Data Processing Agreement

This Data Processing Agreement (“DPA”) sets out the terms, requirements, and conditions on which Fireflies.ai will process Client Personal Data for the purposes of the Objective. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (EU) 2016/679 ("GDPR") for contracts between controllers and processors, as well as compliance with the applicable provisions of the GDPR and related EU data protection laws, including the European Data Protection Board (EDPB) guidelines and the EU Commission’s standard contractual clauses (SCCs) where applicable

1. Definitions

The following definition applies in this DPA.

1.1 Definitions:

Client Personal Data: means Personal Data provided by the Client.

Personal Data: means personal data under the definition set out in GDPR.

Fireflies.ai Data: means Personal Data provided by Fireflies,ai.

Objective: means the Services to be provided by Fireflies.ai according to the Terms of Service updated on May 5 2023, which together with the Order Form constitute a legally binding agreement between the parties (“**Agreement**”).

Data Protection Legislation: means all applicable data protection and privacy legislation in force from time to time, including without limitation:

1. The UK GDPR.
2. The Data Protection Act 2018 (and regulations made thereunder) (DPA 2018).
3. The Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.
4. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) as applicable.
5. The ePrivacy Directive (Directive 2002/58/EC) as amended and national implementations thereof, and any successor legislation or regulations applicable in the UK and the EU.

2. Personal data types and processing purposes

2.1 The Client and Fireflies.ai acknowledge and agree that for the purpose of the Data Protection Legislation:

(a) the Client is the Controller and Fireflies.ai is the Processor, save with respect to Fireflies.ai Data for which Fireflies.ai is a Controller.

(b) the Client retains control of Client Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Fireflies.ai; and

(c) Annex A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which Fireflies.ai may process.

3. Fireflies.ai’s obligations

3.1 Fireflies.ai will only process the Client Personal Data to the extent, and in such a manner, as is necessary for the Objective. Fireflies.ai will not process the Client Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Fireflies.ai must promptly notify the Client if, in its opinion, the Client’s instructions do not comply with the Data Protection Legislation.

3.2 Fireflies.ai will maintain the confidentiality of the Client Personal Data and will not disclose the Client Personal Data to third parties unless the Client or this DPA specifically authorises the disclosure, or as required by domestic or EU law, court, or regulator (including the Commissioner). If a domestic or EU law, court, or regulator (including the Commissioner) requires Fireflies.ai to process or disclose the Client Personal Data to a third-party, Fireflies.ai must first inform the Client of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.3 Fireflies.ai will reasonably assist the Client, at no additional cost to the Client, with meeting the Client's compliance obligations under the Data Protection Legislation, taking into account the nature of Fireflies.ai's processing and the information available to Fireflies.ai, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner under the Data Protection Legislation.

3.4 Fireflies.ai must notify the Client promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Fireflies.ai's performance of the Objective or this DPA.

4. Fireflies.ai Data

4.1 Fireflies.ai Data is made available only for use for the purposes of the Objective and must not be made public by the Client. By making Fireflies.ai Data public or using it other than for the purposes for which it is provided, the Client may be in breach of the Data Protection Legislation and the terms of this DPA. The Client shall not transfer or access Fireflies.ai Data outside of the UK or the European Economic Area ("EEA") except with the prior written consent of Fireflies.ai and subject to appropriate safeguards.

4.2 The client is responsible for keeping Fireflies.ai Data safe and using appropriate security measures to prevent unauthorised access, copying, modification, storage, reproduction, display, or distribution of the data. If any unauthorised access occurs, the client must take immediate action to remedy the situation. The security measures used by the service provider must be at least as good as the security measures used by the client to protect their personal data or confidential information.

4.3 If the Client becomes aware of any misuse of any Fireflies.ai Data, or any security breach in connection with the DPA that could compromise the security or integrity of Fireflies.ai Data or otherwise adversely affect Fireflies.ai, or if the Client learns or suspects that any password or other security feature has been revealed to or obtained by any unauthorised person, the Client shall promptly notify Fireflies.ai and fully co-operate with Fireflies.ai to remedy the issue as soon as reasonably practicable.

4.4 The Client understands and acknowledges that Fireflies.ai gives no opinion and makes no recommendation in relation to any persons appearing in Fireflies.ai Data.

5. Fireflies.ai Employees

5.1 Fireflies.ai shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Data.

5.2 Fireflies.ai will take appropriate steps to ensure compliance with the Security Measures (defined below) by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to process your Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with Fireflies.ai.

5.3 Fireflies.ai shall ensure that access to Personal Data is limited to authorized personnel who require such access to perform the Services.

