

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") is made between

_____ a company incorporated under the laws of _____ (company number _____) whose registered office is _____;

(the "**Company**")

and

FRAUDFINDER LTD, a company incorporated under the laws of England and Wales (company number 10531940) whose registered office is at 71-75 Shelton Street, London, England, WC2H 9JQ;

(the "**Data Processor**")

hereinafter collectively referred to as "**Parties**" and individually "**Party**".

WHEREAS

- (A) The Company acts as a Data Controller and/or a Data Processor, depending on the applicable processing arrangement.
- (B) The Company wishes to evaluate the Services during a trial period and, for that purpose, to submit documents and information which may contain personal data to the Data Processor.
- (C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing, including the UK GDPR and, where applicable, the General Data Protection Regulation (EU) 2016/679.
- (D) The Parties wish to lay down their rights and obligations. This Agreement is limited to the Trial and creates no obligation on either Party to enter into any further agreement.

Roles of the Parties

Where the Company acts as a data controller, the Company is the controller and the Data Processor is the processor. Where the Company acts as a data processor on behalf of an affiliated entity or other third party acting as the data controller, the Parties acknowledge and agree that Fraudfinder shall act as a sub-processor in respect of such processing. In such circumstances, the obligations set out in this Agreement shall apply mutatis mutandis and shall be equivalent to those the Company owes to the Applicable Controller, as required by Article 28(4) of the UK GDPR, and the Company warrants that it has the authority to appoint Fraudfinder as a sub-processor and to pass down all relevant data protection obligations and instructions on behalf of the applicable data controller.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

- 1.1 Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meaning:
 - 1.1.1 "**Applicable Controller**" means the entity which determines the purposes and means of the processing of Personal Data in the relevant processing arrangement;
 - 1.1.2 "**Anonymised Data**" means data derived from Company Personal Data which has been irreversibly anonymised such that it is no longer personal data under Data Protection Laws;
 - 1.1.3 "**Company Personal Data**" means any Personal Data Processed by the Data Processor on behalf of the Company pursuant to or in connection with the Services;
 - 1.1.4 "**Data Processing Agreement**" means this Agreement and all Schedules;
 - 1.1.5 "**Data Protection Laws**" means the UK GDPR, the Data Protection Act 2018 and, to the extent applicable, the data protection or privacy laws of any other country;
 - 1.1.6 "**EEA**" means the European Economic Area;

- 1.1.7 **"GDPR"** means EU General Data Protection Regulation 2016/679, and **"UK GDPR"** has the meaning given in section 3(10) of the Data Protection Act 2018;
- 1.1.8 **"Data Transfer"** means a transfer of Company Personal Data from the Company to the Data Processor, or an onward transfer from the Data Processor to a Subprocessor or between two establishments of the Data Processor, in each case where such transfer would be prohibited by Data Protection Laws;
- 1.1.9 **"Services"** means the document fraud detection and related risk analysis services provided by the Data Processor to the Company;
- 1.1.10 **"Subprocessor"** means any person appointed by or on behalf of the Data Processor to process Personal Data on behalf of the Company in connection with this Agreement;
- 1.1.11 **"Trial"** means the Company's evaluation of the Services on a no-fee basis for the period set out in Schedule 1.
- 1.2 The terms "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the UK GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

- 2.1 The Data Processor shall:
- 2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
 - 2.1.2 not Process Company Personal Data other than on the Company's documented instructions, unless required to do otherwise by applicable law, in which case the Data Processor shall inform the Company of that requirement before Processing unless prohibited from doing so.
- 2.2 The Company instructs the Data Processor to process Company Personal Data, including where such instructions are provided by the Company acting on behalf of the Applicable Controller. Those instructions are set out in this Agreement, including Schedule 1.
- 2.3 The Data Processor shall promptly inform the Company if, in its opinion, an instruction infringes Data Protection Laws.
- 2.4 The Company shall not submit special category data or criminal offence data during the Trial, other than where it is unavoidably contained within a document submitted for assessment. The Company is responsible for the accuracy, quality and lawfulness of the Company Personal Data and for having a valid lawful basis for the Processing.

3. Processor Personnel

- 3.1 The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Company Personal Data as strictly necessary for the purposes of this Agreement, and ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality and receive data protection training at onboarding and at least annually.

