



**iTCHYROBOT**

**ITCHYROBOT**

**Data Processing Agreement – v1.0**

# Foreword

This document contains the Data Processing Agreement for ITCHYROBOT to undertake works in the position as a processor of data for customers (ie The Controller) in adherence to the 2021 UK General Data Protection Regulation.

Please note that the contents of this document are strictly confidential between the provider (ITCHYROBOT) and the Company and, as such, this document cannot be shared with any third-party without express permission.

Policy Version Control				
<b>Policy type</b>		Data Processing Agreement		
<b>Audience &amp; Distribution</b>		Private / Customer		
<b>Policy prepared by (name and designation)</b>		Tristen Coad		
<b>Document Owner</b>		ITCHYROBOT DPO		
<b>Date of approval</b>		26 <sup>th</sup> June 2024		
<b>Date released</b>		26 <sup>th</sup> June 2024		
Version	Changes	Author	Date of Issue	Date for Review
1.0	<ul style="list-style-type: none"><li>Document creation</li></ul>	T. Coad	26 <sup>th</sup> June 2024	26 <sup>th</sup> June 2025

# Data Processing Agreement — ITCHYROBOT

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services

("Principal Agreement") between

\_\_\_\_\_ (the  
"**Company**")

and

\_\_\_\_\_ (the "**Data  
Processor**")

(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the General Data Protection Regulation UK 2021 of the UK Parliament on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing EU GDPR 2018.

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

## 1. Definitions and Interpretation

1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1. "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2. "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3. "Contracted Processor" means a Subprocessor;

1.1.4. "Data Processing Particulars" means, in relation to any processing: (a) the subject matter, duration, nature and purpose of the processing; (b) the type of Personal Data being processed; and (c) the categories of data subjects;

1.1.5. "Data Protection Laws" means: (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the processing of Personal Data to which a Party is subject, including but not limited to the UK General Data Protection Regulation ("UK GDPR"), Data Protection Act 2018 ("DPA") and the EU GDPR; and (b) any code of practice or guidance published by a Regulatory Body from time to time;

- 1.1.6. "Data Subject Request" means an actual or purported request, notice or complaint from (or on behalf of) a data subject exercising his rights under the Data Protection Legislation;
- 1.1.7. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- 1.1.8. "Participant/Respondent" means any individual or organisation from or about whom data are collected;
- 1.1.9. "Permitted Purpose" means the purpose of the processing as set out in more detail;
- 1.1.10. "Personal Data" has the meaning set out in applicable Data Protection Legislation;
- 1.1.11. "Personnel" means all personnel involved in performing the Counterparty's obligations under this Agreement from time to time (including its employees, staff, temporary staff, other workers, agents, consultants and its sub-contractors);
- 1.1.12. "Regulatory Body" means any competent governmental, statutory, regulatory or enforcement authority or regulator concerned with the activities carried on by any Party or any part, division or element thereof, in respect of the activities carried out pursuant to this Agreement including but not limited to the UK Information Commissioner, and their relevant successors (for the avoidance of doubt, this does not include any regulator whose authority arises pursuant to any voluntary code of conduct);
- 1.1.13. "Regulatory Body Correspondence" means any correspondence or communication (whether written or verbal) from a Regulatory Body;
- 1.1.14. "Company Supplied Personal Data" means the Personal data supplied by the Company to be shared with the Data Processor under this Agreement
- 1.1.15. "Third Party Request" means a written request from any third party for disclosure of Company data where compliance with such request is required or purported to be required by law or regulation;
- 1.1.16. "Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- 1.1.17. "UK Data Protection Laws" includes, but not limited to, the UK GDPR and Data Protection Act 2018;
- 1.1.18. "GDPR" means UK General Data Protection Regulation 2021;
- 1.1.19. "Data Transfer" means:
- 1.1.19.1. a transfer of Company Personal Data from the Company to a Contracted Processor; or
- 1.1.19.2. an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);
- 1.1.20. "Services" means the business services the Company provides with include, but is not exclusive to:

- 1.1.20.1. Website design
- 1.1.20.2. Website hosting
- 1.1.20.3. Website management

1.1.21. "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2. The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## 2. Data Protection

2.1. For the purposes of this Agreement, "**controller**", "**processor**", "**data subject**", "**Personal Data**" and "**process**" shall have the meanings set out in the UK GDPR and "**process**" and "**processed**" when used in relation to the processing of Company's Data, will be construed accordingly, and will include both manual and automatic processing. Any reference to "**Personal Data**" includes a reference to "special categories of personal data", as applicable, whereby "special categories of personal data " means Company's Data that incorporates such categories of data as are listed in Article 9(1) of the UK GDPR.