6. Security

6.1 Fireflies.ai is required to take necessary steps to prevent unauthorised or illegal processing, access, disclosure, copying, modification, storage, reproduction, display, or distribution of Client Personal Data. Additionally, Fireflies.ai must take measures to prevent accidental or illegal loss, destruction, alteration, disclosure, or damage of Client Personal Data.

6.2 Fireflies.ai shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data. Fireflies.ai will implement and maintain technical and organizational measures to protect your data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 1 (the "Security Measures", available to those with login credentials). As described in Appendix 1, the Security Measures include measures to protect Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Fireflies.ai's systems and services; to help restore timely access to Personal Data following an incident; and for regular testing of effectiveness. Fireflies.ai may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

7. Personal Data Breach

7.1 Fireflies.ai shall, without undue delay, notify the Client if it becomes aware of:

(a) any accidental, unauthorised, or unlawful processing of the Client Personal Data; or

(b) any Personal Data Breach.

7.2 Following any Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Fireflies.ai will reasonably co-operate with the Client in the Client's handling of the matter, including:

(a) assisting with any investigation.

(b) making available all relevant records, logs, files, data reporting and other materials required to comply with Data Protection Legislation or as otherwise reasonably required by the Client; and

(c) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the personal data breach.

8. Cross-border transfers of personal data

8.1 Fireflies.ai must not transfer or otherwise process Client Personal Data outside the EEA or UK without obtaining the Client's prior written consent, such consent not to be unreasonably withheld, conditioned or delayed provided that all transfers by Fireflies.ai of Client Personal Data shall (to the extent required under the Data Protection Legislation) be affected by way of appropriate safeguards and in accordance with Data Protection Legislation.

8.2 If any Client Personal Data transfer between the Client and Fireflies.ai requires execution of Standard Contractual Clauses ("**SCC**'s") in order to comply with the Data Protection Legislation (where the Client is the entity exporting Client Personal Data to Fireflies.ai outside the EEA), the parties will complete all relevant details in, and execute the SCC's, and take all other actions required to legitimise the transfer. The SCC's are part of this DPA as Annex A.

9. Subcontractors

9.1 The Client grants to Fireflies.ai specific authorisation to appoint the sub-processors listed in Annex A in connection with the Objective.

9.2 Subject to clause 8.1, Fireflies.ai may only authorise a subcontractor to process the Client Personal Data if:

(a) the Client is provided with an opportunity to object to the appointment of each subcontractor within fourteen (14) days after Fireflies.ai supplies the Client with details regarding such subcontractor; and

(b) Fireflies.ai enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures.

9.3 Where the subcontractor fails to fulfil its obligations under such written DPA, Fireflies.ai remains fully liable to the Client for the subcontractor's performance of its DPA obligations.

10. Complaints, data subject requests and third-party rights

10.1 Fireflies.ai shall provide such information to the Client as the Client may reasonably require, to enable the Client to comply with:

(a) the rights of data subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Client by any supervisory authority under the Data Protection Legislation.

10.2 Fireflies.ai must notify the Client immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Client Personal Data or to either party's compliance with the Data Protection Legislation.

10.3 Fireflies.ai must notify the Client within seven (7) working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

10.4 Fireflies.ai will give the Client its full co-operation and assistance in responding to any complaint, notice, communication, or data subject request.

10.5 Fireflies.ai must not disclose the Client Personal Data to any Data Subject or to a third party other than at the Client’s request or instruction, as provided for in this DPA or as required by law.

11. Data return and destruction

11.1 At the Client’s request, Fireflies.ai will give the Client a copy of or access to all or part of the Client’s Personal Data in its possession or control.

11.2 On expiry or termination of this DPA, Fireflies.ai will securely delete or destroy or, if directed in writing by the Client, return, all or any Client Personal Data related to this DPA in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires Fireflies.ai to retain any documents or materials that Fireflies.ai would otherwise be required to return or destroy, it will notify the Client in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

12. Records

12.1 Fireflies.ai will keep accurate and up-to-date written records regarding any processing of Client Personal Data it carries out for the Client, including but not limited to, the access, control and security of the Client Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 6.1 ("**Records**").

12.2 Fireflies.ai will ensure that the Records are sufficient to enable the Client to verify Fireflies.ai's compliance with its obligations under this DPA and Fireflies.ai will provide the Client with copies of the Records upon request.

13. **miscellaneous**

13.1 This DPA will take effect on the execution date (the "Effective Date") and will remain in effect until, and automatically expire upon, the deletion of all of your Personal Data by Fireflies.ai as described in this DPA.

13.2 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

13.3 Where Your Affiliates are Data Controllers of the Personal Data, they may enforce the terms of this DPA against Fireflies.ai directly.

