

DATA PROCESSING AGREEMENT

Made pursuant to Article 28 of the UK General Data Protection Regulation

Version 1.0 · Effective 24 August 2026 · fuzzy.studio/dpa

PARTIES

The Controller	The person or entity that accepts this Agreement in the course of ordering or subscribing to the Services, as identified in the Order ("the Controller", "you")
The Processor	Fuzzy Studio Ltd, a company registered in England and Wales under company number 16128918, whose registered office is at Horizon House, Sittingbourne Road, Maidstone, Kent ME14 3EN, registered with the Information Commissioner's Office under reference ZB832686 ("the Processor", "we", "us")
Effective date	The date on which the Controller accepts this Agreement, or the date the Services commence, whichever is earlier.

BACKGROUND

- A The Processor provides the Controller with the services described in Schedule 1 ("the Services") under the Processor's Terms of Business, together with the order, subscription or quotation accepted by the Controller (together, "the Principal Agreement").
- B In providing the Services, the Processor processes personal data on behalf of the Controller. The Controller is the controller and the Processor is the processor in respect of that personal data.
- C Article 28(3) of the UK GDPR requires that such processing be governed by a written contract. This Agreement is that contract. It forms part of, and is subject to, the Principal Agreement.
- D This Agreement is accepted electronically. The Controller enters into this Agreement by ticking the box confirming acceptance of the Processor's Terms of Business and this Agreement, by clicking the button to place an order or subscribe where that button is presented together with a statement that doing so constitutes acceptance, or by continuing to use the Services. Article 28(9) of the UK GDPR provides that such a contract may be in electronic form, and no signature is required for it to bind the parties.
- E The Processor records the identity of the person accepting, the date and time of acceptance, and the version of this Agreement accepted. The Controller may request a copy of that record, or a countersigned copy of this Agreement, at any time by contacting the Processor.

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement:

- (a) "Data Protection Legislation" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and any other applicable law relating to the processing of personal data, in each case as amended or replaced from time to time;
- (b) "UK GDPR" has the meaning given in section 3(10) of the Data Protection Act 2018;
- (c) "Personal Data" means the personal data described in Schedule 1 that is processed by the Processor on behalf of the Controller under the Principal Agreement;
- (d) "Sub-processor" means any third party engaged by the Processor to process Personal Data on the Controller's behalf;

- (e) "Restricted Transfer" means a transfer of Personal Data to a country or territory outside the United Kingdom which is not the subject of adequacy regulations under the Data Protection Act 2018;
 - (f) the terms "controller", "processor", "data subject", "processing", "personal data breach" and "supervisory authority" have the meanings given to them in the UK GDPR.
- 1.2 A reference to a statute or statutory provision includes any subordinate legislation made under it and any amendment or re-enactment of it.
- 1.3 In the event of any conflict between this Agreement and the Principal Agreement in relation to the processing of Personal Data, this Agreement prevails.

2. STATUS OF THE PARTIES AND SCOPE

- 2.1 The parties acknowledge that, for the purposes of the Data Protection Legislation, the Controller is the controller and the Processor is the processor in respect of the Personal Data.
- 2.2 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of data subject are set out in Schedule 1.
- 2.3 The Controller warrants that it has a lawful basis for the processing described in Schedule 1, that it has provided all necessary privacy information to data subjects, and that its instructions to the Processor will not cause the Processor to breach the Data Protection Legislation.
- 2.4 Each party shall comply with its own obligations under the Data Protection Legislation. Nothing in this Agreement relieves either party of its own direct responsibilities.

