caniphish

Can I Phish Pty Ltd
PO Box 186, Peregian Beach
QLD 4573, Australia

This Data Processing Agreement ("**Agreement**") is supplementary to, and forms part of, the terms & conditions available at https://caniphish.com/terms-conditions, between,

(company name, address)

_____

_____

_____

(the "**Company**")

and

Can I Phish Pty Ltd
PO Box 186, Peregian Beach,
QLD 4573,
Australia

(the "**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). The Parties further intend this Agreement to address, where applicable to the processing, the UK GDPR and the Swiss FADP.
(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 the Processor and/or a Subprocessor;

1.1.4 **"Controller"** means the Company as defined above.

1.1.5 **"Data Protection Laws"** means EU Data Protection Laws, the UK GDPR and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.6 "**EEA**" means the European Economic Area;

1.1.7 "**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means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.8 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.9 "**Data Transfer**" means:

1.1.9.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.9.2 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);

1.1.10 "**Services**" mean the Phishing Simulation & Security Awareness Training services the Data Processor provides.

1.1.11 **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of personal data to third countries as adopted by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("SCCs"), Module 2 (controller to processor).

1.1.12 "**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.

1.1.13 **"Aggregated and Anonymized Data"** means data derived by the Processor from the Processing that has been irreversibly rendered such that it no longer relates to an identified or identifiable natural person and from which no individual can be re-identified by any means reasonably likely to be used, by the Processor or any other person.

1.1.14 **"Security Threat Indicator"** means information relating to automated, non-human, fraudulent, abusive, or malicious activity or infrastructure — including the network address (IP address or

autonomous system number), reverse-DNS, or behavioral characteristics of automated systems, security scanners, sandboxes, bots, crawlers, or proxying infrastructure — that does not relate to, identify, or reasonably permit the identification of any natural person.

1.1.15 **"Service Security and Integrity Purposes"** means: (a) detecting, preventing, investigating, and mitigating fraud, abuse, spam, automated or non-human activity, and security threats; (b) ensuring and protecting the security, availability, accuracy, and integrity of the Service, including the accuracy of simulation results and reporting by distinguishing genuine human interactions from automated or non-human interactions; and (c) generating, maintaining, and using Aggregated and Anonymized Data and Security Threat Indicators for the foregoing.

1.1.16 **"Swiss FADP"** means the Swiss Federal Act on Data Protection of 25 September 2020 (as revised, in force from 1 September 2023);

1.1.17 **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022) issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018, as revised under Section 18 of its Mandatory Clauses;

1.1.18 **"UK GDPR"** means Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended), together with the Data Protection Act 2018;

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.

1.3 In respect of processing of Company Personal Data that is subject to the UK GDPR, references in this Agreement to the GDPR, or to Chapters or Articles of the GDPR, shall be construed as references to the UK GDPR and its corresponding provisions.

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.

2.3 The Company instructs and authorizes the Processor to Process Company Personal Data to the extent strictly necessary and proportionate for the Service Security and Integrity Purposes. Such Processing forms part of the provision of the Service and constitutes the Company's documented instructions for the purposes of §2.1.2 and, where applicable, further instructions of the data exporter for the purposes of Clause 8.2 of the Standard Contractual Clauses.

2.4 The Processor may create Aggregated and Anonymized Data and Security Threat Indicators from the Processing and may retain and use them for the Service Security and Integrity Purposes and to operate, secure, and improve the Service, including across the Processor's customer base. Aggregated and Anonymized Data and Security Threat Indicators do not constitute Company Personal Data.

2.5 The Processor shall not disclose Company Personal Data, or any data that identifies or could reasonably be used to identify any natural person or the Company, to any other customer of the Processor. Only Security Threat Indicators may be shared with or consulted across the Processor's customers, and only for the Service Security and Integrity Purposes.

2.6 Nothing in §§2.3–2.5 diminishes the Data Subject rights in Section 6, the security obligations in Section 4, or the Processor's obligation to Process Company Personal Data (as distinct from Aggregated and Anonymized Data and Security Threat Indicators) only in accordance with this Agreement.