4. Security

- 4.1 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 Processor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR.
- 4.2 Without limiting clause 4.1, the Data Processor maintains encryption in transit (TLS 1.2 or 1.3) and at rest (AES-256), least-privilege access control with enforced multi-factor authentication, continuous monitoring and logging, annual independent penetration testing, and Cyber Essentials certification with an information

security management system aligned to ISO 27001. A summary of the Data Processor's technical and organisational measures is available on request.

5. Subprocessing

5.1 The Data Processor may appoint Subprocessors to process Company Personal Data, provided that the Company is notified in advance and given the opportunity to object on reasonable data protection grounds. The Data Processor shall impose on each Subprocessor, by written contract, data protection obligations no less protective than those set out in this Agreement, and shall remain fully liable for the acts and omissions of any Subprocessor.

5.2 The Data Processor's current sub-processor register is available on request at privacy@fraudfinderai.com.

6. Providing Assistance and Cooperation

6.1 The Data Processor shall provide the Company with all necessary assistance and cooperation in complying with the obligations borne by the Parties on the basis of the UK GDPR and other applicable legislation and regulations concerning the Processing of Personal Data.

6.2 Taking into account the nature of the Processing, the Data Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.3 The Data Processor shall:

6.3.1 promptly notify the Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.3.2 ensure that it does not respond to that request except on the documented instructions of the Company or as required by applicable law, in which case the Data Processor shall, to the extent permitted by applicable law, inform the Company of that legal requirement before responding to the request.

7. Personal Data Breach

7.1 The Data Processor shall notify the Company without undue delay, and in any event within forty-eight (48) hours, upon becoming aware of a Personal Data Breach affecting Company Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Data Processor shall co-operate with the Company and take reasonable commercial steps as are directed by the Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

8.1 The Data Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Company reasonably considers to be required by Article 35 or 36 of the UK GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by the Data Processor and taking into account the nature of the Processing and the information available to the Data Processor.

9. Deletion or Return of Company Personal Data

9.1 Subject to this clause 9, the Data Processor shall promptly and in any event within thirty (30) business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data, or return them to the Company if the Company so elects in writing before the Cessation Date.

9.2 At the Company's request, the Data Processor shall confirm in writing that it has satisfied all obligations under clause 9.1 within thirty (30) business days of the Cessation Date.

9.3 Clause 9.1 does not apply to the extent the Data Processor is required to retain Company Personal Data by applicable law, or where retention is necessary for the establishment, exercise or defence of legal claims, in which case the Data Processor may retain the minimum data necessary and it shall remain subject to clauses 3, 4, 7 and 12. Data held in backups is deleted in accordance with the Data Processor's backup rotation cycle.

10. Audit Rights

10.1 Subject to this clause 10, the Data Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data.

10.2 The Data Processor may satisfy clause 10.1 by providing its current security questionnaire responses, penetration test summary, Cyber Essentials certificate, sub-processor register and relevant policy summaries. Any audit shall be on reasonable written notice, no more than once during the Trial, during business hours, and subject to confidentiality obligations.

10.3 Where the Company acts as a data processor, the rights in this clause 10 may be exercised by the Applicable Controller through the Company, and not directly.

11. Data Transfer

11.1 The Data Processor hosts and processes Company Personal Data within the United Kingdom and the EEA. The Data Processor may not transfer or authorise the transfer of Company Personal Data to countries outside the United Kingdom or the EEA without first putting in place an appropriate transfer mechanism, being the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses and/or the EU Standard Contractual Clauses, and completing a transfer risk assessment where required. The Company authorises the Data Processor to enter into such a mechanism with any Subprocessor on the Company's behalf for this purpose.

12. Confidentiality of Personal Data

12.1 All Personal Data are qualified as confidential and must be treated as such.

12.2 The Parties shall keep all Personal Data confidential and shall not disclose them in any way, either internally or externally, except in so far as:

12.2.1 disclosure and/or provision of the Personal Data is necessary in the context of the performance of this Agreement;

12.2.2 any mandatory statutory provision or court decision requires the Parties to disclose and/or provide the Personal Data, in which case the Parties shall first notify the other Party of this unless such notification is prohibited on the grounds of applicable legislation or court order; or

12.2.3 disclosure and/or provision of the Personal Data takes place with prior consent in writing from the other Party.

12.3 This clause is without prejudice to, and does not replace, any separate non-disclosure agreement between the Parties.

13. Anonymised Data

13.1 The Company grants the Data Processor a perpetual, irrevocable, worldwide, royalty-free right to create Anonymised Data and to use it to develop, train, test and improve the Data Processor's fraud detection models and services and to produce aggregated fraud intelligence. The Data Processor shall not disclose Anonymised Data in any form that identifies the Company, the Applicable Controller or any Data Subject. All intellectual property rights in Anonymised Data vest in the Data Processor. This clause survives termination of this Agreement.

14. Liability

- 14.1 The Company warrants that it has lawfully obtained the Personal Data it provides to the Data Processor and that the Data Processor can lawfully process the Personal Data pursuant to the Company's instructions in order to provide the Services. If the Data Processor does not follow the instructions of the Company or acts outside the scope of its powers and responsibilities under the UK GDPR and this Agreement, it shall qualify as a controller with additional obligations.
- 14.2 Nothing in this Agreement limits or excludes either Party's liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for any liability that cannot lawfully be limited. Subject to that, neither Party shall be liable for loss of profit, loss of anticipated savings, loss of business opportunity, loss of reputation or goodwill, or any indirect or consequential loss, and each Party's total aggregate liability arising out of or in connection with this Agreement is limited to £50,000. The Services are provided during the Trial free of charge and on an "as is" basis.

15. Term and Termination

- 15.1 This Agreement takes effect on the date of last signature and continues for the duration of the Trial and for so long thereafter as the Data Processor Processes Company Personal Data.
- 15.2 Either Party may terminate this Agreement at any time on written notice, with immediate effect and without liability. The Company is further entitled to terminate this Agreement if the Data Processor fails to comply with, or can no longer fulfil, an essential obligation under it, after the Company has informed the Data Processor in writing of the shortcoming and provided a reasonable period to remedy it.
- 15.3 Clauses 3, 4, 7, 9, 12, 13, 14 and 16 survive termination or expiry.

16. Governing Law and Jurisdiction

- 16.1 This Agreement will be construed in accordance with and governed by the laws of England and Wales.
- 16.2 The Parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement.

IN WITNESS WHEREOF, this Data Processing Agreement is entered into with effect from the date first set out below.

FRAUDFINDER LTD	For and on behalf of _____
Signature:	Signature:
Name: Alexander Siedes	Name:
Title: CEO, Director	Title:
Date signed:	Date signed:

SCHEDULE 1

Details of Processing

Item	Detail
Trial period	7 days from the date of last signature, unless extended or terminated earlier by written agreement.
Role of the Company	Data controller, or data processor acting on behalf of an Applicable Controller. Where the Company is a processor, Fraudfinder acts as sub-processor.
Role of Fraudfinder	Data processor or sub-processor, as applicable.
Subject matter	Provision of the Services, being automated detection of fraud in submitted documents and related risk analysis, and where enabled, data extraction, identity verification and confirmation of payee.
Nature of the processing	Collection, receipt, storage, structuring, optical character recognition, automated analysis, scoring, retrieval, disclosure to the Company by report or API, erasure and destruction.
Purpose of the processing	Detection and prevention of document fraud, identity fraud and financial crime, and provision of the Services to the Company for the purposes of the Trial.
Duration of the processing	The Trial period, plus the deletion window and any retention permitted under clause 9.3.
Categories of Data Subjects	Applicants, customers and other individuals whose documents or information are submitted for assessment by or on behalf of the Company, and named additional persons appearing on those documents.
Types of Personal Data	Identity data (name, date of birth, address, contact details); financial and payment data (bank account number, sort code, balances, salary and transaction information); employment data; document content, images and metadata; user credentials and usage logs; IP address and coarse location; where enabled, identity document images.
Special category data	None required or intentionally processed. See clause 2.4.
Processing locations	United Kingdom and EEA. Primary hosting AWS eu-west-1 (Ireland) and Google Cloud europe-west4 (Netherlands).
Retention	Deletion within thirty (30) business days of the Cessation Date, in accordance with clause 9.
Fraudfinder contact	support@fraudfinderaai.com. Security incidents: support@fraudfinderaai.com.
Company contact	_____, _____, _____
Applicable Controller	As notified by the Company from time to time