3. PROCESSING ON DOCUMENTED INSTRUCTIONS

- 3.1 The Processor shall process the Personal Data only on the documented instructions of the Controller, including in relation to Restricted Transfers, unless required to do otherwise by law to which the Processor is subject.
- 3.2 The Principal Agreement, this Agreement and Schedule 1 constitute the Controller's initial documented instructions. Further instructions must be given in writing (including by email) and may be recorded as a variation to Schedule 1.
- 3.3 Where the Processor is required by law to process the Personal Data other than on the Controller's instructions, it shall inform the Controller of that legal requirement before processing, unless the law prohibits it from doing so on important grounds of public interest.
- 3.4 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the Data Protection Legislation. The Processor may suspend the affected processing until the instruction is confirmed, amended or withdrawn.
- 3.5 The Processor shall not sell, share, disclose or otherwise use the Personal Data for its own purposes, including for the training of artificial intelligence or machine learning models, or for marketing to data subjects on its own behalf.

4. CONFIDENTIALITY

- 4.1 The Processor shall ensure that any person authorised to process the Personal Data is subject to a binding duty of confidentiality, whether by contract of employment, written undertaking or statutory obligation.
- 4.2 The Processor shall limit access to the Personal Data to those personnel and Sub-processors who need access in order to provide the Services.
- 4.3 The Processor shall ensure that persons with access to the Personal Data are appropriately trained in their data protection responsibilities.

5. SECURITY

- 5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk to data subjects, the Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, as required by Article 32 of the UK GDPR.
- 5.2 The measures in place as at the Effective Date are described in Schedule 2. The Processor may update those measures from time to time provided that the level of protection is not reduced.
- 5.3 The Processor shall regularly test and evaluate the effectiveness of those measures.

6. SUB-PROCESSORS

- 6.1 The Controller gives the Processor general written authorisation to engage Sub-processors, subject to this clause 6.
- 6.2 The Sub-processors authorised as at the Effective Date are listed in Schedule 3.
- 6.3 The Processor shall give the Controller at least 30 days' written notice before engaging any additional or replacement Sub-processor. The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, either party may terminate the affected Services on written notice, without penalty to the Controller.
- 6.4 The Processor shall impose on each Sub-processor, by written contract, data protection obligations that are no less protective than those set out in this Agreement.
- 6.5 The Processor remains fully liable to the Controller for the performance of each Sub-processor's obligations.

7. INTERNATIONAL TRANSFERS

- 7.1 The Processor shall not make a Restricted Transfer of the Personal Data unless it has first put in place a lawful transfer mechanism under Chapter V of the UK GDPR, such as the ICO's International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or the transfer being made to a recipient certified under an applicable UK extension to a data privacy framework.
- 7.2 The Restricted Transfers taking place as at the Effective Date, and the transfer mechanism relied on for each, are identified in Schedule 3.
- 7.3 The Processor shall carry out and document a transfer risk assessment where one is required, and shall provide a copy to the Controller on request.

8. ASSISTANCE WITH DATA SUBJECT RIGHTS

- 8.1 The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests from data subjects exercising their rights under Chapter III of the UK GDPR.
- 8.2 The Processor shall notify the Controller without undue delay, and in any event within three working days, if it receives a request from a data subject relating to the Personal Data. The Processor shall not respond to that request itself unless authorised in writing by the Controller or required to do so by law.
- 8.3 The Processor shall provide the assistance described in this clause at no additional charge, save where the assistance required is materially disproportionate to the scale of the Services, in which case the Processor's standard rates shall apply and shall be agreed in advance.

9. PERSONAL DATA BREACHES

- 9.1 The Processor shall notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting the Personal Data.

- 9.2 That notification shall, so far as the information is available, describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed to address it, and the name and contact details of a point of contact.
- 9.3 The Processor shall take all reasonable steps to contain and investigate the breach, shall preserve relevant evidence, and shall keep the Controller informed as further information becomes available.
- 9.4 The Processor shall not notify a supervisory authority, a data subject or any third party of a breach affecting the Personal Data unless required to do so by law, or unless the Controller has first authorised it in writing.

10. ASSISTANCE WITH THE CONTROLLER'S WIDER OBLIGATIONS

- 10.1 The Processor shall provide the Controller with reasonable assistance, taking into account the nature of the processing and the information available to it, in complying with the Controller's obligations under Articles 32 to 36 of the UK GDPR, including in relation to security, breach notification, data protection impact assessments and prior consultation with the supervisory authority.

