

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

(the "**Company**")

and

Can I Phish Pty Ltd
PO Box 21, Eumundi,
QLD 4562,
Australia

(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 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
- (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 Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
 - 1.1.5 "**EEA**" means the European Economic Area;
 - 1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
 - 1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;
 - 1.1.8 "**Data Transfer**" means:
 - 1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or
 - 1.1.8.2 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);
 - 1.1.9 "**Services**" mean the Phishing Simulation & Security Awareness Training services the Data Processor provides.
 - 1.1.10 "**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. Processing of Company Personal Data

- 2.1 Processor shall:
 - 2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
 - 2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. 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.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 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 GDPR.

4.2 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. Subprocessing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

5.2 Processor shall provide prior written notice to the Company of the proposed appointment of any new subprocessor after the date of initial agreement. At Companies request Processor shall provide the Company with the identity, location as well as description of the processing activities to be subcontracted or outsourced. Where Processor wishes to appoint a Subprocessor under this DPA, it will verify prior to engaging the Subprocessor, that the Subprocessor is capable of complying with the obligations of the Processor towards the Company, to the extent applicable to the Services assigned to that Subprocessor.

5.3 If within 14 calendar days following receipt of that notice, the Company notifies Processor in writing of any objections, the Parties will endeavour to agree in good faith, the steps to be taken to ensure that such objections are addressed prior to the appointment of the new subprocessor.

5.4 Processor shall be responsible for the work and activities of all Subprocessors as outlined in Appendix A – Can I Phish Pty Ltd Subprocessors.

6. Data Subject Rights

6.1 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.

6.2 Processor shall:

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

6.2.2 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. Personal Data Breach

- 7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 7.2 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.

8. 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 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.

9. Deletion or return of Company Personal Data

- 9.1 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.
- 9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

- 10.1 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.
- 10.2 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.

11. Data Transfer

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

12. General Terms

12.1 **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.

12.2 **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.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of Australia.

13.2 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 courts of Australia.

Appendix A – Can I Phish Pty Ltd Subprocessors

Subprocessor	Nature and Purpose of Processing	Categories of personal data	Storage Location
Amazon Web Services (AWS)	Processor utilize AWS for cloud computing and infrastructure hosting services.	Company employee information including email addresses, first names, last names, job titles, and company names.	Configurable by Company for storage in any of the following locations: Australia, United States of America, United Kingdom, Canada, South Africa, Germany, United Arab Emirates, Brazil and Singapore.
Microsoft	<p>Microsoft 365 Processor utilize Microsoft 365 for customer communication and collaboration.</p> <p>Microsoft Azure Processor utilize Microsoft Azure for its Artificial Intelligence (AI) services, notably Azure OpenAI which powers Processor’s Conversational Phishing functionality.</p>	<p>Microsoft 365 Company information communicated with Processor through email or video conference.</p> <p>Microsoft Azure Company employee information including email addresses, first names, last names, job titles, and company names. If callback phishing is utilized, Azure additionally processes audio data streams during the call.</p>	<p>Microsoft 365 Australia</p> <p>Microsoft Azure Configurable by Company for ephemeral storage in any of the following locations: Australia, United States of America, United Kingdom, Canada, South Africa, Germany, Brazil, Sweden and Japan.</p>
Zendesk	Processor utilize Zendesk for knowledgebase and live chat services.	Company information communicated through live chat.	Australia
Klaviyo	Processor utilize Klaviyo for email marketing automation.	Company user account information including the email address, first name, and last name of the employee who initially created an account with the Processor.	United States
Telnyx	Processor utilize Telnyx for Voice over Internet Protocol (VoIP) calls as part of simulated callback phishing functionality.	Caller phone numbers, call metadata, audio data streams during an active call.	Points of Presence in the USA, Ireland, Netherlands, Australia, Singapore, Canada, and the UK, chosen based on caller location for optimal call latency.
Have I Been Pwned	Processor utilize Have I Been Pwned for dark web monitoring services. No data is shared with Have I Been Pwned, unless Company explicitly opt-in to use the dark web monitoring service.	Company employee email addresses.	Australia

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

Your Company

Signature _____

Name: _____

Title: _____

Date Signed: _____

Processor Company

Can I Phish Pty Ltd (ABN: 24 647 802 266)

Signature  _____

Name: Sebastian Salla

Title: CEO

Date Signed: November 15th, 2024