2.7 The Company may [enable / disable] the contribution of Company Personal Data toward cross-customer Security Threat Indicators via the Service settings. Where contribution is [not enabled / disabled], the Processor shall not use Company Personal Data to generate Security Threat Indicators shared with other customers, but may continue to Process Company Personal Data for the Service Security and Integrity Purposes for the Company's own benefit. Security Threat Indicators and Aggregated and Anonymized Data already created remain unaffected.

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 endeavor 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 Annex III – Approved 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.

9.3 Clauses 9.1 and 9.2 do not apply to Aggregated and Anonymized Data or Security Threat Indicators, which do not constitute Company Personal Data and which the Processor may retain after the Cessation Date, provided they remain irreversibly anonymized. The same applies to the erasure obligation in Clause 8.5 of the Standard Contractual Clauses.

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. International Transfers

11.1 The Processor shall not transfer any Company Personal Data outside the EEA, the United Kingdom or Switzerland unless in compliance with Chapter V of the GDPR, Chapter V of the UK GDPR or the Swiss FADP (in each case, as applicable to the transfer).

11.2 To the extent that any such transfer is subject to Chapter V of the GDPR, the parties shall rely on Module 2 (controller to processor) of the SCCs. The Module 2 Clauses are incorporated by reference and form Annex B to this Agreement.

11.3 To the extent that any such transfer is a restricted transfer subject to the UK GDPR, the parties shall rely on the SCCs as amended by the UK Addendum. The UK Addendum is incorporated by reference and is entered into and completed as set out in Annex C to this Agreement.

11.4 To the extent that any such transfer is subject to the Swiss FADP, the parties shall rely on the SCCs as adapted by Annex D to this Agreement.

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 Controllers established outside the EEA, the United Kingdom and Switzerland: This Agreement (excluding the Standard Contractual Clauses in Annex B, as amended or adapted by Annex C or Annex D) shall be governed by the laws of Queensland, Australia. Any dispute arising in connection with this Agreement that the Parties are unable to resolve amicably will be submitted to the exclusive jurisdiction of the courts of Queensland, Australia.

13.2 EEA Controllers: To the extent that the processing of Controller Personal Data by the Processor is governed by the Standard Contractual Clauses in Annex B (Module 2: Controller to Processor), Clauses 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) of those SCCs shall apply.

13.3 UK Controllers: To the extent that the processing of Controller Personal Data by the Processor is governed by the SCCs as amended by the UK Addendum (Annex C), the SCCs as so amended shall, in accordance with the Mandatory Clauses of the UK Addendum, be governed by the laws of England and Wales, and any dispute arising from them shall be resolved by the courts of England and Wales.

13.4 Swiss Controllers: To the extent that the processing of Controller Personal Data by the Processor is governed by the SCCs as adapted by Annex D, Clauses 17 and 18 of those SCCs (as completed in Annex B) shall apply, subject to the adaptations set out in Annex D.

Annex I – Transfer Details

Note: This Annex applies only to data transfers subject to the Standard Contractual Clauses in Annex B, including as amended by the UK Addendum (Annex C) or as adapted for Switzerland (Annex D). Controllers whose transfers are not subject to those instruments may disregard or mark all fields "Not applicable."

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:	
Role (controller/processor):	

Data importer(s):

Name:	Can I Phish Pty Ltd
Address:	PO Box 186, Peregian Beach, QLD 4573, Australia
Contact person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	Provision of the Services under the Agreement.
Signature and date:	
Role (controller/processor):	Processor

B. Description of Transfer

1. **Data Subjects:** Natural persons whose data is processed by the Controller in using the Service, including employees, contractors and end users.
2. **Categories of Personal Data:** The categories of personal data are determined and controlled by the Controller in its sole discretion, but may include first names, last names, email addresses, employment data, and device metadata.
3. **Purpose(s) of Processing:** Provision of the Service pursuant to the Agreement and Processing strictly necessary for the Service Security and Integrity Purposes, including detecting and mitigating automated, fraudulent, or abusive activity and maintaining the security, accuracy, and integrity of the Service.
4. **Frequency of Transfer:** Ongoing, in real-time or near real-time as required to deliver the Service.
5. **Duration of Processing:** Processing of personal data shall take place for the duration of the Controller's subscription to the Service. After termination, the Processor shall, at the Controller's request, delete or return all personal data processed on its behalf and certify to the Controller that it has done so. Data subjects may request access, rectification or deletion of their personal data at any time in accordance with the Processor's Privacy Policy and applicable Data Protection Laws; if a deletion request cannot be fulfilled due to legal, regulatory or contractual obligations, the Processor will inform the Controller of the reasons.

