of the Data controller who signed up for the email verification plan of Data Processor.

2.2. Types of Information

In the course of using the Services, Data Processor asks Data Controller to provide certain personally identifiable information of Data Controller that can be used to contact or identify the Data Controller and to administer the Data Controller‘s account (“Personally Identifiable Information”). Personal Information such as the Data Controller’s name and email address are used to create the account for the Site and Services, as well as for email newsletters and invoicing.

Data Controller’s credit card information is used by third parties such as PayPal or Stripe to process the payment(s) of Data Controller for the Services. Data Controller's consent will be required if the Personal Information of the Data Controller is being collected, used and stored by Data Processor in accordance with the Terms and Conditions of Use and the Privacy Policy of the Data Processor.

2.3. Purpose of the Processing

The purpose of processing is to identify whether an email address exists and whether it is possible to deliver an email to this address. This verification happens in an online, fully automated system. The subject matter of the contract is email verification. In no event will Data Processor process any Personal or Navigational Data for its own purpose or those of any third party.

2.4. Duration of the Processing

Personal Data will be processed for the duration of the Agreement, subject to Section 4 of this DPA. Information uploaded to the Site or otherwise submitted to Data Processor in conjunction with the Services, including but not limited to CSV or XLSX files, may be stored for a period of thirty (30) days. If the Data Controller initiates payment for the Services, Data Processor may collect and store Personal Information, as well as any other information provided to us. This Personal Information may be shared with third parties in order to process the payment of the Data Controller. Data Processor encrypts credit card numbers using industry standard technology.

3. Obligations of Processor

3.1. Security

Data 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.

3.2. Confidentiality

Data Processor shall ensure that any personnel whom the Data Processor authorizes to process Personal Data on Data Processor's behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking of confidentiality shall continue after the termination of the above-entitled activities. Data Processor ensures that its personnel who access Personal Data are subject to confidentiality obligations that restrict their ability to disclose Data Controller Personal Data.

3.3. Personal Data Breaches

Data Processor is obliged to promptly notify the Data Controller about a Personal Data Breach without undue delay and in any event within 36 hours after becoming aware of a data breach.

3.4. Data Subject Requests

Data Processor shall 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), to the extent permitted by the law.

3.5. Sub-processors

Data Processor may hire other companies to provide limited services on its behalf (Annexure 1). Any such sub-processors will be permitted to process Personal Data only to deliver the services Data Processor has retained them to provide, and they shall be prohibited from using Personal Data for any other purpose. Data Processor remains responsible for its sub-processors' compliance with the obligations of this DPA. Any subcontractors to whom Data Processor transfers Personal Data will have entered into written agreements with Data Processor requiring that they abide by terms substantially similar to this DPA. If Data Controller requires prior notification of any updates to the list of sub-processors, Data Controller may request such notification in writing by emailing at us@clearout.io. Data Processor will update the list within seventy-two (72) hours of any such notification if Data Controller does not legitimately object within that time frame. Legitimate objections must contain reasonable and documented grounds relating to a subcontractor's non-compliance with applicable Data Protection Legislation. If in Data Processor's reasonable opinion, such objections are not legitimate, the Data Controller may, by providing written notice to Data Processor, terminate the Agreement.

3.6. Geographical Limitations and Restricted Transfers (EEA)

3.6.1. Clearout's data processing services are hosted by Amazon Web Services in Frankfurt, Germany ("AWS Frankfurt"). All processing Services provided by Clearout shall take place at AWS Frankfurt and all Personal Data shall remain within the European Economic Area ("EEA").

3.6.2. Clearout shall not transfer Personal Data to, or process such data in, a location other than AWS Frankfurt or outside the EEA without client's prior written consent, except in compliance with Section below (in each case, a "Restricted Transfer").

3.6.3. Without prejudice to the foregoing, Client's consents to Restricted Transfers where Clearout has implemented a Restricted Transfer solution compliant with Data Protection Law, which such solution may include:

a) there has been an adequacy decision by the European Commission that permits the Restricted Transfer;

b) the Data Controllers' have consented and the Standard Contractual Clauses have been incorporated into this SPA by amendment;

c) another appropriate safeguard pursuant to Article 46 of the EU GDPR applies; or

d) a derogation pursuant to Article 49 of the EU GDPR applies.