13.4 This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one DPA.

Name: _____	Name:_____
Title: _____	Title:_____
Signature:_____	Signature:_____
Date: _____	Date:_____

Annex A:

STANDARD CONTRACTUAL CLAUSES
(MODULE TWO – CONTROLLER TO PROCESSOR)

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

Not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions
(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation
The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal

data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy
If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data
Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing
(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and

the information available to the data importer.

8.7 Sensitive data
Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers
The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance
(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including

in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8.

The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.
(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non- material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical, or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges,

etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(c).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as

required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts mutually agreed by both parties

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex 1 to Schedule A

A. LIST OF PARTIES
Data exporter(s):

Name:
Address:
Contact person's name, position and contact details:
Activities relevant to the data transferred under these Clauses:
Signature and Date: as per execution date.
Role (controller/processor): controller

Data importer(s):
Name: Fireflies.ai
Address: 201 Spear St Ste 16, San Francisco, California, 94105, United States
Sam Udotong
Activities relevant to the data transferred under these Clauses: provision of the Services.
Signature and Date: as per execution date.
Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

● Prospects, customers, business partners and vendors of data exporter (who are natural persons).

● Employees or contact persons of data exporter's prospects, customers, business partners and vendors.

● Employees, agents, advisors, freelancers of data exporter (who are natural persons).

● Data exporter's Users authorized by data exporter to use the Services.

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

<u>Personal Data Categories:</u>

The personal data transferred concern the following categories of personal data: data provided by the account owner Host and meeting participants in order for the data importer to provide the Services as described under the Agreement, including:

- Information provided in connection with registering an account, including name, company name, e-mail, physical address, phone number, and any other information provided.
- Information provided in order to authenticate an account, including account name, password, and any other information provided.
- Information provided in connection with completing a transaction or purchase using the Services.
- Information provided in connection with using the Services, including name, company name, email address, physical address, phone number, and any other information provided.

- Information provided via email, through the “Contact” section on the website or by using the contact details listed on various parts of the website, including name, company name, e-mail address, physical address, phone number;
- Information provided in order to subscribe to our newsletters and updates, including email address, the topic for which the user wish to receive updates, or any other information you decided to bee provided. Users may always unsubscribe from these emails by following the instructions included.
- If controller are one of our customers, suppliers or prospects, we may process limited Personal Information in the course of our business relation, for example when place an order, request a demo or vice versa. Such Personal Information may include name, company, title, e-mail address, phone number, address, order details, and where applicable and relevant, credit registrations and credit limits;
- Transaction and limited (non-PCI) payment data;
- Meeting titles and calendar metadata;
- Encrypted derivatives of transcript data such as summaries;
- Any other information that may wanted to be shared with us, such as Personal Information related to recruitment / job applications.

The parties do not intend for any sensitive data, including special category data, to be processed under the Agreement.

Frequency of Transfer

Personal data will be transferred to the importer on a continuous basis throughout the duration of the Services.

Nature of the Processing

Processing of personal data that the exporter elects, in its discretion, to send to the importer in connection with the use of the Services purchased by the exporter, and as otherwise permitted by the Agreement.

Purpose(s) of the Data Transfer and Further Processing

The data transfer and further processing are for the operation, support, use, or provisioning of the Services.

Retention Period

The period of retention is as set out in the Agreement.

Transfers to (Sub-)Processors

Sub-processors are used by the data importer throughout the entire duration of the Agreement. The subject matter, nature, and duration of the processing by sub-processors are as follows:

Subject Matter: Processing personal data in connection with the Services.
Nature: Operations necessary to provide and support the Services.
Duration: For the entire duration of the Agreement.

The current sub-processors used by the data importer as of the date of this Data Processing Agreement (DPA) are listed in the Sub-processor List.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13. The competent supervisory shall be either (i) the supervisory authority of Ireland, or (ii) otherwise determined in accordance with the GDPR.