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13 of Annex B – Standard Contractual Clauses:
Where the data exporter is established in an EU Member State, this will be the supervisory authority of that Member State. Where the UK Addendum (Annex C) applies, the competent supervisory authority is the Information Commissioner. Where Annex D applies, the competent authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC) insofar as the transfer is subject to the Swiss FADP.

Annex II – Technical And Organizational Security Measures

Technical and organizational measures to ensure the security of personal data include:

1. **Data Security**

- Data Classification & Handling Policy to categorize and manage data by sensitivity.
- Role-based Access Control (with MFA for administrative access) and strict "least-privilege" restrictions.
- Daily database backups, restricted access, and AES-256 encryption at-rest.

2. **Network Security**

- Web Application Firewall and managed DDoS protection at the perimeter.
- All direct server access (SSH/RDP) disabled; network logging and continuous monitoring.
- TLS 1.2+ encryption for all data in-transit.

3. **Application Security**

- Secure Development Lifecycle with formal Change Management practices.
- Annual penetration tests, daily vulnerability scans, and a Responsible Disclosure program.

4. **Infrastructure Security**

- Hardened, auto-scaled infrastructure across multiple data centers with automated security patching.
- MFA on all administrator consoles and load-balanced deployment for resilience.

5. **Product Security**

- Continuous Cloud Anomaly Detection, Configuration Security, Identity Security, and Workload Protection.
- 24/7 System Availability Monitoring and responsive incident handling.

6. **Organizational Security**

- Monthly internal phishing simulations and annual Security Awareness training for staff.
- Endpoint hardening (MDM, anti-malware) and formal Incident Response & Business Continuity plans.

The listed security measures are externally audited through an annual SOC 2 Type 2 assessment. The Processors SOC 2 Type 2 and SOC 3 Reports are available on request (https://caniphish.com/security).

caniphish

Annex III – Approved 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, company names, residing countries, phone numbers, and preferred languages.	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	**Microsoft 365** Processor utilize Microsoft 365 for customer communication and collaboration. **Microsoft Azure** Processor utilize Microsoft Azure for its Artificial Intelligence (AI) services, notably Azure OpenAI which powers Processor's Business Impact Rule Generation; Conversational Email Phishing; AI Threat Analysis; AI Content Generator (training content, simulated phishing emails, simulated phishing websites); AI Program Manager; AI Chat Widget.	**Microsoft 365** Company information communicated with Processor through email or video conference. **Microsoft Azure** Company employee information including email addresses, first names, last names, job titles, company names, residing countries, phone numbers, and preferred languages. Tenant metadata such as enabled features, and recent activity. If callback phishing is utilized, Azure additionally processes audio data streams during the call.	**Microsoft 365** Australia **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.
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
Monday	Processor utilize Monday to support sales processes.	Company information including the email address, first name, last name, and email communication of the employee who engages CanIPhish for sales support.	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
ElevenLabs	Processor utilize ElevenLabs for its Conversational AI services which powers Processor's outbound simulated voice phishing functionality. Additionally, Processor utilize ElevenLabs for its Text-to-Speech services which powers the audio generation component of Processor's AI Video Generator functionality.	Call metadata, audio data streams, call transcripts, and employee information, including email addresses, first names, last names, job titles, company names, residing countries, phone numbers, and preferred languages, during an active call. Video script transcripts provided as part of the AI Video Generation process.	United States
Fal AI	rocessor utilize Fal AI for its API-based serverless infrastructure services which facilitates Processor's AI Video Generator functionality. Fal AI orchestrates the submission and processing of video generation requests. No personal employee information is shared with Fal AI.	Video script transcripts provided as part of the AI Video Generation process.	United States
Veed	Processor utilize Veed for its AI video generation model which provides the underlying technology used to generate AI training videos as part of Processor's AI Video Generator functionality. No personal employee information is shared with Veed.	Video script transcripts provided as part of the AI Video Generation process.	United States
Twilio	Processor utilize Twilio for its phone number verification services which enables Processor’s ability to ensure all participants of outbound simulated voice phishing exercises have explicitly consented via double opt-in. No data is shared with Twilio unless Company explicitly opt-in to use the outbound voice phishing functionality.	Company employee phone numbers.	United States

