Fraudfinder LTD
71-75 Shelton St
London
WC2H 9JQ
United Kingdom

Email: support@fraudfinderai.com

Fraudfinder LTD - Data Protection Policy

*Version:*1.8
Date: 10 September 2025

This document details the Data Protection Policy for Fraudfinder LTD (“Fraudfinder”) located at the commercial premise of 71-75 Shelton Street, WC2H 9JQ, London, UK

Document Owner:	Alexander Siedes, CEO
Next Due for Review:	10 September 2026
Document Classification:	Internal

Contents

Policy Objective

This is the Data Protection Policy for Fraudfinder. The objectives of this Policy are as follows.

- To ensure that Fraudfinder’s customer data is dealt with in a fair, legal and transparent manner
- To support Fraudfinder in applying appropriate controls to data in proportion to the business and privacy risk that data presents
- To define Fraudfinder's approach to record management and archiving

Policy Governance

Roles and Responsibilities
Accountability for the implementation and enforcement of this policy rests with the CEO, who shall also act as the Data Protection Officer.

The Data Protection Officer shall be responsible for owning the relationships with the Information Commissioner's Office and other applicable regulators

Accountability for ensuring this policy continues to meet all legal and regulatory requirements rests with the CEO.

It is the responsibility of all employees to individually comply with all relevant aspects of this policy.

Policy Review & Approval

This policy shall be reviewed and re-approval obtained not less than annually, incorporating input from, at a minimum, the CEO, CTO, COO, and any other relevant stakeholders/professionals as required.

The Fraudfinder Board of Directors is accountable for approval of changes to this policy.

Policy Exceptions

Exceptions to this policy may only be approved by the Data Protection Officer. These must be logged, along with related mitigations, and reviewed by the Board of Directors at least every six months for continued appropriateness.

Definitions & Classifications

Data Subjects
A Data Subject shall be the natural persons that is identifiable from held information

A Data Subject shall be considered identifiable if an individual natural person can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, and online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal Data
Personal data shall mean any information relating to an identified or identifiable natural person ("Data Subject")

Sensitive Personal Data
Sensitive Personal Data shall be defined as anything revealing:

- Racial or ethnic origin

- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Health
- Sex life or sexual orientation
- Genetic or biometric data.

Fraudfinder shall not collect sensitive personally identifiable information unless the Data Subject has consented, or it is legally required, or if it is required for fulfilling a key aspect of the primary purpose for collection.

Information Classification

All information shall be assigned a classification in accordance with the below categories, whether it is held as structured or unstructured data.

Secret Information

Information where the disclosure would result in a very high likelihood of significant harm, whether due to the nature of the data itself (e.g. Sensitive personal data) or where such data increases the risk of exposure of large volumes of other data or systems (e.g. encryption keys). Sensitive Personal Data shall be classified as Secret.

Confidential Information

Information that relates to Fraudfinder's financial details, clients / customers, employees, administration of IT systems or intellectual property and would cause significant financial or reputational damage if it were disclosed. Personal data shall be classified as Confidential or higher.

Internal Information

Information relevant to Fraudfinder's operational business not intended for use outside of Fraudfinder, but with a low risk of harm in the event of exposure

Public Information

Information obtained through public sources, or that is readily available through public sources, and as such does not pose a risk of harm should it be exposed

Inappropriate Information

Inappropriate information shall be defined as information submitted by Users which contains:

- Content that may violate copyrights or trademarks,
- Sexually explicit content,
- Content that is defamatory,
- Encourages or forms part of to the commission of criminal acts,
- Racism,
- Sexism, or
- Abusive or bullying

- Record of an individual's criminal convictions

Inappropriate information shall not be stored on Fraudfinder owned or controlled IT systems and shall be removed immediately, except where preservation is strictly necessary and permissible to support disciplinary or legal proceedings. Data preserved for such proceedings shall be removed at their conclusion.

Consent

Consent is the Data Usage that a Data Subject has agreed to.