3.7. Deletion or Retrieval of Personal Data

Upon termination or expiration of the Agreement or upon the request, the Data Processor will delete or return to Data Controller all individual- and account-related Personal Data that is in its possession or control (including any Data subcontracted to a third party for processing). This requirement will not apply to the extent that Data Processor is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event Data Processor will isolate and protect the Data from any further processing except to the extent required by such law.

4. Assistance to Data Controller

4.1 The Data Processor shall assist the Data Controller by appropriate technical and organizational

measures **(Annexure 2)**, in so far as this is possible, for the fulfillment of the Data Controller's obligation to respond to a request for exercising the data subject's rights under the GDPR.

4.2 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to security and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.

4.3 The Data Processor shall make available all necessary information to Data Controller to demonstrate compliance with the Data Processor's obligations and to allow for and contribute to audits, including inspections conducted by the Data Controller or another auditor mandated by the Data Controller.

5. Liability and Indemnity

The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Protection Law by the Data Processor. The Data Controller indemnifies the Data Processor and holds the Data Processor harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Law by the Data Controller.

6. Duration and Termination

6.1 This Data Processing Agreement shall come into effect on the date the Data Controller electronically signs this Data Processing Agreement.
6.2 Termination or expiration of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.

6.3 The Data Processor shall process Personal Data until the date of termination of the Service Agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on the instruction of the Data Controller.

7. Data Center and Location

Clearout Service is available in the European region for European users to comply with GDPR so that no data processed outside of the European region.

8. Miscellaneous

For the avoidance of doubt and to the extent allowed by applicable law, any and all liability, including limitations thereof, will be governed by the relevant provisions of the Agreement.

If Data Controller does not agree to any changes to the Agreement, do not continue to use the Clearout application.

Annexure 1:

List of GDPR compliant Sub-Processors:

As a data processor under the GDPR, Clearout makes use of the sub-processors listed below. In order to meet its obligations under Art. 28 of the GDPR, the following disclosure relates to the name and processing actions of these sub-processors.

Sub-processor Name	**Sub-processing Actions**
Stripe	Sub-processor for online payment
PayPal	Sub-processor for online payment
Mailgun	Sub-processor for email notifications
Freshchat	Sub-processor for live chat
AWS	Sub-processor for Server Hosting

Annexure 2:

Technical and Organizational Measures (TOMs) – Security Services

This document describes technical and organizational security measures and controls implemented by Clearout, or Clearout affiliates (hereafter Clearout), to protect personal data and ensure the ongoing confidentiality, integrity and availability of Clearout's products and services.

This document is a high-level overview of Clearout's technical and organizational security measures. More details on the measures we implement are available upon request. Clearout reserves the right to revise these technical and organizational measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for personal data that Clearout processes in providing its various services. In the unlikely event that Clearout does materially reduce its security, Clearout shall notify its customers.

Clearout shall take the following technical and organizational security measures to protect personal data:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Clearout's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the Clearout organization, monitoring and maintaining compliance with Clearout policies and procedures, and reporting the condition of its information security and compliance to senior internal management.
3. Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.
4. Communication with Clearout applications utilizes cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model which provides the ability to apply security controls between each layer.
5. Data security controls which include logical segregation of data, restricted (e.g. role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.
6. 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).
7. Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords

8. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
9. Physical and environmental security of data centre, server room facilities and other areas containing client confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Clearout facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
10. Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, 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 Clearout possession.
11. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Clearout technology and information assets.
12. Incident / problem management procedures designed to allow Clearout investigate, respond to, mitigate and notify of events related to Clearout technology and information assets.
13. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
14. 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.
15. Business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.
16. Formal Vendor Management program, including vendor security reviews for critical vendors to ensure compliance with Clearout Information Security Policies.
17. A Data Protection Officer (DPO) who is independent, regularly reviews data protection risks and controls.