caniphish

Annex B – Standard Contractual Clauses

(Module 2: 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) ([i]) for the transfer of 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) Annex I, Annex II, and Annex III referred to therein form 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 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 the 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 ([ii]) (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) GENERAL WRITTEN AUTHORISATION 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 14 calendar 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. ([iii]) 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) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 ([iv]);

(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(e).

(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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

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 of the Netherlands.

(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 C – UK International Data Transfer Addendum

This Annex C applies where a Data Transfer is a restricted transfer subject to the UK GDPR. For such transfers, the Parties enter into the UK Addendum (International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force 21 March 2022), which amends and is appended to the SCCs set out in Annex B, and which is completed as set out in this Annex C.

Part 1: Tables

Table 1: Parties	
Start date	The date of this Agreement.
The Parties	Exporter (who sends the Restricted Transfer): the Company, being the data exporter whose details are set out in Annex I.A. Importer (who receives the Restricted Transfer): Can I Phish Pty Ltd, being the data importer whose details are set out in Annex I.A.
Key Contact	As set out in Annex I.A for each Party.

Table 2: Selected SCCs, Modules and Selected Clauses	
Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to is the SCCs set out in Annex B to this Agreement (Commission Implementing Decision (EU) 2021/914), Module 2 (Controller to Processor), including the Appendix Information, and with: (a) Clause 7 (Docking Clause) not incorporated; (b) Clause 9(a) (General Written Authorisation) with a minimum notice period of 14 calendar days; and (c) Clauses 17 and 18 as completed in Annex B.

Table 3: Appendix Information	
Annex 1A: List of Parties	As set out in Annex I.A of this Agreement.
Annex 1B: Description of Transfer	As set out in Annex I.B of this Agreement.
Annex II: Technical and organisational measures	As set out in Annex II of this Agreement.
Annex III: List of Sub processors	As set out in Annex III of this Agreement.

Table 4: Ending this Addendum when the Approved Addendum Changes	
Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19 of the Mandatory Clauses: the Importer.

Part 2: Mandatory Clauses

The Parties agree to be bound by the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

For information, the Mandatory Clauses amend the SCCs for transfers subject to the UK GDPR so that (among other amendments): references to Regulation (EU) 2016/679 are read as references to the UK GDPR, and references to specific Articles of that Regulation are read as the equivalent provisions of the UK GDPR; references to EU or Member State law are read as references to the laws of the United Kingdom; the Information Commissioner acts as competent supervisory authority; and Clauses 17 and 18 of the SCCs are read such that the SCCs, as amended, are governed by the laws of England and Wales and disputes arising from them are resolved before the courts of England and Wales.

Annex D – Swiss FADP Adaptations to the SCCs

This Annex D applies where a Data Transfer is subject to the Swiss FADP. For such transfers, the SCCs set out in Annex B apply with the following adaptations:

1. The Swiss Federal Data Protection and Information Commissioner (FDPIC) is the competent supervisory authority under Clause 13 of the SCCs insofar as the transfer is subject to the Swiss FADP.

2. References in the SCCs to the GDPR or to Regulation (EU) 2016/679 are, insofar as the transfer is subject to the Swiss FADP, to be read as references to the Swiss FADP.

3. References to the "EU", the "Union" and "Member State" are not to be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the SCCs.

4. In all other respects, the SCCs as completed in Annex B (including Clauses 17 and 18) remain unchanged.

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

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

Signature _____

Name: _____

Title: _____

Date Signed: _____

[i] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[ii] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[iii] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[iv] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.