Consent of a Data Subject shall only be regarded as valid if it is:

- Freely given
- Specific
- Informed
- Unambiguous
- Supported by either by a statement or by a clear affirmative action, indicating agreement to personal data relating to them being processed

Data Usage

Data usage shall include the collection, processing, modification, transfer, disclosure, storage and deletion of data.

Data Breach

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed

Privacy Breach

Privacy Breach means any Data Breach relating to Personal Data

Partner Organisations

Partner Organisations shall encompass any organisation on whose behalf Fraudfinder operates as a Data Processor

Data Suppliers

Suppliers where Fraudfinder legally obtains Personal Data as part of a commercial arrangement (e.g. reference checking)

Data Principles

Collection & Minimisation

Personal Data shall only be collected where a Lawful Basis for processing exists.

Collection of Personal Data shall be limited to data which is adequate, relevant and strictly necessary for purposes for which those data are processed.

Personal Data shall only be collected from the Data Subject directly or received from Partner Organisations and Data Suppliers, and only with a Data Subject's Consent. All other collected personally identifiable information shall be securely destroyed or Consent obtained from the Data Subject.

Consent shall not be obtained through the use of pre-ticked boxes, inaction on the part of the user, silence or any similar methods.

Privacy Notices

At the time of providing Consent, the Data Subject shall be presented with a Privacy Notice containing the following:

- Details of privacy policy and practices;
- Available channel for accessing their personal information and other privacy rights;
- Any planned disclosure of information to third party;
- Organisation and data protection officer contact information;
- Purpose for which the information is being collected;
- Retention periods and planned disclosure of personal information;
- All intended uses of the personal information
- Details of data transfers outside the EEA if any (i.e. how data will be protected and ways to obtain details of the safeguards in place, note ~~Fraudfinder does not currently hold data outside the EEA)~~

The version of the Privacy Notice in force at the time of the granting of Consent shall be recorded for each Data Subject

Least Visibility

Appropriate controls shall be maintained such that employee access to Personal Data shall be restricted to only that data which is strictly required for performance of their duties.

Where processing activities require access to Confidential and Secret data, additional controls shall be implemented to monitor the usage of such data for inappropriate access.

Lawful Basis

Data may not be processed unless there is a Lawful Basis for processing. For this to exist, one of the following must apply:

- The Data Subject has Consented to the processing
- It is necessary for the entry into, or performance of, a contract with the Data Subject or in order to take steps at his or her request prior to the entry into a contract.
- It is necessary for compliance with a legal obligation.
- To protect the vital interests of the Data Subject or of another natural person.
- It is required to comply with employment law
- The data is manifestly made public by the Data Subject
- It relates to legal claims

Processing may also occur when it is necessary to pursue Fraudfinder's (or by a third party) Legitimate Interests, except where the Data Subject's rights are disproportionately impacted.

Data relating to children (<16 years old) shall not be processed except on the basis of a specific contractual or legal obligation.

All Lawful Basis' shall be recorded, along with justifications where Legitimate Interest or Legal Obligations are claimed.

Changing Lawful Basis

Where personal data is to be processed for a new purpose outside the original Lawful Basis, the Data Protection Officer shall consider whether the new purpose is "compatible" with the original purpose taking into account the following factors:

- The link between the original purpose and the new purpose;
- The context in which the data was collected, including Fraudfinder's relationship with the Data Subjects;
- The nature of the personal data, in particular, whether Sensitive Personal Data is included;
- The possible consequences of the new purpose of processing for Data Subjects;
- The existence of appropriate safeguards (e.g., encryption or pseudonymisation).

Changes to the Lawful Basis shall be recorded on the Data Risk Register

If the purposes for which the Fraudfinder is processing the personal data do not require the identification of the Data Subject, the data may be used, however it must be anonymised prior to processing.

Data Accuracy

All Personal Data shall be accurate and kept up to date. Should an error be noted, either through internal activities or through notification by a Data Subject, it shall be corrected at the earliest opportunity

Application Owners shall have the general responsibility to maintain their data sets and proactively monitor data quality.