11. RECORDS, INFORMATION AND AUDIT

- 11.1 The Processor shall maintain written records of all categories of processing carried out on behalf of the Controller, as required by Article 30(2) of the UK GDPR.
- 11.2 The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the UK GDPR.
- 11.3 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller. Such audits shall be carried out on at least 30 days' written notice, no more than once in any twelve-month period (except where required by a supervisory authority or following a personal data breach), during normal business hours, and in a manner that does not unreasonably disrupt the Processor's business.
- 11.4 The Controller shall ensure that any auditor it mandates is bound by appropriate obligations of confidentiality.

12. RETURN AND DELETION

- 12.1 On termination or expiry of the Principal Agreement, or at any earlier point on the Controller's written request, the Processor shall at the Controller's option either return the Personal Data to the Controller or securely delete it, and shall delete all existing copies, unless it is required by law to retain a copy.
- 12.2 Where the Controller requests return, the Processor shall provide the Personal Data within ten working days in a commonly used, machine-readable format such as CSV, together with any associated documents in their native format.
- 12.3 Where the Processor is required by law to retain a copy, it shall inform the Controller of that requirement and shall continue to protect the retained Personal Data in accordance with this Agreement for as long as it is retained.
- 12.4 The Processor shall certify in writing that it has complied with this clause 12 if the Controller asks it to do so.

13. LIABILITY

- 13.1 Each party's liability arising out of or in connection with this Agreement is subject to the limitations and exclusions of liability set out in the Principal Agreement.
- 13.2 Nothing in this Agreement limits or excludes either party's liability where such limitation or exclusion is not permitted by law, or affects the rights of data subjects under Article 82 of the UK GDPR.

14. TERM, VARIATION AND GENERAL

- 14.1 This Agreement takes effect on the Effective Date and continues for as long as the Processor processes Personal Data on behalf of the Controller. Clauses 4, 12 and 13 survive its termination.
- 14.2 The parties shall negotiate in good faith any variation to this Agreement that is necessary as a result of a change in the Data Protection Legislation or guidance issued by a supervisory authority.
- 14.3 This Agreement is versioned. The version accepted by the Controller continues to apply to it until a new version is accepted. Where the Processor issues an updated version, it shall give the Controller not less than 30 days' written notice, and the updated version shall apply from the end of that period unless the Controller objects in writing on reasonable data protection grounds, in which case the parties shall discuss the objection in good faith. Superseded versions are retained by the Processor and available on request.
- 14.4 No update issued under clause 14.3 shall reduce the level of protection afforded to the Personal Data or to data subjects.
- 14.5 Notices under this Agreement shall be given in writing to the contacts identified in Schedule 1.
- 14.6 No third party has any right to enforce any term of this Agreement under the Contracts (Rights of Third Parties) Act 1999.
- 14.7 If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions continue in full force.
- 14.8 This Agreement is governed by the law of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

SCHEDULE 1 — DETAILS OF THE PROCESSING

The mandatory details of the processing, as required by Article 28(3) of the UK GDPR. "Order" means the order, subscription, quotation or sign-up form under which the Controller purchases the Services.