2.2. The Parties shall each process Personal Data under this Agreement. The Parties acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Legislation. For the avoidance of doubt, the parties are not joint controllers for the purposes of Article 26 of the UK GDPR.

2.3. The Parties acknowledge that in the event of any conflict between the provisions of this Agreement and other agreements governing the processing of personal data, the provisions herein shall prevail.

2.4. Where a Company is acting as a Controller in relation to this Agreement, it shall comply with its obligations under the Data Protection Legislation and that Company shall ensure that it records due notification to any relevant Regulator, such notice to include its use and processing of the Personal Data.

2.5. Where the Processor is operating on behalf of the Company in relation to this Agreement it shall:

2.5.1. comply with its obligations under the Data Protection Legislation;

2.5.2. process the Personal Data strictly in accordance with the Company's instructions for the processing of the Company Supplied Personal Data and only for the purposes of providing the Services or as otherwise instructed in writing by the Company;

2.5.3. notify the Company if it believes that any instruction issued by the Company is not compliant with applicable Data Protection Legislation;

2.5.4. keep and maintain a record of processing as required under Article 30 (2) of the UK GDPR;

2.5.5. ensure that access to the Personal Data is limited to only those employees who require access to it for the purpose of providing the Services and that all such employees have undergone training in the law of data protection, their duty of confidentiality and in the care and handling of Personal Data;

- 2.5.6. assist the Company promptly with all subject information requests which may be received from Data Subjects relating to the Company Supplied Personal Data, as set out in Clause 2.12 and Clause 6;
  - 2.5.7. employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure, as set out in Clause 4;
  - 2.5.8. not disclose the Personal Data to a third party in any circumstances other than at the specific written request of the Company, unless the disclosure is required by law;
  - 2.5.9. notify the Company of any information security incident that may impact the processing of the Personal Data within 24 (twenty-four) hours of discovering or becoming aware of any such incident as set out in Clause 5; or
  - 2.5.10. not keep the Personal Data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the Services.
- 2.6. Where a Party collects Personal Data which it subsequently transfers to the other Party, it shall:
- 2.6.1. ensure that it is not subject to any prohibition or restriction which would:
    - 2.6.1.1. prevent or restrict it from disclosing or transferring the Personal Data to the other Party, as required under this Agreement; or
    - 2.6.1.2. prevent or restrict the other Party from processing the Personal Data as envisaged under this Agreement;
  - 2.6.2. ensure that all fair processing notices have been given (and/or, as applicable, valid consents obtained that have not been withdrawn) and are sufficient in scope and kept up-to-date in order to meet the Transparency Requirements to enable each Party to process the Personal Data in order to obtain the benefit of its rights, and to fulfil its obligations, under this Agreement in accordance with the Data Protection Legislation. For the avoidance of doubt, the Parties do not warrant to each other that any use of transferred Personal Data outside the scope of this Agreement shall be compliant with the Data Protection Legislation;
  - 2.6.3. ensure that the Personal Data is:
    - 2.6.3.1. adequate, relevant and limited to what is necessary in relation to the Permitted Purpose; and
    - 2.6.3.2. accurate and, where necessary, up to date; having taking every reasonable step to ensure that any inaccurate Personal Data, (having regard to the Permitted Purpose), has been erased or rectified.
  - 2.6.4. ensure that the Personal Data is transferred between the Parties by a secure means.
- 2.7. Each Party shall not, by its acts or omissions, cause the other Party to breach its respective obligations under the Data Protection Legislation, namely when one of the Parties has the duty to preserve the anonymity of the respondents.
- 2.8. Each Party shall indemnify and keep the other fully indemnified from and against any and all losses, fines, liabilities, damages, costs, claims, amounts paid in settlement and expenses (including legal fees, disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties) that are sustained or suffered or incurred by, awarded against or agreed to be paid by, the other Party as a result of, or arising from, a breach by each Party of its obligations and/or the Data Protection Legislation, including, in particular, pursuant to:

- 2.8.1. any monetary penalties or fines levied by any Regulatory Body on the other Party;
  - 2.8.2. the costs of any investigative, corrective or compensatory action required by any Regulatory Body, or of defending proposed or actual enforcement taken by any Regulatory Body;
  - 2.8.3. any losses suffered or incurred by, awarded against, or agreed to be paid by the other Party, pursuant to a claim, action or challenge made by a third party against the other Party, (including by a data subject); and
- 2.9. Where relevant, each Party shall notify the other promptly (and in any event within thirty-six (36) hours) following its receipt of any Data Subject Request or Regulatory Body Correspondence, which relates directly or indirectly to the processing of Personal Data under this Agreement or to either Party's compliance with the Data Protection Legislation, and together with such notices, or Regulatory Body Correspondence and reasonable details of circumstances giving rise to it. In addition, each Party shall:
  - 2.9.1. only disclose such Personal Data in response to any Data Subject Request or Regulatory Body Correspondence where it has obtained the other party's prior written consent; and
  - 2.9.2. provide the other Party with all reasonable co-operation and assistance required in relation to any such Data Subject Request or Regulatory Body Correspondence.
3. Processing of Company Personal Data
  - 3.1. Processor shall:
    - 3.1.1. comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
    - 3.1.2. not Process Company Personal Data other than on the relevant Company's documented instructions.
  - 3.2. The Company instructs Processor to process Company Personal Data.
4. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.
5. Security
  - 5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR. Such measures will include, but shall not be limited to:
    - 5.1.1.1. the pseudonymisation and encryption of Personal Data, where appropriate;
    - 5.1.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of relevant Processing systems and services;

- 5.1.1.3. the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident, including a Personal Data Breach;
      - 5.1.1.4. a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures in order to ensure the security of the Processing of Personal Data.
    - 5.2. Processor shall maintain and adhere to UK GDPR and UK Law in ensuring the Confidentiality, Integrity and Availability of Company Personal Data.
    - 5.3. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
    - 5.4. The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to personal data does not process them except on instructions from the Controller, unless required to do so by UK law.
  6. Subprocessing
    - 6.1. Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company to undertake and/or complete the required works as directed by the Company.
    - 6.2. Any sub-processing shall be strictly in accordance with the terms of this Agreement. Where the sub-processor fails to fulfil its data protection obligations, the Processor will remain liable to the Company for the performance of such sub-Processor's obligations.
  7. Data Subject Rights
    - 7.1. Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
    - 7.2. Processor shall:
      - 7.2.1. promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
      - 7.2.2. ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.
      - 7.2.3. The parties shall notify each other as soon as reasonably practicable after becoming aware if they:
        - 7.2.3.1. receive a request to rectify, block or erase any Personal Data;
        - 7.2.3.2. receive any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation; or
        - 7.2.3.3. becomes aware of a Data Loss Event.
  8. Personal Data Breach
    - 8.1. Processor shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Article



33 of the UK GDPR and, where applicable, shall each inform the Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data.

8.2. When a Party is acting as a Processor, it shall notify the Company immediately if it becomes aware of, or reasonably suspects the occurrence of, any potential or actual Personal Data Breach affecting Company Supplied Personal Data and, in any event, within twenty-four (24) hours to enable the Company to determine whether it must notify the Regulatory body in its own capacity as Controller.

8.3. The Processor shall provide the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

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

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

10. Deletion or return of Company Personal Data

10.1. Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

11. Audit rights

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

11.2. Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

12. Data Transfer

12.1. The Processor may not transfer or authorize the transfer of Data to countries outside the UK without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the UK to a country outside the UK, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on UK approved standard contractual clauses for the transfer of personal data.

13. General Terms

13.1. Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

- (a) disclosure is required by law;
- (b) the relevant information is already in the public domain.

13.2. Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

#### 14. Governing Law and Jurisdiction

14.1. This Agreement is governed by UK Law.

14.2. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the UK courts, subject to possible appeal.

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

**Controller Company**

Signature \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date Signed: \_\_\_\_\_

**Processor Company**

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date Signed \_\_\_\_\_

Content and specification within this document is subject to change without notice please contact ITCHYROBOT for clarification on any aspect as required.