Data Analytics

Personal Data shall not be used for data analytics except where a Lawful Basis for the analytics exists, or a change in Lawful Basis has been agreed with the Data Protection Officer

Anonymised or Aggregated Data

Personal Data that has been anonymised or aggregated, such that the Data Subject cannot be identified, may be utilised for analytics and market research purposes.

Cross Border Data Flow

Personal Data shall not be transmitted outside the European Economic Area except where the transfer has been risk assessed and adequate legal safeguards have been put in place such as Binding Corporate Rules or EU Model Clauses.

Data & Privacy Processes

Governance

Data Risk Register

The Data Protection Officer shall maintain a record of all data, whether personal or not, held within the organisation, this shall contain:

- A description of the data collected, including identification of any Personal Data or Sensitive Personal Data
- The Information Classification
- Details of the storage arrangements for, and applications processing, the data, whether internal or external to Fraudfinder
- The retention period

For items of Personal Data

- Details of the original Lawful Basis
- Details of any modifications to Lawful Basis
- Details of Consents obtained

For each system holding Personal Data, the register must contain sufficient information to satisfy the Data Protection Officer that the relevant rights of a Data Subject can be enforced, in particular:

- Right of rectification
- Right to erasure
- Right to restrict processing
- Right of data portability
- Right to object to processing
- Right to object to processing for the purposes of direct marketing

Unstructured data shall be logged and governed though equivalent processes, with the Data Protection Officer having accountability for implementation of appropriate controls (e.g. DLP, data discovery)

This register shall be owned by the Data Protection Officer and shall be reviewed not less than on an annual basis

Data Flow Management

All data flows, both internal and external, shall be documented such that:

- The flow of Personal Data can be traced throughout the information lifecycle
- Flows of Confidential and Secret information can be confirmed to be protected in accordance with the risk associated with such flows

In confirming the protections, the following shall be considered as a minimum:

- Whether there is a mechanism to record access to data e.g. Logs
- Granularity of user access controls for access the Personal Data / special categories of data
- Approvals for and periodic review of access rights for users accessing personal data / special categories of data
- Security technologies applied (e.g. encryption, pseudonymisation)

These shall be reviewed by the Data Protection Officer not less than annually.

Confidentiality Agreements

All individuals with access to Secret, Confidential or Internal information shall be bound to confidentiality through a legally binding agreement, either as part of their contract of employment or through a supplementary NDA.

Data Privacy Awareness

The Data Protection Officer shall ensure that all employees are aware of Data Protection requirements and the importance of and their responsibilities with regards to privacy and data protection.

All employees must complete appropriate training, with regard to their role, within 14 days of joining the organisation, and annually thereafter. The Data Protection Officer shall monitor compliance.

Data Privacy Reporting

The Data Protection Officer shall report annually to the management board on data protection issues, including:

- Key data risks
- Major changes to Fraudfinder's data strategy
- Incidents resulting in Data Breaches, along with progress of remedial actions and lessons learned
- Future plans, including legal/regulatory updates as appropriate

The Data Protection Officer shall ensure that Privacy is considered when developing the annual audit plan.

Technology & Change

Privacy by Design

Privacy shall be formally considered during the design and implementation of all systems, in particular the approach to data and access minimisation shall be explicitly documented, along with updates to the Data Flow documentation.

Where a change to a previously implemented system has an impact on privacy, such an assessment will be repeated.

Data Subject Rights

All systems developed in-house shall be designed such as to support the following:

- Ability to remove a Data Subject's Personal Data
- Ability to correct a Data Subject's Personal Data

- Ability to prevent further processing of a Data Subject's Personal Data
- Ability to extract a Data Subject's Personal Data in machine readable format
- Ability to record a preference for direct marketing (if relevant)

All third party systems, where Fraudfinder acts as Data Controller, shall have their ability to meet these criteria evaluated. Where it is not technically feasible, this shall be recorded in the Data Flow Management documentation.