Approved Sub-processors:

Name of sub-processor	**Location of the sub-processor**	**Purpose**	**website**
Amazon Web Services	USA	Data Management	https://aws.amazon.com/
Assembly.ai	USA	Transcription Service	https://www.assemblyai.com
Google Cloud Platform	USA	Data Management	https://cloud.google.com/
MongoDB Atlas	USA	cloud-based database service	https://www.mongodb.com/atlas
OpenAI	USA	Large Language Model Service: We signed a BAA with Open AI and subscribed for ZERO data retention with Openai. Zero retention was applied to Fireflies	https://openai.com/
Anthropic	USA	Large Language Model	https://www.anthropic.com/

Annex 2 of Schedule A

Overview of Fireflies.ai's Technical and Operational Security Measures

Confidentiality

- **Electronic Access Control**:Fireflies.ai's systems are designed to prevent unauthorised use of our data processing and storage systems. We also utilize (secure) passwords, automatic blocking/locking mechanisms and two-factor authentication.
- **Internal Access Control**:(i.e., permissions for user rights of access to and amendment of data): We create and maintain strict Access Control Lists (ACL's). All incoming requests to our systems seeking access to personal data are authenticated to prevent unauthorised reading, copying, changes or deletions of data within the system. Each user and subsystem has access to the minimal set of resources it requires to function and no more (i.e., least privileged). We also log and audit system access events.

Integrity

- **Data Transfer Controls**: All data is encrypted in transit and at rest. Over-the-wire encryption uses RSA 2048 bits keys. At rest, we encrypt files using 256-bit Advanced Encryption Standard (AES-256); we utilize some of the strongest block ciphers and encryption techniques available. We store our recordings on Amazon's S3 where they are protected using server-side encryption and transferred over a secure TLS connection. Our metadata are stored in databases on our hosting providers which are also encrypted at rest and with which we communicate over secure connections.
- **Data Entry Control**: Our systems contain access logs to enable us to verify whether and by whom personal data is entered into our systems – or is changed or deleted.
- **Local Devices & Corporate Network**: Our employees' machines are password-protected and the storage devices we use are encrypted; our corporate network sits behind a firewall and a VPN.

Data Center

- **Infrastructure**: Fireflies.ai utilizes geographically distributed data centers.
- **Redundancy**: Fireflies.ai infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated risks. Most services have been designed to allow Fireflies.ai to release enhancements or corrective maintenance without service interruption. Maintenance is scheduled through a process according to internal policies.
- **Server Operating Systems**: Most Fireflies.ai servers use a Linux-based implementation. Data is stored using algorithms which secure the data in order to enhance all products in production environments.
- **Personnel Security**: Fireflies.ai personnel are required to conduct themselves in a manner consistent with the company's guidelines, professional standards, ethics and confidentiality requirements. Fireflies.ai employees are contractually bound to confidentiality. Personnel handling customer data are required to have a higher level of knowledge, authorization, and training regarding such access.
- **Subprocessor Security**: From time to time Fireflies.ai will employ carefully selected data SubProcessors. Fireflies.ai conducts diligence on the business suitability, reputation, and technical skills of our SubProcessors. Once Fireflies.ai has assessed the suitability of the Subprocessor, Fireflies.ai subjects our SubProcessors to the minimum-security requirements for a Fireflies.ai Subprocessor.

Availability and Resilience

- **Availability Control**: Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning.
- **Rapid Recovery**: Fireflies.ai replicates data over multiple systems to help to protect against accidental destruction or loss. Fireflies.ai has designed and regularly plans and tests its business continuity planning/disaster recovery programs.
- **Penetration Testing**: At Fireflies.ai, ensuring a culture of cybersecurity and hygiene is crucial to protect our users and their data. We work with skilled security researchers and white-hat hackers to identify security issues.

Procedures for regular testing, assessment and evaluation

- **Data Protection Management**: Fireflies.ai maintains an information security program which includes internal policies and procedures designed to secure data against accidental or unlawful loss, access or disclosure, identify to security and unauthorized access our systems, and minimize security risks, including through risk assessment and regular testing.
- **Penetration Testing**: At Fireflies.ai, ensuring a culture of cybersecurity and hygiene is crucial to protect our users and their data. We work with skilled security researchers and white-hat hackers to identify security issues.
- **Cyber Hygiene**: The security-first culture we're fostering at Fireflies.ai starts with our individual commitment to cyber hygiene (personal and professional accounts alike).
- **Passwords**: All employees protect their accounts using strong passwords, the most critical of which are required to be updated regularly, and we employ multifactor authentication (MFA).
- **Local Devices & Corporate Network**: Our employees' machines are password-protected and the storage devices we use are encrypted; our corporate network sits behind a Unified Threat Management firewall and a VPN.
- **Incident Response Management**: Fireflies.ai has an incident response plan and monitors a variety of communication channels for security incidents, and our security personnel will react promptly to known incidents.
- **Incident Response Communications**: Any security event that materially impacts our customers will result in a customer notification through an account team.
- **Order or Contract Control:** All data processing via Integration Partners is done solely at the request of each client and no data processing operations may take place without instructions from each client. Fireflies.ai takes reasonable steps to evaluate the privacy and security practices of each Subprocessor and each Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms with Fireflies.ai.