Subject matter	The provision by the Processor of the Fuzzy Logic App — a hosted customer relationship, communications and marketing platform — together with any website design, hosting, automation, support or related digital services included in the Controller's Order.
Duration	For the term of the Principal Agreement, and thereafter only for so long as is necessary to comply with clause 12.
Nature of the processing	Collection, recording, organisation, structuring, storage, retrieval, consultation, use, transmission, hosting, backup, erasure and destruction of the Personal Data, by automated and manual means, as necessary to provide the Services.
Purpose of the processing	To enable the Controller to communicate with and manage its own clients and prospective clients, to operate its website and enquiry forms, to deliver marketing communications authorised by the Controller, and to administer its own internal workflows, in each case only to the extent covered by the Controller's Order.
Types of personal data	Identification and contact data: name, business and personal email address, telephone and mobile number, postal address. Relationship data: employer or business name, job title, client or enquiry status, service interest, contract and account details. Communications content: the content and metadata of emails, SMS, instant messages, web chat, form submissions, call recordings and call transcripts. Behavioural data: website activity, email opens and clicks, appointment and booking history, marketing preferences and consent records. Financial data: invoice and payment status and transaction references, where the Controller uses the Services for invoicing or payment collection. The precise categories depend on the data the Controller chooses to enter into or collect through the Services. The Controller determines what is collected. Special category data: none is intended to be processed. Where the Controller's use of the Services would involve special category data under Article 9, or criminal offence data under Article 10, the Controller shall notify the Processor and the parties shall agree any additional measures in writing before that processing begins.
Categories of data subject	The Controller's clients and their personnel; the Controller's prospective clients and enquirers; the Controller's suppliers and professional contacts; the Controller's own personnel who use the Services; website visitors and recipients of the Controller's communications.
Controller's contact	The individual named as the account or billing contact in the Controller's Order, unless the Controller notifies the Processor of a different data protection contact in writing.

Processor's contact	Fuzzy Studio Ltd Email: sam@fuzzy.studio Post: Horizon House, Sittingbourne Road, Maidstone, Kent ME14 3EN
----------------------------	--

SCHEDULE 2 — TECHNICAL AND ORGANISATIONAL MEASURES

The measures in place as at the Effective Date, as required by clause 5 and Article 32 of the UK GDPR. Measures are described at two levels: those provided by the platform on which the Services run, and those operated by the Processor itself.

Platform-level measures

- The Services run on the HighLevel platform, which encrypts Personal Data in transit using TLS and at rest using industry-standard encryption.
- The platform provider maintains automated backups, documented restoration procedures and ongoing availability monitoring across its hosting infrastructure.
- The platform provider operates its own access control, logging and intrusion detection measures, and makes its security documentation available on request.
- The Processor reviews the platform provider's security and data protection terms and does not disable or weaken the platform's security controls.

Access control

- Multi-factor authentication is enforced on all accounts with access to the Personal Data.
- Access to the Personal Data is limited to named individuals on a least-privilege basis, and is reviewed at least annually.
- Credentials are held in a dedicated password manager and are not shared by email or instant message.
- Access is revoked promptly when an individual ceases to require it, or when the Principal Agreement ends.

Devices

- Devices used to access the Personal Data have full-disk encryption enabled.
- Devices are kept current with vendor security updates and are protected by automatic screen lock and strong authentication.
- Personal Data is not stored on removable media.

Organisational measures

- Any individual with access to the Personal Data, whether employee or contractor, is bound by a written duty of confidentiality.
- The Processor maintains a written record of the categories of processing carried out on behalf of each controller, as required by Article 30(2) of the UK GDPR.
- The Processor maintains a documented personal data breach procedure providing for notification to the Controller within the period stated in clause 9.
- The data protection and security terms of any new Sub-processor or tool are assessed before it is adopted.

Data minimisation and retention

- Only Personal Data necessary to provide the Services is collected and retained.
- Personal Data is returned or deleted in accordance with clause 12.
- Where practicable, testing and development work uses anonymised or sample data rather than live Personal Data.

SCHEDULE 3 — AUTHORISED SUB-PROCESSORS

The Sub-processors authorised as at the Effective Date, and the transfer mechanism relied on where a Restricted Transfer takes place.

Sub-processor	Processing carried out	Location and transfer mechanism
HighLevel Inc.	Hosting and operation of the platform on which the Services run, including storage of contact records, message history, form submissions, call recordings and related content, and the transmission of email and SMS messages sent through the platform.	United States. Restricted Transfer made under the transfer terms of HighLevel's data processing agreement, incorporating the UK International Data Transfer Addendum to the EU Standard Contractual Clauses.