Third Party Management

Disclosing Personal Data

Fraudfinder shall not disclose personally identifiable information unless one of the following applies:

- The Data Subject has given explicit Consent
- The disclosure is legally required
- It is reasonably expected to be required to fulfil the primary purpose of collection
- The data has sufficiently been anonymised so as to make the Third Party unable to identify the Data Subject

Third Party Management

Fraudfinder shall ensure that where a Third Party processes data on behalf of Fraudfinder:

- Have records of processing activities in place
- Acknowledge their obligations to notify Fraudfinder in their capacity as Data Controller
- Have appropriate security controls in place in proportion to the Privacy risk
- Have documented allocations of shared roles & responsibilities as Data Controller and Data Processor

Data Subject Rights & Requests

Requirement for External Privacy Policy

Fraudfinder shall publish an external data privacy policy defining scope, approach and responsibilities in processing and safeguarding Personal Data of people outside of the organisation.

Exercising Rights

Data Subjects may request Fraudfinder to disclose, correct or delete all personally identifiable information stored relating to them. All requests shall be coordinated by the Data Protection Officer.

-

Application Owners shall be accountable for ensuring that data on their systems is correctly updated or deleted (as applicable) as rapidly as practicable.

Processing Access Requests

The Data Protection Officer who shall respond if appropriate within one month from the data of request

The Data Protection Officer shall coordinate a response to the requesting Data Subject within the one month timeframe.

The response shall provide:

- Confirmation of whether, and where, Fraudfinder is processing their personal data
- Information about the purposes of the processing
- Information about the categories of data being processed
- information about the categories of recipients with whom the data may be shared
- Information about the period for which the data will be stored (or the criteria used to determine that period)
- Information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing
- Information about the existence of the right to complain to the ICO
- Where the data was not collected from the Data Subject, information as to the source of the data
- Information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on Data Subjects.
- Additionally, Data Subjects may request a copy of the personal data being processed.

Access Request Denial

An access request may be denied if one of the following conditions applies:

- The request is excessive in nature (e.g. repeated requests),
- The Data Subject is currently involved in related legal proceedings,
- The requestor is not the Data Subject (with the exception of legal guardians),
- The request is incomplete, or
- The request is not submitted in writing.

Managing Complaints

All complaints relating to data privacy shall be forwarded to the Data Protection Officer.

Withdrawal of Consent

Fraudfinder shall make available a simple process for withdrawing of consent to processing and publish this such that it can be accessed by Data Subjects. The Data Protection Officer shall be responsible for coordinating the response to such requests

Restriction of Processing

Where Lawful Basis relies on Consent, processing shall be restricted immediately if one of the following applies:

- Accuracy of the data is contested

- Processing is not supported by a lawful basis
- The personal data is no longer needs the data for their original purpose
- The Data Subject has requested erasure and this has not been executed yet

Where accuracy is contested, restriction is only necessary for as long as it takes to verify that accuracy

Objection to Processing

Where Lawful Basis relies on Legitimate Interest, processing shall be restricted immediately unless one of the following overriding grounds applies:

- There are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject
- The data is required the data in order to establish, exercise or defend legal rights

Where one of the above conditions exist, Fraudfinder shall provide the Data Subject with an explanation as to the reason for continued processing.

Right of Erasure

Where a request for erasure is received, the Data Subject's Personal Data shall be removed from all Fraudfinder systems providing one of the following applies:

- The data is no longer needed for their original purpose, and no new lawful purpose exists
- The lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
- The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
- The data has been processed unlawfully
- The erasure is necessary for compliance with EU law or the national law of the relevant Member State

Opt Out of Marketing

Fraudfinder shall not contact anyone who has requested to opt out of being contacted for marketing purposes, or where consent was not explicitly obtained for such use at the time of collection.

Breach Management

Breach Management

The Data Protection Officer shall ensure that incident response processes take into account the specific needs of Data and Privacy Breaches, including as a minimum: Obligation to notify management immediately

Privacy Breach

Notification to Data Controllers

Where Fraudfinder acts as a Data Processor, the breach shall be immediately reported to the Data Controller.

Notification to ICO

In the event of a Privacy Breach, the Data Protection Officer, or authorised deputy, must report the breach to the DPA without undue delay, and in any event within 72 hours of becoming aware of the breach unless, on the basis of the nature of the breach, and the precautions taken (e.g. encryption), the Data Protection Officer is satisfied the data breach is unlikely to result in any harm to Data Subjects.

The notification must include at least:

- A description of the data breach, including the numbers of Data Subjects affected and the categories of Personal Data affected
- The name and contact details of the DPO (or authorised deputy)
- The likely consequences of the data breach
- Any measures taken to remedy or mitigate the breach

Notification to Data Subjects

Should a Privacy Breach result in a high risk to Data Subjects (in the opinion of the Data Protection Officer), Fraudfinder shall notify the affected Data Subjects without undue delay. The notification must include at least:

- The name and contact details of the DPO (or other relevant point of contact);
- The likely consequences of the data breach;
- Any measures taken by the controller to remedy or mitigate the breach.

In considering the level of risk, the Data Protection Officer shall have regard for whether:

- The nature of the data impacted (particularly Sensitive Personal Data)
- The affected data is protected (e.g., through strong encryption)
- Effective measures can be taken to protect against the harm (e.g., suspending affected accounts)

Should the Data Protection Officer consider the risk of harm is high, however the effort required to reach individual Data Subjects is disproportionate, the Data Protection Officer may elect to make a public notification of the breach by any appropriately public form.

Breach Recording

The Data Protection Officer shall record the details of all Privacy Breaches, including the facts and effects of the breach and any remedial action taken

Archiving and Data Retention

Collection Purpose Related Storage

Data collected for different purposes shall be stored so that they are distinguishable and can be aligned to the respective primary purpose of collection.

Retention Periods

Information shall be retained and archived in compliance with all local and relevant international laws and regulation.

Personal Data may only be stored as long as it is required to fulfil the Lawful Basis for processing for which it was collected, except where required by law or with explicit permission of the Data Subject.

Where not otherwise specified, Commercial Information shall be retained for 10 years.

Commercial information includes

- Correspondence with clients / customers,
- Communication between staff and management,
- Communications with vendors / suppliers relating to a transaction,
- Communication with law enforcement or regulators,
- Information relating to accounting,
- Information relating to transfer pricing,
- Information relating to intellectual property owned by the organisation
- Any information that may have relevance for litigation.

Anonymisation

Where Personal Data is retained solely on the basis of Legitimate Interest, explicit consideration shall be given as to whether, if the data were to be anonymised, the legitimate interest can still be met. If the Legitimate Interest can be met by anonymised data, the anonymization shall be performed at the earliest opportunity.

Archiving Arrangements

Fraudfinder shall run a backup of data on a daily basis and will archive that data, in line with the relevant retention period, utilising Amazon Web Services within the European Economic Area

Archived Data Accessibility

When transitioning to a different media or software platform, the structure and context of archived data shall remain restorable for the remainder of the legal or regulatory retention period.

Retrieval

All archived information shall be retrievable within a timeframe without impacting dependent business processes.

Data Deletion

All physical and electronic data no longer relevant to Fraudfinder's business shall be destroyed securely if not required to be retained by law or after the end of the legal retention period.

Where practicable, the deletion should be automatic, in other cases the Data Protection Officer is responsible for ensuring that the deletion is performed and shall review this position every 6 months.

Secure Storage

All archived physical data shall be stored in a location that is appropriately protected from unauthorised access, as well as natural influences such as water and fire.

Physical security precautions shall include a safe rated to at least EN-1143-1 Grade 0 standards, as well as pass controlled access, building alarms and cameras.

Document Control

Version	Date	Prepared By	Approved By	Changes
1.1	09/12/2017	Alexander Siedes	N/A	
1.2	09/12/2018	Alexander Siedes	N/A	
1.3	09/12/2019	Alexander Siedes	N/A	
1.4	09/12/2020	Alexander Siedes	N/A	Address
1.5	09/12/2021	Alexander Siedes	N/A	
1.6	09/12/2022	Alexander Siedes	N/A	
1.7	10/09/2024	Alexander	NA	Address
1.8	10/09/2025	Alexander Siedes	NA	

Approvals

Approved by: Fraudfinder

Policy Owner: Alexander Siedes, Director CEO

On behalf of the Fraudfinder LTD Board: