

PROCUREMENT PACK

Everything your vendor review needs, in one file.

Security overview, data processing agreement, sub-processors, master service agreement, security and retention policies, and pre-answered GDPR questions.

VENDOR

**Headshot Pro Photography Pte.
Ltd.**

GENERATED

October 13, 2026

CONTACT

sales@headshotpro.com

What's inside

01	Security Overview	IT & security
A one-page summary of HeadshotPro's security, privacy, and compliance posture for IT and security teams reviewing the platform.		
02	Data Processing Agreement	Legal & privacy
This Data Processing Agreement outlines how HeadshotPro processes personal data on behalf of its customers.		
03	Sub-Processors	Privacy
The third-party sub-processors HeadshotPro uses to deliver its services.		
04	Master Service Agreement	Legal
The Master Service Agreement governs the terms under which HeadshotPro provides its services.		
05	Security Policy	IT & security
HeadshotPro's security policy outlines the organizational and technical safeguards implemented to protect customer data.		
06	Data Management and Retention Policy	IT & privacy
How HeadshotPro manages, stores, and retains customer data.		
07	GDPR Questionnaire Responses	Privacy
Pre-answered responses to the GDPR and Article 28 data-processor questions most commonly asked during an enterprise vendor review.		

SOC 2 Type II Report available through our Trust Center: trust.headshotpro.com	GDPR data processor Your organization stays the data controller
No AI training Photos are never used to train AI models	SSO SAML 2.0 and OAuth, with domain enforcement

Security Overview

A one-page summary of HeadshotPro's security, privacy, and compliance posture for IT and security teams reviewing the platform.

Last updated: June 24, 2026

This overview summarizes how HeadshotPro protects your team's data. It's written for IT, security, and procurement teams running a vendor review. For the underlying documents, see [Documentation for your security review](#) at the end.

At a glance

Area	Summary
Certification	SOC 2 Type II (Security); report available on request
Compliance	GDPR, UK GDPR, CCPA, Singapore PDPA
AI training	Your photos are never used to train AI models, no exceptions
Data at rest	Stored in the EU (Cloudflare, Western Europe); encrypted US failover for backup
Encryption	TLS 1.2+ in transit, AES-256 at rest
Photo retention	Input photos auto-deleted 30 days after generation
Account deletion	Personal data erased within 14 days of request
Identity	SAML 2.0 / OAuth SSO, JIT provisioning, admin MFA
Availability	99.9% uptime target; RTO 2h / RPO 1h
Incident response	Breach notification within 48–72 hours

Certifications and compliance

- **SOC 2 Type II** for the Security Trust Services Criteria, examined by an independent auditor. The full report can be [requested via our Trust Center](#).
- Compliant with **GDPR, UK GDPR, CCPA, and Singapore PDPA**. HeadshotPro acts as the data processor; your organization remains the data controller.
- A **Data Processing Agreement** is publicly available and applies automatically to all customers. [International transfers](#) are covered by the EU Standard Contractual Clauses (Module Two) and the UK IDTA.
- **Independent penetration testing** is conducted regularly, alongside continuous automated security scanning on a 24-hour cycle (dependency vulnerabilities, file integrity, and suspicious-request patterns).

Your photos are never used to train AI

Uploaded photos and generated headshots are never used to train, fine-tune, or otherwise improve any AI model, ours or any third party's. This is an absolute commitment with no exceptions. Customer content is processed only to generate your headshots and to operate, secure, and support the service.

Data storage and residency

- **Primary storage** for uploaded photos and generated headshots is in the **European Economic Area** (Western Europe).
- **Failover storage** is replicated in encrypted form to the **United States** (GCS, us-east-1) for backup and disaster recovery only.
- **Application servers** run in the United States (US-West).
- Production databases are managed (MongoDB Atlas), with network access restricted to an IP allowlist and protected by authentication and TLS, and sit behind deny-by-default firewall rules. Direct unauthenticated access is not permitted.
- Customer-selectable or contractually pinned data residency is not currently offered.

International data transfers

Where personal data is transferred out of the EEA, the UK, or Switzerland to a country without an adequacy decision, the transfer is covered by an approved safeguard under Article 46 GDPR. These mechanisms are incorporated into our [Data Processing Agreement](#) (Section 6) and apply automatically to every customer — there is nothing to sign separately.

- **EU / EEA:** The EU **Standard Contractual Clauses, Module Two (Controller to Processor)** from Commission Implementing Decision (EU) 2021/914 are incorporated by reference. The SCC Annexes (parties, description of transfer, technical and organisational measures, sub-processors) are completed by the corresponding Annexes of the DPA. Clause 17 Option 1 applies, governed by the laws of **Ireland**; the competent supervisory authority is the **Data Protection Commission of Ireland**.
- **United Kingdom:** The **International Data Transfer Addendum (Version B1.0)** to the EU SCCs, issued by the UK Information Commissioner, applies — with its tables completed by reference to the EU SCCs and the DPA Annexes.
- **Switzerland:** The EU SCCs apply with the modifications required under the Swiss Federal Act on Data Protection (FADP), including reference to the Swiss FDPIC and protection for data of legal entities.
- **Data importer:** Headshot Pro Photography Pte. Ltd. (Singapore). Our EU representative under Article 27 GDPR is iuro Rechtsanwälte GmbH t/a Prighter (Vienna, Austria).

Encryption

- **In transit:** TLS 1.2 or higher (256-bit). HTTPS only, with no unencrypted channels.
- **At rest:** AES-256 across account data, uploaded photos, and generated headshots.
- Encryption keys are managed at the infrastructure-provider layer; staff cannot access raw encryption keys.

Retention and deletion

- **Input photos** are automatically deleted **30 days** after your headshots are generated. Earlier deletion is available on request.
- **Account deletion** triggers full erasure of personal data within **14 days** of confirmation.
- **Backups** are taken hourly with point-in-time recovery, retained for up to one year, then securely deleted.
- Generated headshots are exportable at any time, including within 30 days of account termination.

For full details, see the [Data Management & Retention](#) policy.

Identity and access

- **Single Sign-On (enterprise)**: SAML 2.0 and OAuth via major identity providers (Okta, Microsoft Entra ID, Google Workspace), with enforced SSO and just-in-time provisioning.
- **Multi-factor authentication**: email-based MFA for organization administrators, enforceable across the whole organization. Admins re-verify with a one-time code every 24 hours.
- **Authentication**: every API request is authenticated and scoped to the signed-in user, so users access only their own records.
- **Least-privilege access**: production access is role-based, requires approval, is logged with MFA enforced, and is reviewed at least annually. Developers work against staging data, not production customer data.
- **Rate limiting** is enforced per IP and per account to protect against brute-force and abuse.

Infrastructure and monitoring

- HeadshotPro runs entirely on managed cloud infrastructure (Render, Cloudflare, Google Cloud, Vercel) and operates no facilities of its own. Physical and environmental controls are inherited from these providers' certified data centers.
- Customer data is logically isolated per account on multi-tenant infrastructure.
- Application health and errors are monitored continuously via Sentry. Production console access and security-relevant events are logged and reviewed for anomalous activity.
- Changes follow secure-SDLC practices, including code review and dependency scanning.

Availability and disaster recovery

- **Uptime target**: 99.9% monthly, with service credits available if missed.
- **Recovery objectives**: RTO of 2 hours and RPO of 1 hour, supported by hourly backups with point-in-time recovery.
- **Regional separation**: primary storage (EU) and failover storage (US) are in separate regions.
- Restoration tests are performed at least quarterly.

Incident response

HeadshotPro maintains a documented incident-response and breach-notification process. We notify affected customers without undue delay, and in any event within **48 hours** of confirming a personal-data breach and within **72 hours** for other security incidents affecting customer personal data. Notice includes

the nature of the incident, the categories of data affected, and the remediation taken or proposed, with cooperation and updates as the investigation progresses.

Sub-processors

HeadshotPro publishes and maintains a current list of all sub-processors with access to customer content, including the function each performs and its country. See the [Sub-processors](#) page for the live list and our process for notifying customers of changes.

Documentation for your security review

Document	How to access
Security Policy	Read online
Master Service Agreement	Read online
Data Processing Agreement	Read online
International data transfer terms (EU SCCs Module Two + UK IDTA)	Read online
GDPR questionnaire responses	Read online
Sub-processor list	Read online
Trust Center (live status, audited by Oneleet)	trust.headshotpro.com
SOC 2 Type II report	Request via Trust Center
Penetration-test summary	Request via Trust Center
Disaster-recovery test summary	Request via Trust Center

Running a security review or have a questionnaire to complete? Email support@headshotpro.com and we'll turn it around quickly.

Data Processing Agreement

This Data Processing Agreement outlines how HeadshotPro processes personal data on behalf of its customers.

DATA PROCESSING AGREEMENT

Last Updated: February 27, 2026

This Data Processing Agreement ("DPA") is between Headshot Pro Photography Pte. Ltd., 7 TEMASEK BOULEVARD, #12-07, SUNTEC TOWER ONE, SINGAPORE 038987 ("HeadshotPro," "Processor," "we," "us," or "our") and the customer who has entered into a Master Service Agreement, Order Form, or Terms of Service with HeadshotPro ("Customer," "Controller," or "you").

This DPA forms part of and is incorporated by reference into the agreement between the Parties governing Customer's use of the Service (the "MSA"). It applies to the extent that HeadshotPro processes Personal Data on behalf of Customer in the course of providing the Service.

Acceptance. By executing an MSA or Order Form that references this DPA, or by using the Service after this DPA has been published, Customer agrees to be bound by the terms of this DPA. Customers who wish to enter into a separately executed copy of this DPA may contact legal@headshotpro.com.

1. Definitions

Capitalised terms not defined herein have the meanings given in the MSA. In this DPA:

"Applicable Data Protection Law" means all laws and regulations relating to the processing of Personal Data that apply to the processing described in this DPA, including (where applicable) Regulation (EU) 2016/679 (the "GDPR"), the UK GDPR, the Swiss Federal Act on Data Protection, and any national implementing legislation.

"Controller" means the entity that determines the purposes and means of the processing of Personal Data.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

"Personal Data" means any information relating to a Data Subject that is processed by HeadshotPro on behalf of Customer in connection with the Service.

"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.

"Processing" (and its cognates "Process," "Processed") means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure or destruction.

"Processor" means the entity that processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (Controller to Processor).

"Sub-processor" means any third party engaged by HeadshotPro to process Personal Data on behalf of Customer.

"Supervisory Authority" means an independent public authority established by an EU/EEA Member State pursuant to the GDPR.

"Technical and Organisational Measures" or "TOMs" means the technical and organisational security measures described in Annex II.

2. Scope, Roles and Processing Details

2.1. **Roles.** Customer is the Controller and HeadshotPro is the Processor with respect to the Personal Data processed under this DPA.

2.2. **Scope.** This DPA applies to the processing of Personal Data by HeadshotPro on behalf of Customer as described in **Annex I** and as necessary to provide the Service under the MSA.

2.3. **Duration.** This DPA shall remain in effect for the duration of the MSA and shall automatically terminate upon termination or expiry of the MSA, subject to Section 11 (Data Deletion/Return).

2.4. **Processing Details.** The subject matter, nature, purpose, duration, categories of Data Subjects, and types of Personal Data processed are set out in **Annex I**.

3. Processor Obligations

HeadshotPro shall:

3.1. **Documented Instructions.** Process Personal Data only on documented instructions from Customer (including as set out in the MSA and this DPA), unless required to do so by applicable law to which HeadshotPro is subject. In such a case, HeadshotPro shall inform Customer of that legal requirement before processing, unless that law prohibits such notification on important grounds of public interest.

3.2. **Purpose Limitation.** Process Personal Data solely for the purpose of providing the Service as described in the MSA and this DPA, and not for any other purpose including HeadshotPro's own purposes.

3.3. **Prohibition on Marketing, Advertising and Profiling.** HeadshotPro shall not use Personal Data for marketing, advertising, profiling, or any form of behavioural analysis, unless Customer has specifically requested and provided prior written consent for such processing. Any such consent may be withdrawn by Customer at any time, upon which HeadshotPro shall immediately cease the relevant processing.

3.4. **Confidentiality.** Ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5. **Security.** Implement and maintain the Technical and Organisational Measures described in **Annex II** to ensure a level of security appropriate to the risk, including as appropriate:

- (a) the pseudonymisation and encryption of Personal Data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.6. **Sub-processors.** Comply with the conditions set out in Section 5 before engaging any Sub-processor.

3.7. **Data Subject Rights.** Taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to requests for exercising Data Subjects' rights under Applicable Data Protection Law (including rights of access, rectification, erasure, restriction, portability and objection).

3.8. **Assistance with Compliance.** Assist Customer in ensuring compliance with its obligations under Articles 32 to 36 of the GDPR (security of processing, notification of breaches, data protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to HeadshotPro.

3.9. **Deletion or Return.** Upon termination or expiry of the MSA, at Customer's election, delete or return all Personal Data to Customer in accordance with Section 11, unless applicable law requires storage of the Personal Data.

3.10. **Audit.** Make available to Customer all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, in accordance with Section 10.

3.11. **Notification of Conflicting Instructions.** Immediately inform Customer if, in HeadshotPro's opinion, an instruction from Customer infringes Applicable Data Protection Law.

3.12. **Records of Processing Activities.** Maintain records of processing activities carried out on behalf of Customer in accordance with Article 30(2) of the GDPR, including the categories of processing performed, any transfers to third countries, and a general description of the Technical and Organisational Measures. Such records are maintained as part of HeadshotPro's SOC 2 Type II programme and shall be made available to the competent Supervisory Authority upon request.

4. Customer Obligations

4.1. Customer shall comply with its obligations as Controller under Applicable Data Protection Law, including ensuring that it has a lawful basis for the processing of Personal Data and that it provides appropriate notice to Data Subjects.

4.2. Customer shall ensure that its instructions to HeadshotPro comply with Applicable Data Protection Law.

4.3. Customer is responsible for the accuracy, quality and lawful provision of Personal Data submitted to the Service and for ensuring it has the right to transfer such data to HeadshotPro for processing.

5. Sub-processors

5.1. **General Authorisation.** Customer provides a general written authorisation to HeadshotPro to engage Sub-processors to process Personal Data on Customer's behalf. The current list of Sub-processors is available at <https://www.headshotpro.com/legal/sub-processors>.

5.2. **Notification of Changes.** HeadshotPro shall notify Customer of any intended additions or replacements of Sub-processors at least **thirty (30) days** before engaging the new or replacement Sub-processor by sending an email to the address associated with Customer's account. The Sub-processor list at <https://www.headshotpro.com/legal/sub-processors> will also be updated accordingly.

5.3. **Right to Object.** If Customer reasonably objects in writing within **thirty (30) days** after receiving the notification described in Section 5.2 on documented privacy or security grounds, the Parties will confer in good faith to resolve the objection. If the objection is not resolved within thirty (30) days, Customer may terminate the affected Service upon written notice and receive a pro-rata refund of prepaid, unused fees for the terminated portion, as set forth in the MSA.

5.4. **Sub-processor Agreements.** HeadshotPro shall enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those set out in this DPA. HeadshotPro shall remain fully liable to Customer for the performance of each Sub-processor's obligations.

5.5. **Emergency Changes.** HeadshotPro may engage a new Sub-processor without prior notice only where strictly necessary to address an active security incident or to comply with a binding legal obligation. In such cases, HeadshotPro shall notify Customer within five (5) business days and Customer shall retain the right to object in accordance with Section 5.3.

6. International Data Transfers

6.1. **Transfer Mechanism.** To the extent that the processing of Personal Data involves a transfer of Personal Data from the European Economic Area ("EEA"), the United Kingdom or Switzerland to a country that has not been recognised as providing an adequate level of data protection, the Parties agree that such transfer shall be subject to the Standard Contractual Clauses as set out in Section 6.2.

6.2. **Incorporation of SCCs.** The Parties hereby incorporate by reference the Standard Contractual Clauses (Module Two: Controller to Processor) set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the official text is available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj). The SCCs shall apply as follows:

- (a) In Clause 7, the optional docking clause **is included**;
- (b) In Clause 9(a), **Option 2 (General written authorisation)** applies; the time period for prior notice of Sub-processor changes shall be as set out in Section 5.2 of this DPA;
- (c) In Clause 11, the optional language **is not included**;
- (d) In Clause 13, the competent supervisory authority shall be the **Data Protection Commission of Ireland** (or such other supervisory authority as is competent under the GDPR with respect to Customer);
- (e) In Clause 17, Option 1 applies and the SCCs shall be governed by the laws of **Ireland**;
- (f) In Clause 18(b), disputes shall be resolved before the courts of **Ireland**;
- (g) Annexes I, II and III of the SCCs shall be deemed completed with the information set out in the corresponding Annexes of this DPA.

6.3. **UK Transfers.** For transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, as issued by the UK Information Commissioner under Section 119A(1) of the Data Protection Act 2018) ("UK Addendum") shall apply, completed as follows:

- (a) Table 1 shall be completed with the relevant information in Annex I of this DPA;
- (b) Table 2 shall reference the EU SCCs as set out in Section 6.2, Module Two (Controller to Processor);
- (c) Table 3 shall be completed with the information in Annexes I, II and III of this DPA;
- (d) In Table 4, neither Party may end the UK Addendum in accordance with Section 19 of the Mandatory Clauses; the Importer's country is Singapore; the competent supervisory authority is the **UK Information Commissioner's Office (ICO)**.

In the event of a conflict between the UK Addendum and the SCCs, the UK Addendum shall prevail.

6.4. Swiss Transfers. For transfers subject to the Swiss Federal Act on Data Protection ("FADP"), the SCCs shall apply with the following modifications:

- (a) references to "Regulation (EU) 2016/679" and the "GDPR" shall be read as references to the FADP;
- (b) references to "EU," "Union" and "Member State" shall not be interpreted to exclude Data Subjects in Switzerland from exercising their rights;
- (c) the competent supervisory authority under Clause 13 shall be the Swiss Federal Data Protection and Information Commissioner ("FDPIC");
- (d) the SCCs shall be governed by the laws of Switzerland; and
- (e) disputes shall be resolved before the courts of Switzerland.

6.5. Transfer Impact Assessment. HeadshotPro shall, upon Customer's reasonable request, provide information regarding the laws and practices in the country of destination relevant to the transfer, to assist Customer in conducting a transfer impact assessment.

6.6. Government and Law Enforcement Access Requests. HeadshotPro shall:

- (a) promptly notify Customer if it receives a request from any government authority or law enforcement agency for access to or disclosure of Customer's Personal Data, unless such notification is prohibited by applicable law;
- (b) where notification is legally prohibited, use reasonable efforts to obtain a waiver of the prohibition and, to the extent permissible, provide Customer with as much information as possible about the request;
- (c) review the legality of each such request and challenge any request that it reasonably considers to be unlawful, overly broad, or otherwise disproportionate, including by seeking interim measures to suspend the effects of the request pending judicial review;
- (d) disclose only the minimum amount of Personal Data necessary to comply with any request that is determined to be legally binding;
- (e) not provide government authorities or law enforcement agencies with direct, bulk, or indiscriminate access to Personal Data; and
- (f) document all government and law enforcement requests received and make a summary of such requests available to Customer on an annual basis, to the extent permitted by law.

7. Data Subject Rights

7.1. HeadshotPro shall promptly notify Customer if it receives a request from a Data Subject to exercise their rights under Applicable Data Protection Law, and shall not respond to such request without Customer's prior written instructions unless required by applicable law.

7.2. HeadshotPro shall provide reasonable assistance to Customer in responding to Data Subject requests, taking into account the nature of the processing. Such assistance may include providing relevant data extracts, facilitating erasure or rectification requests, and supporting access requests.

7.3. To the extent that Customer is unable to independently address a Data Subject request through the Service, HeadshotPro shall, upon Customer's written request, provide reasonable cooperation. Customer shall reimburse HeadshotPro for reasonable costs incurred in providing such assistance beyond what is available through the Service's standard functionality.

8. Personal Data Breach Notification

8.1. **Notification.** HeadshotPro shall notify Customer without undue delay and in any event within **forty-eight (48) hours** after becoming aware of a Personal Data Breach affecting Customer's Personal Data, so as to enable Customer to fulfil its own notification obligations under Article 33 of the GDPR.

8.2. **Content of Notification.** Such notification shall include, to the extent then known:

- (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned;
- (b) the name and contact details of HeadshotPro's point of contact from whom more information can be obtained;
- (c) a description of the likely consequences of the Personal Data Breach;
- (d) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

8.3. **Cooperation.** HeadshotPro shall provide reasonable cooperation and updates as information becomes available, and shall take reasonable steps to contain and remediate the Personal Data Breach.

8.4. **Record-Keeping.** HeadshotPro shall maintain a record of all Personal Data Breaches, including the facts relating to each breach, its effects and the remedial action taken.

9. Data Protection Impact Assessments

9.1. HeadshotPro shall provide reasonable assistance to Customer in conducting data protection impact assessments and prior consultations with Supervisory Authorities, where required under Applicable Data Protection Law, taking into account the nature of the processing and the information available to HeadshotPro.

10. Audit Rights

10.1. **Right to Audit.** Customer may, no more than once per twelve (12) month period (unless a Personal Data Breach has occurred or a Supervisory Authority requires an additional audit), audit HeadshotPro's compliance with this DPA.

10.2. **Audit Process.** Customer shall provide at least thirty (30) days' prior written notice of any audit. Audits shall be conducted during normal business hours and shall not unreasonably interfere with HeadshotPro's operations. Customer shall comply with HeadshotPro's reasonable security and confidentiality requirements.

10.3. **Third-Party Reports.** HeadshotPro may satisfy audit requests by providing Customer with copies of relevant third-party audit reports or certifications (including SOC 2 Type II reports). If such reports do not reasonably address Customer's audit concerns, Customer may conduct a further audit as described above.

10.4. **Cost Allocation.** Customer shall bear its own costs associated with any audit. If an audit reveals a material breach of this DPA by HeadshotPro, HeadshotPro shall bear its own costs of remediation.

10.5. **Confidentiality.** Audit findings and any reports or certifications provided by HeadshotPro shall be treated as HeadshotPro's Confidential Information under the MSA.

11. Term, Termination, and Data Deletion/Return

11.1. **Term.** This DPA shall commence on the effective date of the MSA and shall remain in force for as long as HeadshotPro processes Personal Data on behalf of Customer.

11.2. **Effect of Termination.** Upon termination or expiry of the MSA:

- (a) HeadshotPro shall, at Customer's written election within thirty (30) days of termination, either return all Personal Data to Customer in a commonly used, machine-readable format or securely delete all Personal Data;
- (b) If Customer does not make an election within thirty (30) days, HeadshotPro shall securely delete all Personal Data;
- (c) Input photos are automatically deleted thirty (30) days after gallery generation by default, as set forth in the MSA;
- (d) HeadshotPro shall confirm deletion in writing upon Customer's request.

11.3. **Retention Exceptions.** HeadshotPro may retain Personal Data to the extent required by applicable law, provided that HeadshotPro shall maintain the confidentiality of such data and shall process it only for the purpose required by law.

12. Liability

12.1. Each Party's liability under this DPA shall be subject to the limitations and exclusions of liability set out in the MSA.

12.2. For the avoidance of doubt, the aggregate liability of each Party under and in connection with this DPA (including the SCCs) shall be subject to the aggregate liability cap set out in the MSA.

12.3. Nothing in this DPA limits either Party's liability for claims by Data Subjects or Supervisory Authorities to the extent such limitation would be prohibited by Applicable Data Protection Law.

13. General Provisions

13.1. **Governing Law.** This DPA shall be governed by the laws of the Republic of Singapore, consistent with the MSA. The SCCs shall be governed as specified in Section 6.2(e).

13.2. **Order of Precedence.** In the event of a conflict between this DPA and the MSA, this DPA shall prevail with respect to data protection matters. In the event of a conflict between this DPA and the SCCs, the SCCs shall prevail.

13.3. **Severability.** If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

13.4. **Amendments.**

- (a) **Non-material changes.** HeadshotPro may update this DPA to reflect changes that do not materially reduce Customer's rights or HeadshotPro's obligations, such as: updates to reflect changes in applicable law or regulatory guidance, updates to Sub-processor details, corrections of typographical errors, or updates to contact information. Such changes will be communicated by email to Customer at least thirty (30) days before taking effect. If Customer reasonably considers that a change is material, Customer may

object in writing within the thirty (30) day notice period, in which case the Parties shall confer in good faith to resolve the objection.

- (b) **Material changes.** Changes that materially reduce Customer's data protection rights or HeadshotPro's obligations require Customer's affirmative consent. HeadshotPro shall notify Customer by email of any proposed material change at least sixty (60) days before the intended effective date. If Customer does not consent, Customer may terminate the affected Service upon written notice within that sixty (60) day period and receive a pro-rata refund of prepaid, unused fees.
- (c) **Individually executed DPAs.** For individually executed DPAs, all amendments require written agreement of both Parties.

13.5. **Entire Agreement.** This DPA, together with the MSA and the SCCs, constitutes the entire agreement between the Parties with respect to data processing matters and supersedes all prior agreements on the subject.

13.6. **Individually Executed DPAs.** Where Customer and HeadshotPro have entered into a separately executed copy of this DPA, the executed version shall take precedence over this published version in the event of any conflict.

13.7. **EU Representative.** HeadshotPro is established outside the European Union and processes Personal Data of Data Subjects who are in the EU. In accordance with Article 27 of the GDPR, HeadshotPro has appointed the following entity as its representative in the European Union:

- **Name:** iuro Rechtsanwälte GmbH t/a Prighter
- **Address:** Schellinggasse 3, 1010 Vienna, Austria
- **Contact:** support@prighter.com

The EU Representative may be contacted by Data Subjects and Supervisory Authorities on all issues related to the processing of Personal Data under the GDPR.

ANNEX I: DETAILS OF PROCESSING

A. List of Parties

Data Exporter (Controller):

- Name: The Customer as identified in the applicable MSA or Order Form
- Address: As set out in the applicable MSA or Order Form
- Contact person: As set out in the applicable MSA or Order Form
- Activities relevant to the data transferred: Use of HeadshotPro's AI headshot generation service for generating professional headshots of Data Exporter's personnel
- Role: Controller

Data Importer (Processor):

- Name: Headshot Pro Photography Pte. Ltd.
- Address: 7 TEMASEK BOULEVARD, #12-07, SUNTEC TOWER ONE, SINGAPORE 038987
- Contact person: Danny Postma, CEO, legal@headshotpro.com
- Activities relevant to the data transferred: Provision of AI headshot generation services, including processing of uploaded photographs and generating AI-generated headshots

- Role: Processor

EU Representative of the Data Importer (Article 27 GDPR):

- Name: iuro Rechtsanwälte GmbH t/a Prighter
- Address: Schellinggasse 3, 1010 Vienna, Austria
- Contact: support@prighter.com

B. Description of Processing

Subject matter of processing: Processing of Personal Data as necessary to provide AI headshot generation services under the MSA.

Duration of processing: For the term of the MSA, plus the period until all Personal Data has been deleted or returned in accordance with Section 11 of this DPA.

Nature of processing: Collection, storage, organisation, use, AI-based image generation, transmission, and deletion of Personal Data. Specifically: receiving uploaded photographs from Customer, processing those photographs through AI models to generate professional headshots, storing generated outputs, and delivering results to Customer.

Purpose of processing: To provide, maintain, secure and support the AI headshot generation Service as described in the MSA.

Categories of Data Subjects:

- Employees, contractors and agents of Customer whose photographs are uploaded
- Other individuals designated by Customer for headshot generation

Categories of Personal Data:

- Facial photographs (biometric-adjacent data)
- Names and email addresses (used for account management, delivery of results, and authentication)
- Payment-related metadata (processed by Stripe; HeadshotPro does not store full payment card data)
- IP addresses and device identifiers (collected incidentally via web platform access)
- AI-generated headshot images (derived from uploaded photographs)

Sensitive data (if any): HeadshotPro processes photographs solely for the purpose of generating AI headshots. Photographs are not processed for the purpose of uniquely identifying a natural person and therefore do not constitute biometric data within the meaning of Article 9(1) GDPR.

Frequency of processing: On a continuous basis during the term of the MSA, as initiated by Customer through use of the Service.

Retention period: As set out in HeadshotPro's Data Management and Retention Policy at <https://www.headshotpro.com/legal/data-management-retention>. Key defaults: input photographs are automatically deleted thirty (30) days after gallery generation; AI-generated headshots are retained for the duration of the MSA and exportable by Customer within thirty (30) days of termination.

C. Competent Supervisory Authority

The competent supervisory authority shall be the **Data Protection Commission of Ireland**, or such other supervisory authority as is competent under the GDPR with respect to the Data Exporter.

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES

HeadshotPro's complete technical and organisational security measures are described in HeadshotPro's Security Policy at <https://www.headshotpro.com/legal/security-policy>. These measures are maintained and updated in accordance with HeadshotPro's SOC 2 Type II programme and internal policies.

In accordance with Article 32(1) of the GDPR, HeadshotPro implements the following measures as appropriate to the risk:

(a) Pseudonymisation and encryption of Personal Data: All data is encrypted in transit using TLS/SSL with 256-bit encryption (100% HTTPS) and at rest using AES-256 encryption. Backups are encrypted in transit and at rest.

(b) Ongoing confidentiality, integrity, availability and resilience of processing systems and services: Cloud-based infrastructure hosted by Google Cloud Storage, Render and Vercel. Multi-factor authentication enforced for production infrastructure and systems that store or process Personal Data. Role-based access control with least-privilege principles. All personnel authorised to process Personal Data are bound by confidentiality obligations and undergo annual security training.

(c) Ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident: Automated hourly backups with point-in-time recovery. Recovery objectives: RTO of two (2) hours, RPO of one (1) hour. Backup restoration tested at least quarterly.

(d) Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures: Regular penetration testing by qualified third parties. Continuous vulnerability scanning. Structured incident response framework with mandatory post-incident reviews. SOC 2 Type II programme for relevant processes.

ANNEX III: LIST OF SUB-PROCESSORS

An up-to-date list of Sub-processors, including entity names, purposes, data access tiers, and entity countries, is maintained at: <https://www.headshotpro.com/legal/sub-processors>.

Customer may subscribe to notifications of changes to the Sub-processor list by emailing legal@headshotpro.com.

Questions? — legal@headshotpro.com

Sub-Processors

The third-party sub-processors HeadshotPro uses to deliver its services.

What is a Sub-processor?

A sub-processor is a third-party data processor engaged by HeadshotPro, including entities from within HeadshotPro, who has or potentially will have access to or process Customer Content containing personal information. HeadshotPro engages different types of sub-processors to perform various functions as explained in the tables below.

Due Diligence & Contractual Safeguards

HeadshotPro evaluates the security, privacy and confidentiality practices of proposed sub-processors that will or may have access to or otherwise process Customer Content and enters into Data Protection Agreements with each such sub-processor.

This advisory does not give Customers any additional rights or remedies and should not be construed as a binding agreement. The information herein is only provided to illustrate HeadshotPro’s engagement process for sub-processors as well as to provide the actual list of third party sub-processors and content delivery networks used by HeadshotPro as of the date of this advisory (which HeadshotPro may use in the delivery and support of its Services).

If you are a HeadshotPro customer and wish to enter into our DPA, please email us at legal@headshotpro.com.

Process to Engage New Sub-processors:

HeadshotPro provides notice via this advisory of updates to the list of sub-processors that are utilized, or which HeadshotPro proposes to utilize to deliver its Services. HeadshotPro undertakes to keep this list updated regularly to enable its Customers to stay informed of the scope of sub-processing associated with the Services.

The following is an up-to-date list (as of the date of this advisory) of the names and locations of HeadshotPro sub-processors and content delivery networks.

Infrastructure Sub-processors – Service Data Storage and Processing

HeadshotPro owns or controls access to the infrastructure that HeadshotPro uses to host and process Customer Content, other than as set forth herein. Currently, the HeadshotPro production systems used for hosting Customer Content for the Services are in facilities in the United States and in the infrastructure sub-processors listed below. The following table describes the countries and legal entities engaged by HeadshotPro in the storage of Service Data. HeadshotPro also uses additional services provided by these sub-processors to process Service Data as needed to provide the Services.

Entity Name	Entity Type	Entity Country
Render	Cloud Computing/Data Center Hosting	US
Vercel Inc.	Cloud Computing/Frontend Hosting	US
Google Cloud Platform	Cloud Computing/Data Center Hosting	EU/US

Entity Name	Entity Type	Entity Country
MongoDB, Inc.	Cloud Database/Data Center Hosting	US
Replicate Inc.	AI Processing and Training	US
Features & Labels (Fal.ai)	AI Processing and Training	US
Cloudflare Inc.	Data storage	US
OpenAI	AI Processing, Content Generation and Vision	US
Google Gemini	AI Processing and Vision	US

Service Specific Sub-processors

HeadshotPro works with certain third parties to provide specific functionality within the Services. These providers are the Sub-processors set forth below. In order to provide the relevant functionality these Sub-processors access Customer Content. Their use is limited to the indicated Services.

Entity Name	Purpose	Entity Country
Front Labs, Inc.	Customer support	US
Functional Software, Inc. (Sentry)	Application Monitoring & Error Tracking	US
Bento, Backpack Internet Pty. Ltd	Email Marketing	Australia
PostHog	Analytics	US
Stripe	Payment Processing	US
PayPal Holdings, Inc.	Payment Processing	US
HitPay	Payment Processing	Singapore
Trustpilot A/S	Review Management	Denmark
Rewardful	Affiliate Program	US

Content Delivery Networks

As explained above, HeadshotPro may use content delivery networks (“CDNs”) to provide the Services, for security purposes, and to optimize content delivery. CDNs are commonly used systems of distributed services that deliver content based on the geographic location of the individual accessing the content and the origin of the content provider. Website content served to website visitors and domain name information may be stored with a CDN to expedite transmission, and information transmitted across a CDN may be accessed by that CDN to enable its functions. The following describes use of CDNs by HeadshotPro’s Services.

CDN Provider	Services Using CDN	Description of CDN Services	CDN Location
Google Cloud Platform	All HeadshotPro Services	Public website content served to website visitors may be stored with Cloudflare, Inc., and transmitted by Cloudflare, Inc., to website visitors, to expedite transmission.	Global

Advertising

HeadshotPro uses third-party advertising services to deliver targeted advertisements. These services may collect and use customer data to provide personalized advertising experiences.

Entity Name	Purpose	Entity Country
Meta Platforms, Inc.	Advertising	US
Google LLC	Advertising and Analytics	US
Microsoft Corporation	Advertising	US

Master Service Agreement

The Master Service Agreement governs the terms under which HeadshotPro provides its services.

MASTER SERVICE AGREEMENT

Version 1.1 — Enterprise Template / Last Updated: 24-06-2026

This Master Service Agreement (this “Agreement”) is entered into as of the Effective Date set forth in the applicable Order Form (the “Effective Date”) by and between Headshot Pro Photography Pte. Ltd., operating as HeadshotPro (“HeadshotPro,” “we,” “us,” or “our”), and the customer identified in the Order Form (“Customer”). This Agreement governs Customer’s access to and use of HeadshotPro’s AI headshot generation services, websites, and applications (collectively, the “Service”).

This Agreement incorporates the Exhibits expressly attached or named below. In the event of a conflict, the following order of precedence applies, except that **Section 12 (Limitation of Liability) governs and controls each party’s monetary liability under this Agreement and all Exhibits notwithstanding anything to the contrary:**

1. the Order Form;
2. this Agreement (main body);
3. Exhibit B (Data Processing Addendum), with respect to data-protection matters;
4. Exhibit A (Information Security), Exhibit C (AI Terms), Exhibit D (Standard Support), and Exhibit E (System Architecture).

The Exhibits expressly named herein are the only exhibits or external terms that govern this Agreement. No other terms, including any consumer or online terms of service published by HeadshotPro, apply.

Table of Contents

- 1. Definitions
- 2. Service; Access; Accounts
- 3. Ownership; Use of Data; No Training
- 4. Data Protection; Security; Deletion
- 5. Service Levels; Credits
- 6. Support
- 7. Acceptable Use; No Benchmarking
- 8. Fees; Taxes; Invoicing; Suspension
- 9. Confidentiality
- L0. Warranties; Disclaimers; Exclusive Remedies; AI Outputs
- L1. Indemnification
- L2. Limitation of Liability
- L3. Term; Termination; Data Return

Exhibits — Exhibit A (Information Security) · Exhibit B (Data Processing Addendum) · Exhibit C (AI Terms of Use) · Exhibit D (Standard Support Offering) · Exhibit E (System Architecture Documentation)

1. Definitions

“AI Headshots” means images generated by the Service from Customer’s uploaded photos and prompts.

“Customer Content” means photos, prompts, and other content or materials uploaded to or processed by the Service on behalf of Customer or its end users.

“Customer Data” means Customer Content and Customer Personal Data, collectively.

“Order Form” means a mutually executed document or electronically accepted ordering interface specifying the Service tier(s), quantities, pricing, term, and any additional terms.

“Confidential Information” has the meaning set forth in Section 9.

“Security Incident” means a confirmed breach of HeadshotPro’s security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Content or Customer Personal Data. The term “Security Incident” is used throughout this Agreement and the Exhibits in place of, and has the same meaning as, the terms “Data Breach” and “Personal Data Breach.”

“Sub-processor List” means the list of HeadshotPro sub-processors made available at <https://www.headshotpro.com/legal/sub-processors>, as updated from time to time per Section 4(b).

“Policies” means HeadshotPro’s publicly posted Privacy Policy, Security Policy, and Sub-processor List, each as referenced herein.

2. Service; Access; Accounts

(a) Provision of Service. HeadshotPro will make the Service available to Customer in accordance with this Agreement and the Exhibits. HeadshotPro may make non-material modifications or improvements to the Service from time to time that do not materially degrade or remove core functionality, performance, or security. Customer acknowledges that artificial intelligence is the core technology underlying the Service, and that this Agreement constitutes Customer’s authorization for the use of AI in delivering the Service.

(b) Access Controls; SSO. The Service supports passwordless Magic-Link authentication for end users by default. Single Sign-On via SAML 2.0 or OIDC (e.g., Microsoft Entra ID, Okta) is available where elected in the Order Form. For designated administrators, multi-factor authentication is enforced via one-time codes sent to administrator email(s). Customer administrators may revoke user access at any time.

(c) Customer Responsibilities. Customer is responsible for: (i) the accuracy, quality, and lawful use of Customer Content; (ii) configuring allowed email domains and administrator recipients; (iii) the acts and omissions of users authorized by Customer under Customer’s accounts; and (iv) obtaining all necessary consents from individuals depicted in Customer Content.

(d) Opt-In Invitations to Customer Employees. Where Customer elects, HeadshotPro will provide Customer administrators a means to invite Customer’s employees via standard-form email invitations. Such invitations clearly identify the Service as opt-in, and end users may decline to participate without penalty.

3. Ownership; Use of Data; No Training

(a) Outputs. Subject to Customer's compliance with this Agreement, HeadshotPro hereby assigns to Customer any right, title, and interest HeadshotPro may have in and to AI Headshots generated from Customer Content. HeadshotPro retains all right, title, and interest in and to the Service, the underlying technology, and any improvements thereto (excluding Customer Content and AI Headshots).

(b) No Model Training. HeadshotPro does not, and will not, use Customer Content or AI Headshots to train, retrain, fine-tune, or otherwise improve HeadshotPro's or any third party's generative models. This is an absolute commitment; no opt-in or other exception applies.

(c) Operational Use Only. HeadshotPro processes Customer Content and AI Headshots solely to provide, maintain, secure, and support the Service, and to comply with law and the Policies.

(d) Aggregated/Anonymous Usage Data. HeadshotPro may collect and use technical, operational, and aggregated usage data that does not identify Customer or any individual ("Usage Data") to operate, analyze, secure, and improve HeadshotPro's products and services.

4. Data Protection; Security; Deletion

(a) Security. HeadshotPro maintains administrative, technical, and organizational measures as described in Exhibit A (Information Security), including encryption in transit and at rest, and operates a program audited under SOC 2 Type II for relevant processes.

(b) Sub-processors; Subscription Notice. Processing is described in the Privacy Policy and Exhibit B (Data Processing Addendum). Customer consents to HeadshotPro's use of the sub-processors identified on the Sub-processor List. HeadshotPro will provide notice of additions or replacements of sub-processors by (i) updating the Sub-processor List, and (ii) sending email notice to each Customer administrator who has enabled sub-processor change notifications in HeadshotPro's admin settings (the "Subscription List"). Customer administrators may enable, disable, or update sub-processor notification recipients at any time via the admin settings; HeadshotPro has no obligation to provide individualized notice to contacts not enrolled in the Subscription List. Normal additions or replacements will be noticed at least ten (10) days before taking effect. If Customer reasonably objects in writing within fifteen (15) days after notice on documented privacy or security grounds, the parties will confer in good faith; if unresolved within thirty (30) days, Customer may terminate the affected Service upon written notice and receive a pro-rata refund of prepaid, unused fees for the terminated portion. HeadshotPro may implement sub-processor changes immediately, with notice posted promptly thereafter, where required to (A) maintain Service availability, security, or legal compliance; (B) respond to a sub-processor's failure, withdrawal, deprecation, or material change in terms; or (C) adopt a sub-processor that offers a meaningful improvement in the security, performance, or quality of the Service.

(c) Retention & Deletion. Input photos are automatically deleted thirty (30) days after gallery generation by default. Customer and individual end users may request earlier deletion at any time. AI Headshots are retained as described in Exhibit E.

(d) Security Incident Notice. HeadshotPro will notify Customer without undue delay, and in any event within seventy-two (72) hours after confirming a Security Incident affecting Customer Personal Data. Such notice will include, to the extent then known, a description of the incident, categories of data affected, and remedial measures taken or proposed. HeadshotPro will provide reasonable cooperation and updates as information becomes available.

(e) Data Location. Customer Data is stored at rest in the European Union, and is passively replicated in encrypted form to United States locations solely for backup and disaster-recovery purposes. Processing of Customer Data may occur in the United States or other locations where HeadshotPro’s sub-processors (identified on the Sub-processor List) perform the AI generation, enhancement, and related functions. Customer Data may transit and be transiently cached by HeadshotPro’s global content-delivery and edge network in encrypted form solely to deliver the Service. HeadshotPro personnel operating outside the European Union storage location may securely and remotely access Customer Data, but will not download, copy, transfer, mirror, or replicate Customer Data to locations other than the European Union primary storage location and the United States backup location described above.

5. Service Levels; Credits

(a) Uptime Commitment. HeadshotPro will use commercially reasonable efforts to achieve 99.9% Monthly Uptime Percentage for the core Service (excluding Maintenance Windows and SLA Exclusions set forth below).

(b) Service Credits. If Monthly Uptime Percentage falls below 99.9% in a calendar month, Customer may request a credit applied to Customer’s account balance for that month, as follows:

Monthly Uptime	Credit
99.0% – 99.89%	5% of monthly fees (or equivalent credits)
95.0% – 98.99%	10% of monthly fees (or equivalent credits)
< 95.0%	25% of monthly fees (or equivalent credits)

Claim Process. To receive a credit, Customer must email billing or support within thirty (30) days after month-end, include reasonable supporting details (timestamps, affected org/workspace), and be in good standing on invoices. **Service Credits are Customer’s sole and exclusive remedy for uptime issues under this Agreement.**

(c) Maintenance Windows. Scheduled maintenance (on reasonable prior notice via status page or Changelog) and emergency maintenance are excluded; HeadshotPro endeavors to schedule during low-usage hours.

(d) SLA Exclusions. Downtime resulting from Customer systems or networks, third-party networks outside HeadshotPro’s reasonable control, denial-of-service attacks, force majeure, misuse, or use contrary to documentation is excluded.

6. Support

Standard support is provided as described in Exhibit D (Standard Support Offering). Any priority or enhanced support offering will be specified in the applicable Order Form.

7. Acceptable Use; No Benchmarking

(a) Acceptable Use. Customer and its users will not, and will not permit any third party to: (i) use the Service for unlawful, infringing, harassing, or fraudulent purposes; (ii) upload Customer Content for which Customer lacks necessary rights or consents; (iii) attempt to circumvent security, rate limits, or access controls; or (iv) generate content that depicts non-consensual likenesses, minors in inappropriate contexts, or that violates

applicable law. HeadshotPro's consumer Terms of Service do not govern this Agreement, and the acceptable-use obligations set forth in this Section 7 apply in their place.

(b) No Competitive Use. Customer will not use the Service, AI Headshots, or any output, performance data, or other information derived from the Service to (i) develop, train, or improve a competing AI image-generation or AI headshot product; or (ii) publish public benchmarks or comparative performance studies without HeadshotPro's prior written consent.

(c) Suspension for Misuse. HeadshotPro may suspend access to the Service in whole or in part on reasonable notice (which may be immediate where required for security, legal, or platform-integrity reasons) where Customer or a user is engaged in a material violation of this Section.

8. Fees; Taxes; Invoicing; Suspension

(a) Fees. Fees, billing frequency, credits packages, and payment terms are set forth in the Order Form. Unless expressly stated otherwise, fees are non-cancellable and non-refundable, and exclusive of taxes (other than those imposed on HeadshotPro's net income), which are Customer's responsibility.

(b) Late Payment; Suspension. Invoices not disputed in good faith within fifteen (15) days of receipt are deemed accepted. Undisputed invoices not paid within thirty (30) days of the due date accrue interest at 1.5% per month (or the maximum legal rate, whichever is lower). HeadshotPro may suspend access to the Service on ten (10) days' written notice if any undisputed amount is more than thirty (30) days past due, without prejudice to its other rights.

(c) Renewal and Pricing Adjustments. Order Forms renew for successive one-year terms unless either party provides written notice of non-renewal at least thirty (30) days prior to the end of the then-current term. HeadshotPro may increase fees at each renewal by providing at least sixty (60) days' written notice, with any increase capped at the greater of (i) 7% or (ii) the percentage change in CPI (US, all urban consumers) over the preceding 12 months.

9. Confidentiality

Each party (the "Receiving Party") will protect the other party's Confidential Information using measures at least as protective as those it uses for its own similar information (and no less than reasonable care) and will use such information solely to perform under this Agreement. Confidential Information excludes information that (i) is or becomes public through no fault of the Receiving Party; (ii) was rightfully known or received from a third party without duty of confidentiality; or (iii) is independently developed without use of the disclosing party's Confidential Information. Each party may disclose Confidential Information as required by law or legal process, provided that (where legally permitted) the Receiving Party gives prompt notice to allow the disclosing party to seek a protective order. The obligations in this Section 9 continue for three (3) years after termination or expiration of this Agreement, except that Confidential Information that constitutes a trade secret remains protected for as long as it qualifies as a trade secret under applicable law.

10. Warranties; Disclaimers; Exclusive Remedies; AI Outputs

(a) By HeadshotPro. HeadshotPro warrants that it will provide the Service in a professional and workmanlike manner and maintain the safeguards described in Exhibit A (Information Security).

(b) Mutual. Each party represents and warrants that it has the power and authority to enter into this Agreement and will comply with all laws applicable to its performance hereunder.

(c) Disclaimers. Except as expressly provided in Section 10(a), the Service and AI Headshots are provided “AS IS” and “AS AVAILABLE,” and HeadshotPro disclaims all other warranties, whether express, implied, statutory, or otherwise, including any implied warranties of merchantability, fitness for a particular purpose, title, non-infringement, or error-free or uninterrupted operation.

(d) AI Outputs. Customer acknowledges that AI Headshots are probabilistic outputs of a generative model and may contain artifacts, inaccuracies, biases, hallucinations, or imperfect renderings of likeness. HeadshotPro makes no warranty as to the accuracy, fitness, suitability, or non-infringement of any specific AI Headshot. Customer is solely responsible for human review and selection of AI Headshots prior to publication or use.

(e) Warranty Remedy. If the Service materially fails to conform to the warranty in Section 10(a) and Customer provides reasonably detailed written notice, HeadshotPro will use commercially reasonable efforts to cure within thirty (30) days. If not cured within that period, Customer may terminate the affected Service and receive a pro-rata refund of prepaid, unused fees for the terminated portion. This Section 10(e) is Customer’s sole and exclusive remedy for breach of the warranty in Section 10(a).

11. Indemnification

(a) By HeadshotPro. HeadshotPro will defend Customer against any third-party claim alleging that the Service, as provided by HeadshotPro and used by Customer in accordance with this Agreement, directly infringes a third party’s intellectual property rights, and will pay finally awarded damages and approved settlements. HeadshotPro’s obligations do not apply to claims arising from: (i) Customer Content; (ii) combinations with items not provided by HeadshotPro; (iii) modifications not made by HeadshotPro; (iv) use of the Service not in accordance with this Agreement or documentation; or (v) any AI Headshot used in a manner not reviewed and approved by Customer.

If the Service becomes, or in HeadshotPro’s reasonable opinion is likely to become, the subject of an infringement claim, HeadshotPro may, at its option: (1) procure for Customer the right to continue using the Service; (2) modify the Service to be non-infringing while retaining substantially equivalent functionality; or (3) terminate the affected Service and refund prepaid, unused fees. The remedies in this Section 11(a) are Customer’s sole and exclusive remedies, and HeadshotPro’s entire liability, for any third-party infringement claim.

(b) By Customer. Customer will defend HeadshotPro against any third-party claim arising from: (i) Customer Content (including allegations that Customer Content infringes any right of a third party or violates any law); (ii) Customer’s or its end users’ use of the Service in violation of this Agreement or applicable law; (iii) Customer’s failure to obtain necessary consents from individuals depicted in Customer Content; or (iv) Customer’s breach of Section 7(b) (No Competitive Use / Benchmarking).

(c) Conditions. The indemnified party must promptly notify the indemnifying party of the claim, provide reasonable cooperation, and grant sole control of the defense and settlement (provided any settlement unconditionally releases the indemnified party and imposes no admission, payment obligation, or material affirmative obligation on the indemnified party).

Sections 11(a) and 11(b) state each party’s sole and exclusive obligations, and the other party’s sole and exclusive remedy, for the types of third-party claims described therein.

12. Limitation of Liability

(a) Exclusion of Indirect Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY WILL BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE

DAMAGES, OR FOR LOSS OF PROFITS, REVENUE, BUSINESS, GOODWILL, ANTICIPATED SAVINGS, OR DATA, IN EACH CASE EVEN IF ADVISED OF THE POSSIBILITY AND REGARDLESS OF THE THEORY OF LIABILITY (WHETHER IN CONTRACT, TORT, STATUTE, OR OTHERWISE).

(b) General Cap. SUBJECT TO SECTION 12(a) AND EXCEPT AS PROVIDED IN SECTION 12(d), EACH PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING ALL EXHIBITS AND ORDER FORMS) WILL NOT EXCEED THE AMOUNTS PAID OR PAYABLE BY CUSTOMER TO HEADSHOTPRO UNDER THE APPLICABLE ORDER FORM DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY (THE "GENERAL CAP"). SERVICE CREDITS ARE NOT "DAMAGES" AND DO NOT COUNT AGAINST THE GENERAL CAP.

(c) Enhanced Cap for Specified Claims. Subject to Section 12(a), the General Cap in Section 12(b) does not apply to: (i) either party's indemnification obligations under Section 11; (ii) HeadshotPro's breach of its data-security, data-privacy, or Section 9 (Confidentiality) obligations; (iii) Customer's breach of Section 7(b) (Acceptable Use; No Benchmarking / No Competitive Use); or (iv) liability arising from a party's gross negligence, willful misconduct, or willful infringement of the other party's intellectual property, in each case to the extent a cap on such liability is permitted by applicable law. For the claims described in clauses (i)–(iv), **each party's aggregate liability shall not exceed one (1) times the total amounts paid or payable by Customer to HeadshotPro under the applicable Order Form during the twelve (12) months immediately preceding the event giving rise to liability (the "Enhanced Cap"), it being expressly acknowledged that the Enhanced Cap equals the General Cap in amount but applies to the categories enumerated in this Section 12(c) so that such categories are subject to a cap rather than uncapped.**

(d) Carve-Outs from All Caps. No cap in Sections 12(b) or 12(c) applies to: (i) Customer's outstanding payment obligations to HeadshotPro under any Order Form; or (ii) liability that, as a matter of applicable law, cannot be limited or excluded by agreement (for example, liability for death or personal injury caused by negligence, or for fraud or fraudulent misrepresentation). To the extent applicable law would otherwise permit a higher limitation, the parties intend the General Cap and Enhanced Cap to apply to the fullest extent so permitted.

(e) Acknowledgment; Allocation of Risk. The parties acknowledge that the limitations and exclusions in this Section 12 reflect the agreed allocation of risk between them, are an essential basis of the bargain, and will apply even if any limited remedy is found to have failed of its essential purpose.

(f) Controlling Provision. **Notwithstanding anything to the contrary in any Exhibit, Schedule, Addendum, or Order Form, this Section 12 governs and controls each party's monetary liability arising out of or related to this Agreement and all Exhibits.**

13. Term; Termination; Data Return

(a) Term. This Agreement commences on the Effective Date and continues for so long as any Order Form remains in effect.

(b) Termination for Cause. Either party may terminate this Agreement or an affected Order Form for material breach not cured within thirty (30) days after written notice. Either party may terminate immediately on written notice if the other party becomes insolvent, makes an assignment for the benefit of creditors, or is subject to bankruptcy or similar proceedings not dismissed within sixty (60) days.

(c) Effect of Termination. Upon termination or expiry: (i) Customer's access to the Service ceases; (ii) Customer retains its AI Headshots subject to Section 13(d); (iii) HeadshotPro will delete Customer Content in accordance with Section 4(c) and Exhibit B; and (iv) any prepaid, unused fees for the terminated portion will

be refunded only if termination is by Customer under Section 10(e), Section 11(a)(3), or Section 13(b) due to HeadshotPro's uncured material breach.

(d) Data Return. Upon termination or expiry, and upon Customer's written request within thirty (30) days, HeadshotPro will provide a one-time export of AI Headshots and reasonably available related metadata in a commonly used, machine-readable format.

(e) Survival. Sections 1, 3 (provided that Section 3(b) (No Model Training) and Section 3(d) survive in full; HeadshotPro's right to continue processing Customer Content under Section 3(c) ends on deletion per Section 4(c)), 8, 9, 10(c)–(e), 11, 12, 13(c)–(e), 14, and 15 survive termination.

14. Publicity

HeadshotPro may identify Customer by name and logo as a customer on its website, customer lists, and pitch decks, in each case in a manner consistent with Customer's brand guidelines provided to HeadshotPro. Customer may opt out of such use by notice in the Order Form or by written request to legal@headshotpro.com (effective within thirty (30) days). Any press release, joint case study, or other public statement that quotes or characterizes Customer requires Customer's prior written consent. Customer may identify HeadshotPro as a vendor in Customer's internal communications.

15. General

(a) Governing Law; Venue. This Agreement is governed by the laws of the State of New York, USA (or, if so designated in the Order Form, Singapore), in each case excluding its conflict-of-laws principles. The parties submit to the exclusive jurisdiction of the courts located in the corresponding forum.

(b) Force Majeure. Neither party is liable for delay or failure to perform (other than payment obligations) caused by events beyond its reasonable control, including acts of God, war, terrorism, civil disturbance, pandemic, government action, labor disruption, internet or telecommunications failures, or third-party provider outages. The affected party will use commercially reasonable efforts to mitigate and resume performance.

(c) Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent (not to be unreasonably withheld), except to an affiliate or in connection with a merger, acquisition, or sale of substantially all assets, provided the assignee assumes all obligations hereunder. Any purported assignment in violation of this Section is void.

(d) Notices. Legal notices must be sent to the addresses set forth in the Order Form, with a copy to legal@headshotpro.com (for HeadshotPro) and the address designated by Customer in the Order Form (for Customer). Notices are deemed given upon receipt (or, for email notices to legal@headshotpro.com, upon written confirmation of receipt).

(e) Independent Contractors. The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, agency, fiduciary, or employment relationship.

(f) Compliance with Laws. Each party will comply with all laws applicable to its performance under this Agreement, including export control, sanctions (OFAC, EU, UK), anti-corruption (FCPA, UK Bribery Act), and data protection laws. Customer represents that neither it nor any of its authorized users is located in, or a national or resident of, a country subject to comprehensive US, EU, or UK sanctions, or is on any restricted-party list.

(g) No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties and their permitted successors and assigns.

(h) Severability; Waiver. If any provision is held invalid or unenforceable, the remaining provisions will continue in full force. A party's failure to enforce any provision is not a waiver of its right to do so later.

(i) Entire Agreement. This Agreement, the applicable Order Form(s), and the Exhibits expressly named herein constitute the entire agreement between the parties and supersede all prior or contemporaneous agreements on the subject matter. No other terms, including any consumer or online terms of service published by HeadshotPro and any “click-through” terms encountered by end users, apply. No waiver or modification is effective unless in writing and signed by both parties (or, for Order Forms, accepted through the designated electronic process).

Signatures

HeadshotPro	Customer
Name: Danny Postma	Name: _____
Title: CEO	Title: _____
Date: _____	Date: _____

Questions? — legal@headshotpro.com

Exhibit A — Information Security

1. Scope

This Exhibit describes the administrative, technical, and organizational measures HeadshotPro maintains to protect Customer Content and Customer Confidential Information. In the event of a conflict between this Exhibit and the main body of the Agreement, the main body governs. Section 12 (Limitation of Liability) of the Agreement controls over any conflicting provision of this Exhibit with respect to monetary liability.

2. Information Security Program

HeadshotPro maintains a written, comprehensive information security program that includes commercially reasonable administrative, organizational, and technical safeguards commensurate with the sensitivity of Customer Content. The program is reviewed at least annually and updated as appropriate.

3. Technical Safeguards

- **Encryption in transit:** TLS 1.2 or higher for all data in transit between HeadshotPro components and between HeadshotPro and external endpoints.
- **Encryption at rest:** AES-256 (or equivalent) for object storage holding source photos and AI Headshots.
- **Access controls:** Role-based access control with least-privilege defaults; MFA required for all HeadshotPro personnel with production access.
- **Logging and monitoring:** Security events are logged and reviewed; anomaly alerts route to the on-call security function.
- **Vulnerability management:** Routine vulnerability scanning; remediation timelines commensurate with severity.
- **Secure development:** Code review and standard secure-SDLC practices for changes to the Service.
- **Malware protection:** Anti-malware controls on production systems and endpoint devices.

- **Network controls:** Firewalling, segmentation between environments, and IDS/IPS as appropriate.

4. Audits

4.1 SOC 2 Type II. HeadshotPro operates a SOC 2 Type II program for relevant processes and will provide its then-current SOC 2 Type II report (and, if applicable, bridge letter) under NDA upon Customer's reasonable written request, no more than once per year.

4.2 Audit by Report. Delivery of HeadshotPro's then-current SOC 2 Type II report (and any applicable bridge letter) satisfies Customer's audit rights under this Agreement. Customer may conduct a direct audit only (i) following a confirmed Security Incident affecting Customer Content, or (ii) where required by Customer's regulator. In either case, such audit is limited to documentation reviews, questionnaires, and interviews conducted under reasonable scheduling, on at least thirty (30) days' notice, no more than once per twelve (12) months, subject to confidentiality and at Customer's expense.

4.3 Audit Exclusions. No audit shall extend to: (i) HeadshotPro source code; (ii) data or information of HeadshotPro's other customers; (iii) HeadshotPro's internal financial, pricing, or commercial information; or (iv) any electronic, penetration, or social-engineering testing of HeadshotPro's systems, except with HeadshotPro's prior written authorization.

5. Incident Response

5.1 Notification. HeadshotPro will notify Customer without undue delay, and in any event within seventy-two (72) hours after confirming a Security Incident affecting Customer Content or Customer Personal Data. Notification will include, to the extent then known, the nature of the incident, categories of data affected, and remedial actions taken or proposed.

5.2 Cooperation. HeadshotPro will cooperate reasonably with Customer's investigation of a Security Incident attributable to HeadshotPro and will share status updates as information becomes available.

5.3 Remediation. HeadshotPro will remediate the underlying cause of a confirmed Security Incident in accordance with the severity and risk, and at HeadshotPro's expense where the Security Incident is attributable to HeadshotPro's acts or omissions.

6. Malware

HeadshotPro will not knowingly introduce malware into the Service and uses commercially reasonable measures (signature- and behavior-based detection, dependency scanning) to prevent introduction of malware. If malware is identified within HeadshotPro's systems that affects Customer Content, HeadshotPro will treat it as a Security Incident and respond under Section 5.

7. Data Return and Destruction

Upon termination of the Agreement or upon Customer's written request, HeadshotPro will delete Customer Content from active systems within ninety (90) days, except (i) Customer Content that HeadshotPro is required to retain by law, and (ii) Customer Content residing on backup media that does not permit selective deletion (which will expire on the standard backup-rotation schedule, not to exceed twelve (12) months). The confidentiality protections of the Agreement continue to apply to any such retained Customer Content.

8. Personnel

HeadshotPro personnel with access to Customer Content are subject to written confidentiality obligations and receive security and privacy training appropriate to their role.

Exhibit B — Data Processing Addendum

1. Scope and Roles

This Exhibit B applies where HeadshotPro processes personal data on behalf of Customer in connection with the Service. For purposes of applicable data-protection laws (including the EU/UK General Data Protection Regulation (“GDPR”), the California Consumer Privacy Act / California Privacy Rights Act (“CCPA”), and other state, federal, or foreign privacy laws of substantially similar effect, collectively “Data Protection Laws”), Customer is the controller (or business) and HeadshotPro is the processor (or service provider) of Customer Personal Data.

2. Definitions

“Customer Personal Data” means personal data within Customer Content.

“Personal Data” has the meaning given under applicable Data Protection Laws (and includes “Personal Information” under the CCPA).

“Process” and “Processing” have the meanings given under applicable Data Protection Laws.

“Sub-processor” means any third party engaged by HeadshotPro to Process Customer Personal Data in connection with the Service.

3. Processing Instructions; Purpose Limitation

HeadshotPro will Process Customer Personal Data only on Customer’s documented instructions (which include this Agreement, the Order Form, and Customer’s reasonable use of the Service) and solely to provide, maintain, secure, and support the Service. HeadshotPro will not:

- Sell or Share (as defined under the CCPA) Customer Personal Data;
- retain, use, or disclose Customer Personal Data outside the direct business relationship with Customer or for any commercial purpose other than to provide the Service;
- combine Customer Personal Data with personal data received from or on behalf of other persons except as expressly permitted by Data Protection Laws; or
- use Customer Personal Data to train, fine-tune, or otherwise improve any generative AI model.

HeadshotPro certifies that it understands and will comply with the foregoing.

4. Sub-processors

Customer provides general written authorization for HeadshotPro to engage Sub-processors to Process Customer Personal Data, subject to (i) the Sub-processor List and the notice, objection, and termination mechanics set forth in Section 4(b) of the Agreement (which Customer agrees satisfy any “prior written authorization” requirement under applicable Data Protection Laws), and (ii) HeadshotPro entering into a written agreement with each Sub-processor imposing data-protection obligations no less protective than those in this Exhibit. Notice and effective-date mechanics, including the broadened circumstances under which HeadshotPro may implement Sub-processor changes immediately, are governed exclusively by Section 4(b) of the Agreement.

5. Data Subject Requests

HeadshotPro will, taking into account the nature of the Processing, provide reasonable assistance through appropriate technical and organizational measures to enable Customer to respond to verifiable requests from data subjects to exercise their rights under Data Protection Laws (access, deletion, correction, opt-out

of Sale/Share, data portability). HeadshotPro will promptly notify Customer if it receives a data-subject request directly relating to Customer Personal Data.

6. Retention and Deletion

Upon expiration or termination of the Agreement, or earlier upon Customer's written request, HeadshotPro will delete or return Customer Personal Data in accordance with Section 4(c) of the Agreement and Exhibit A, Section 7, except where retention is required by law. Upon request, HeadshotPro will provide written confirmation of deletion.

7. International Transfers

Where Customer Personal Data is transferred from the European Economic Area, United Kingdom, or Switzerland to a third country lacking an adequacy decision, the parties incorporate by reference the applicable Standard Contractual Clauses (and UK addendum, as applicable) issued by the European Commission and UK ICO, with HeadshotPro acting as data importer.

8. Security and Security Incident Notification

HeadshotPro will implement and maintain the security measures described in Exhibit A. In the event of a Security Incident affecting Customer Personal Data, HeadshotPro will notify Customer in accordance with Section 4(d) of the Agreement and Section 5 of Exhibit A.

9. Audits

Customer's audit rights under Data Protection Laws are satisfied as described in Section 4 of Exhibit A.

10. CCPA-Specific Provisions

To the extent the CCPA applies, HeadshotPro is a "service provider" and not a "third party." HeadshotPro will (a) comply with applicable obligations under the CCPA; (b) notify Customer if it determines it can no longer meet its obligations under the CCPA; and (c) permit Customer to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information.

11. Order of Precedence

In the event of any conflict between this Exhibit B and the main body of the Agreement with respect to data-protection matters, this Exhibit B controls, except that Section 12 (Limitation of Liability) of the Agreement controls with respect to monetary liability.

Exhibit C — AI Terms of Use

1. Definitions

"AI" means artificial-intelligence systems, including machine-learning and generative models, used by HeadshotPro to provide the Service.

"Inputs" means Customer Content provided to the AI to generate AI Headshots.

"Outputs" means AI Headshots and any other content generated by the AI from Inputs.

2. Authorization

Customer authorizes HeadshotPro to use AI to deliver the Service. AI is the core technology underlying the Service.

3. No Training on Customer Content

HeadshotPro does not, and will not, use Inputs, Outputs, or any other Customer Content to train, fine-tune, or otherwise improve any AI model — whether HeadshotPro's own or a third party's. This commitment is absolute; no opt-in or other exception applies.

4. Ownership of Outputs

Subject to Customer's compliance with the Agreement, HeadshotPro assigns to Customer all right, title, and interest HeadshotPro may have in Outputs generated from Customer's Inputs. HeadshotPro retains all rights in the underlying AI systems, models, and HeadshotPro Confidential Information. Customer does not, by virtue of this Agreement, acquire any rights in HeadshotPro's AI.

5. Acceptable AI Use

Customer will not use the Service to:

- create deepfakes intended to deceive or harm any person;
- generate content depicting non-consensual likenesses or minors in inappropriate contexts;
- generate content that infringes any third party's intellectual property rights;
- generate harmful, hateful, harassing, defamatory, or unlawful content; or
- circumvent any content-moderation, safety, or rate-limiting control of the Service.

6. Output Disclaimer

Customer acknowledges that Outputs are probabilistic and may contain inaccuracies, biases, hallucinations, artifacts, or imperfect likeness rendering. HeadshotPro applies automated quality controls and, where reasonably necessary to address potential biases, hallucinations, or other indicia of unreliability, human review. HeadshotPro makes no warranty as to the accuracy, fitness, or non-infringement of any specific Output. Customer is solely responsible for human review and selection of Outputs prior to publication or use.

7. Compliance

HeadshotPro represents that its use of AI in delivering the Service complies in all material respects with applicable laws and industry standards governing data protection, algorithmic accountability, information security, and AI transparency.

8. No Separate AI Indemnity

AI-related claims are addressed under Section 11 (Indemnification) of the Agreement; this Exhibit does not create any separate indemnification obligation.

9. Order of Precedence

In the event of conflict between this Exhibit C and the main body of the Agreement, the main body governs. Section 12 (Limitation of Liability) of the Agreement controls over any conflicting provision of this Exhibit with respect to monetary liability.

Exhibit D — Standard Support Offering

Applies to Enterprise customers on the Standard Support tier per the Order Form. Priority and Enhanced Support tiers are described separately and elected in the Order Form.

HeadshotPro provides Standard Support to assist Enterprise customers with account access, product usage, billing, and incident reporting. This Exhibit supplements Section 6 (Support) and Section 5 (Service Levels; Credits) of the Agreement.

1. Support Channels

Channel	Address	Use for
Email	support@headshotpro.com	All issues, including account, billing, and incidents
In-product chat	In application	Usage and feature questions

Phone support is not included in the Standard tier.

2. Hours of Operation

- Standard Support is staffed on business days across multiple regions, providing responsive coverage during Southeast Asia / Australia business hours and US East Coast business hours.
- Tickets received outside staffed windows are queued and answered as soon as the next shift comes online.
- Severity 1 incidents affecting platform availability are monitored on a 24/7 basis by the on-call engineering team via the status page and internal alerting, independent of ticket submission.
- HeadshotPro observes a limited number of public holidays each year. Any temporary changes to support coverage are communicated via the status page.

3. Severity Levels and Target Response Times

Severity	Definition	Target First Response (business hours)
Sev 1 — Critical	Service unavailable for all users	Within 2 business hours
Sev 2 — High	Major feature unavailable; significant impact	Within 1 business day
Sev 3 — Normal	Partial impact; workaround available	Within 2 business days
Sev 4 — Low	Questions, minor cosmetic issues	Within 3 business days

Response time is measured from ticket receipt during business hours. Response time is time-to-first-human-response, not time-to-resolution. Resolution time depends on issue complexity.

4. What's Included

- Troubleshooting and diagnosis of platform issues
- Account, billing, and access assistance
- Guidance on documented product features and APIs
- Bug reporting and escalation to engineering
- Incident communication and post-incident summaries on request
- Access to product documentation and the customer status page

5. What's Not Included (Standard Tier)

- 24/7 live support

- Phone or video support
- Dedicated Customer Success or Technical Account Manager
- Custom integration development or scripting
- Training sessions or onboarding workshops
- Named support contact with guaranteed response SLA
- Support for third-party tools, browsers, or environments not officially supported

The above are available under Priority / Enhanced Support tiers — see the Order Form.

6. Designated Customer Contact (Section 5 — Credits)

Per Section 5 of the Agreement, Customer is responsible for monitoring uptime and submitting credit requests. Customer designates in the Order Form:

- Primary Authorized Contact — single point of contact authorized to report incidents and submit Service Credit requests on behalf of Customer.
- Up to two (2) Secondary Contacts — may submit tickets and receive incident communications.

A typical arrangement is for the Customer's IT function (e.g., internal IT Help Desk) to:

- Track outage durations against the published status page.
- Provide a summary to HeadshotPro Support when an issue is reported internally.
- Submit any Service Credit request via email to support@headshotpro.com within thirty (30) days of the incident, per Section 5.

HeadshotPro will validate the reported downtime against internal monitoring and confirm the credit in writing.

7. Service Credit Request Process

- Customer's Authorized Contact emails support@headshotpro.com with subject line: "Service Credit Request — [Date of Incident]."
- Include: affected service window (start/end UTC), description of impact, and any ticket reference.
- HeadshotPro acknowledges within 2 business days and provides a written determination within 10 business days.
- Approved credits are applied to the next invoice; they are not paid in cash and do not extend the Term.

8. Exclusions from Uptime / Credits

Consistent with Section 5 of the Agreement, downtime does not include:

- Scheduled maintenance announced at least 48 hours in advance on the status page
- Emergency maintenance required to protect platform security or integrity
- Issues caused by Customer's systems, network, or misuse
- Force majeure events
- Outages of third-party services outside HeadshotPro's reasonable control

9. Escalation

If a ticket has not received a response within the target window, the Authorized Contact may escalate by replying to the original thread with "ESCALATION" in the subject line. Escalations are reviewed by the Support Lead the same business day.

10. Updates to This Document

HeadshotPro may update this Standard Support Offering from time to time. Material changes that reduce service levels will be communicated to the Authorized Contact at least thirty (30) days in advance.

Contact for questions about this document: support@headshotpro.com

Exhibit E — System Architecture Documentation

1. Purpose and Scope

This Exhibit describes the architecture and data flows of the HeadshotPro Service as deployed for Customer's enterprise users. It is provided to support Customer's security and privacy review and to satisfy the AI implementation documentation referenced in the Agreement.

This document describes system components by function. The specific third-party providers performing each function are identified, and kept current, on HeadshotPro's Sub-processor List referenced in Section 4(b) of the Agreement, which HeadshotPro may update in accordance with that Section. Where the Agreement and this Exhibit conflict, the Agreement governs.

Scope is limited to the enterprise (SSO- or Magic-Link-authenticated, opt-in) deployment. Public marketing-site analytics and consumer self-service billing flows are outside the scope of the Service provided to Customer and are not described here.

2. System Components

Functional components include: identity / SSO broker, application database, object storage, image quality-validation, image generation, image enhancement, transactional email, status page, and in-product support chat. Specific providers are listed on the Sub-processor List.

3. Data Flows

3.1 Authentication and Access

- An end user accesses the Service and authenticates through Customer's identity provider via SSO (SAML 2.0 or OIDC/OAuth; e.g., Microsoft Entra ID) brokered through HeadshotPro's SSO provider, or via passwordless Magic-Link where SSO is not elected.
- The authentication service validates the user and establishes a session; account and workspace records are read from the application database.
- Administrator access additionally requires multi-factor authentication via one-time codes sent to administrator email(s). Administrators may revoke user access at any time.

3.2 Photo Upload and Quality Validation

- An authenticated user uploads source photos through the web application.
- Photos are stored in object storage; a file reference is recorded in the application database.
- The image quality-validation sub-processor performs automated suitability checks. Photos that fail validation are flagged to the user for re-upload.

3.3 Headshot Generation

- Validated photos and prompts are sent to the image generation sub-processor, which generates AI Headshots.

- Generated images are processed by the image enhancement sub-processor for upscaling and enhancement.
- Final AI Headshots are written to object storage; a file reference is recorded in the application database.

3.4 Delivery, Notifications, and Support

- Users are notified and may download their AI Headshots during the applicable retention window. Opt-in invitations and notifications are sent via the transactional email service in a standard form approved for Customer.
- Support is provided through the email and in-product chat support channel, consistent with Section 6 of the Agreement and Exhibit D.

4. Data Storage and Retention

Retention periods stated above are maximums; deletion may occur earlier. Customer Content is processed solely to provide, maintain, secure, and support the Service, consistent with Section 3(c) of the Agreement and Exhibit B (Data Processing Addendum). Customer Content is not used to train HeadshotPro's or any third party's models.

5. Sub-processors

The third-party providers performing the functions described in Section 2 are listed, and maintained current, on HeadshotPro's Sub-processor List referenced in Section 4(b) of the Agreement. HeadshotPro may update providers in accordance with Section 4(b) without amendment to this Exhibit, provided the functional architecture described here is materially maintained.

6. Security

Administrative, technical, and organizational safeguards — including encryption in transit and at rest — are described in Exhibit A (Information Security). Data in transit between components and sub-processors is encrypted, and access to stored Customer Content is restricted to the operations described above.

— End of Master Service Agreement and Exhibits — HeadshotPro v1.1 Enterprise Template —

Security Policy

HeadshotPro's security policy outlines the organizational and technical safeguards implemented to protect customer data.

Security Policy EFFECTIVE DATE: March 12, 2025

Overview

At HeadshotPro, protecting customer data is our top priority. This Security Policy outlines the organizational and technical safeguards implemented to prevent unauthorized access, use, alteration, or disclosure of customer data. HeadshotPro utilizes Google Cloud Storage (GCS), Render, and Vercel platforms. We encourage reviewing our Terms of Service and Privacy Policy for additional details.

Security Team

Our security team includes experienced professionals who have successfully designed, built, and operated secure, internet-facing systems across startups and large corporations.

Security Best Practices

Incident Response

- Established formal procedures for security events with comprehensive training for all staff.
- Immediate escalation, team assembly, and response to security incidents.
- Detailed post-mortem analyses following each incident, reviewed internally and distributed to all relevant teams.
- Prompt written notification to affected customers upon verifying any security breach, detailing the breach and status of our investigation.

Build Automation

- Fully automated deployment processes enabling secure and reliable updates within minutes.
- Multiple daily deployments facilitate rapid deployment of critical security patches.

Authentication

- Mandatory two-factor authentication (2FA) and strong password policies enforced across GitHub, Render, GCS, and Vercel.

Infrastructure Security

- Entirely cloud-based operations; HeadshotPro does not operate physical servers or infrastructure hardware.
- Customer data and services hosted and protected by GCS, Render, and Vercel security practices.
- Robust disaster recovery strategies, including comprehensive backups for all customer data.

Application Monitoring

- Active monitoring using Sentry to rapidly identify and resolve issues.
- Logging of all access to HeadshotPro applications and production consoles.

Data Management

- Customer photos and generated headshots are stored at rest in the European Economic Area by default (Cloudflare R2, Western Europe).
- Failover storage is replicated in encrypted form to the United States (Google Cloud Storage, us-east-1) for backup and disaster recovery only. Application servers run in the United States (Render, hosted on AWS).
- Customer data stored securely in multi-tenant environments, with strict logical separation enforced by application-level privacy controls.
- Systems handling customer data are securely configured following industry-standard security and system-hardening practices.
- Use of subprocessors (Cloudflare, GCS, Render, Vercel) to assist in securely managing customer data.

AI Model Training

- Uploaded photos and generated headshots are never used to train, fine-tune, or otherwise improve any AI model, ours or any third party's. This is an absolute commitment with no exception.

Data Transfer

- 100% HTTPS service delivery.
- Encryption of all data transmissions using industry-standard TLS/SSL protocols with 256-bit encryption.
- Sensitive data encrypted using AES-256 encryption standards.

Payment Processing

- All transactions processed securely through Stripe.

Customer Responsibilities

- Secure management of user accounts and organizational data.
- Protection of user credentials and access via secure email practices.
- Compliance with the HeadshotPro Terms of Service and applicable laws.
- Immediate notification to HeadshotPro regarding compromised credentials or suspected security incidents.
- Security penetration testing or assessments require explicit advance written authorization from HeadshotPro.

Data Management and Retention Policy

How HeadshotPro manages, stores, and retains customer data.

1. Purpose and Scope

This policy details the protocols and measures that HeadshotPro employs to oversee the entire data lifecycle, from the point of creation or acquisition through to retention and eventual deletion.

This policy applies to all employees, contractors, and third parties who have access to our organization's data, regardless of its format or storage location.

2. Policy Statements: Our Commitments

The following commitments outline how HeadshotPro will manage data throughout its lifecycle.

2.1 Data Classification and Labeling

All data must be classified based on its sensitivity and labeled accordingly to ensure proper handling and retention.

HeadshotPro classifies data into the following categories:

Public	Information that is intentionally made available to the public. No potential for damage if disclosed.	Press releases, Public website content, Marketing materials, Annual reports	No restrictions on distribution, Can be freely shared internally and externally, Should be reviewed for accuracy before publication
Internal	Information intended for use within the organization. Limited damage potential if disclosed.	Internal memos or emails, employee directories, internal policies and procedures, project schedules	Share only within the organization. Encrypt when transmitting externally. Use caution when discussing in public places. Dispose of securely (e.g. shredding)
Confidential	Sensitive information that requires protection. Moderate to high damage potential if disclosed.	Customer data, Financial records, Contracts, Intellectual Property (IP)	Share only on a need-to-know basis. Encrypt during storage and transmission. Use strong access controls. Securely dispose (e.g., secure digital wiping, physical destruction). Set contractual agreements with all third parties (e.g., NDAs, security measures)
Critical	Highly sensitive information. Severe damage potential if disclosed.	Passwords, Encryption keys, Merger and Acquisition plans, Trade secrets.	Strictest access controls (e.g. multi-factor authentication). Encrypted at rest and in transit. Audit logging and access monitoring. Prohibited from being stored on mobile device. Dispose only through certified destruction methods.

2.2 Inventory Creation and Maintenance

A data inventory must be created and maintained for all types of data processed by HeadshotPro, covering both structured (databases, CRM systems) and unstructured data (documents, emails).

The inventory should include key details such as:

- Data type (e.g., personal data, financial data)
- Data owner or custodian
- Data location (e.g., servers, cloud platforms, physical storage)
- Data format (e.g., electronic, physical)
- Sensitivity classification (e.g., confidential, internal, public)
- Retention period and disposal requirements

The data inventory must be reviewed and updated regularly to ensure its accuracy and completeness. Any new data sources, data sets, or changes to existing data must be promptly reflected in the inventory.

2.3 Data Flow Mapping

A data flow map must be maintained to document how data moves within the organization and externally (e.g., data transfers to third parties, external storage locations).

This map should be regularly updated to reflect changes in processes, systems, or third-party relationships.

2.4 Data Retention Periods

Data must be retained only for as long as it is needed to fulfill the purposes for which it was collected or as required by legal, regulatory, or contractual obligations.

The default retention period for data types is as follows (adjustable based on business and legal needs):

- **Financial Records:** 7 years
- **Customer Data:** Retained as long as customer relationship exists + at least 30 days to allow the customer to bring their account back into good standing
- **Personal Data (PII):** Retained as specified by data protection regulations (e.g., GDPR) or until the purpose for its collection has been fulfilled
- **Intellectual Property (IP):** Retained for the duration of the IP's legal protection or until no longer required by the organization
- **Security Logs:** Minimum of 1 year, maximum of 5 years
- **Backup Data:** Retained for 1 year and then securely deleted or overwritten.

2.5 Data Disposal and Deletion

Data no longer required must be securely deleted or anonymized. This applies to both physical and electronic records. Physical records must be shredded, while electronic data must be permanently erased using secure data destruction methods.

Backup data must be deleted following its retention period or when it is no longer necessary for restoration or recovery purposes according to the Backup Policy.

2.6 Legal and Regulatory Compliance

All data management activities must comply with relevant legal, regulatory, and contractual obligations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), or other

applicable laws.

Data subject rights (e.g., access, rectification, erasure) must be honored as required by law. A process to handle data subject access requests (DSARs) in compliance with applicable privacy regulations is implemented.

When data is subject to litigation hold or regulatory investigation, retention periods may be extended as needed.

2.7 Data Minimization and Accuracy

Only data that is necessary for the business process should be collected and retained. Data should be accurate, relevant, and kept up-to-date to prevent unnecessary storage of outdated or incorrect information.

2.8 Breach Notification Procedures

HeadshotPro has established a clear process for identifying, reporting, and responding to data breaches. Affected individuals and relevant authorities are notified within required timeframes.

3. Compliance and Enforcement

Compliance with this policy is mandatory for all employees, contractors, and third parties with access to HeadshotPro's data.

In rare cases, business needs, local laws, or regulations may require exceptions. Management will approve any exceptions and define alternative solutions.

Non-compliance may lead to disciplinary action, including termination, as per HeadshotPro's policies.

4. Policy Review and Maintenance

This policy will be reviewed annually or when significant changes occur to maintain its continuing suitability, adequacy, and effectiveness.

Reviews must consider changes in the regulatory landscape.

Version	Last Review Date	Next Review Date	Reviewed By	Approved By
1.0	12-03-2025	01-06-2026	Danny Postma	Danny Postma

GDPR Questionnaire Responses

Pre-answered responses to the GDPR and Article 28 data-processor questions most commonly asked during an enterprise vendor review.

Last updated: June 24, 2026

This document answers the questions HeadshotPro is most often asked during a GDPR vendor assessment. It follows the structure of a standard Article 28 data-processor due-diligence questionnaire, so you can map our answers straight onto your own template.

Every answer here is drawn from documents you can read in full: our [Data Processing Agreement \(DPA\)](#), [Security Overview](#), [Security Policy](#), [Data Management & Retention Policy](#), and [Sub-processor list](#). Where an answer summarises a longer document, we link to the source.

If your questionnaire asks something not covered here, email support@headshotpro.com and we'll respond quickly.

At a glance

Question	Answer
Our role under GDPR	Processor (Customer is Controller)
Legal entity	Headshot Pro Photography Pte. Ltd., Singapore
EU Article 27 representative	iuro Rechtsanwälte GmbH t/a Prighter, Vienna
Data processing agreement	Public, applies automatically to all customers
International transfers	EU SCCs (Module Two) + UK IDTA + Swiss FADP
Certification	SOC 2 Type II (Security)
Sub-processors	Published list, with change notifications
AI training on customer data	Never, no exceptions
Breach notification	Within 48–72 hours of confirmation
Privacy contact	legal@headshotpro.com / support@headshotpro.com

1. Roles, scope and lawful basis

What is HeadshotPro's role under the GDPR — controller or processor?

HeadshotPro acts as a data processor. Your organisation is the data controller and determines the purposes and means of processing. We process personal data only on your documented instructions, as set out in our [DPA](#).

Which legal entity is the processor, and where is it established?

Headshot Pro Photography Pte. Ltd., 7 Temasek Boulevard, #12–07, Suntec Tower One, Singapore 038987.

Do you have an EU representative under Article 27?

Yes. Our Article 27 representative is iuro Rechtsanwälte GmbH t/a Prighter, Schellinggasse 3, 1010 Vienna, Austria (support@prighter.com).

What personal data do you process, and for whom?

We process facial photographs, names and email addresses, payment-related metadata (via Stripe; we do not store full card data), and incidental IP/device identifiers — solely to generate professional headshots for the individuals your organisation designates. Full categories are listed in [Annex I of the DPA](#).

Do you process special-category (Article 9) data?

We process photographs only to generate AI headshots. They are not processed for the purpose of uniquely identifying a natural person and therefore do not constitute biometric data within the meaning of Article 9(1) GDPR.

On what basis do you process the data?

We process strictly as a processor under the controller's instructions and the documented purposes in the DPA. Establishing a lawful basis for the underlying processing (e.g. consent or legitimate interests of the employees photographed) is the controller's responsibility; we support you in meeting it.

2. Article 28 processor obligations

Do you have a written data processing agreement that meets Article 28?

Yes. Our [DPA](#) is publicly available and applies automatically to every customer — there is nothing separate to sign. It covers all Article 28(3) requirements: documented instructions, confidentiality, security, sub-processing, assistance with data-subject rights, breach support, deletion/return, and audit rights.

Do you process personal data only on documented instructions?

Yes. We process personal data only to provide the service and on the controller's documented instructions, and we will inform you if an instruction appears to infringe the GDPR.

Are your personnel bound by confidentiality?

Yes. All personnel authorised to process personal data are bound by confidentiality obligations and complete annual security training.

Will you make information available to demonstrate compliance and allow audits?

Yes. We make our SOC 2 Type II report, penetration-test summaries, and this documentation available to support your assessment, and the DPA provides for audits in line with Article 28(3)(h).

3. International data transfers

Where is personal data stored?

Primary storage for uploaded photos and generated headshots is in the European Economic Area (Western Europe). Encrypted failover backups are replicated to the United States for disaster recovery only. Application servers run in the US. See the [Security Overview](#).

What transfer mechanism covers transfers outside the EEA/UK?

Transfers are covered by approved Article 46 safeguards, incorporated into [Section 6 of the DPA](#):

- **EU/EEA:** EU Standard Contractual Clauses, Module Two (Controller to Processor) from Commission Implementing Decision (EU) 2021/914, with the SCC Annexes completed by the DPA Annexes. Governed by the laws of Ireland (Clause 17, Option 1); competent supervisory authority is the Irish Data Protection Commission.
- **UK:** The International Data Transfer Addendum (Version B1.0) to the EU SCCs, issued by the UK ICO.
- **Switzerland:** EU SCCs as modified for the Swiss FADP (reference to the Swiss FDPIC; protection extended to legal-entity data).

Do you perform transfer impact assessments?

Yes — the transfer safeguards are supported by the technical and organisational measures in [Annex II of the DPA](#) and our [Security Policy](#), which together address the supplementary-measures expectation from the *Schrems II* ruling.

4. Sub-processors

Do you use sub-processors, and is there a current list?

Yes. A current list of all sub-processors — including each entity's function, the data it can access, and its country — is published at </legal/sub-processors>.

How are sub-processors authorised and contracted?

Customers grant general written authorisation for the sub-processors on the published list. Each sub-processor is bound by data-protection terms that are no less protective than those in our DPA.

Will you notify us of changes to sub-processors?

Yes. You can subscribe to change notifications in the admin dashboard, and you may object to a new sub-processor as set out in the DPA.

5. Data-subject rights

How do you assist with data-subject requests (access, erasure, etc.)?

As a processor, we assist the controller in responding to data-subject requests under Articles 12–22. Customers can export generated headshots at any time, and account deletion triggers full erasure of personal data within 14 days of confirmation.

Can individuals' data be deleted on request?

Yes. Input photos are automatically deleted 30 days after generation (earlier on request), and account deletion erases personal data within 14 days. See [Data Management & Retention](#).

6. Security and technical/organisational measures

Is data encrypted in transit and at rest?

Yes. TLS 1.2+ (256-bit) in transit (HTTPS only) and AES-256 at rest across account data, uploaded photos, and generated headshots. Encryption keys are managed at the infrastructure-provider layer; staff cannot access raw keys.

What access controls are in place?

Role-based, least-privilege access with approval and logging; MFA enforced for production infrastructure and for organisation administrators; per-IP and per-account rate limiting. Developers work against staging data, not production customer data.

Do you hold security certifications?

Yes — SOC 2 Type II for the Security Trust Services Criteria, examined by an independent auditor. The report is available via our [Trust Center](#). We also undergo regular independent penetration testing and continuous automated vulnerability scanning.

Where are your full technical and organisational measures documented?

In our [Security Policy](#) and [Annex II of the DPA](#), maintained in line with our SOC 2 Type II programme.

Do you use customer photos or headshots to train AI models?

No. Uploaded photos and generated headshots are never used to train, fine-tune, or improve any AI model — ours or any third party's. This is an absolute commitment with no exceptions.

7. Retention and deletion

How long do you retain personal data?

Input photos are auto-deleted 30 days after generation. Generated headshots are retained for the term of the agreement and remain exportable for 30 days after termination. Backups are taken hourly with point-in-time recovery, retained up to one year, then securely deleted. Full schedule: [Data Management & Retention](#).

What happens to data when the contract ends?

On termination, personal data is deleted or returned in accordance with Section 11 of the [DPA](#), subject to the export window above.

8. Breach notification and incident response

Do you have an incident-response process and breach-notification commitment?

Yes. We maintain a documented incident-response and breach-notification process. We notify affected customers without undue delay and, in any event, within 48 hours of confirming a personal-data breach (and within 72 hours for other security incidents affecting customer personal data). Notice includes the nature of the incident, the categories of data affected, and remediation taken or planned.

9. Accountability, governance and contacts

Have you appointed a Data Protection Officer or privacy contact?

A formal DPO appointment under Article 37 is not mandatory given the nature and scale of our processing. We maintain a designated privacy and data-protection contact who handles all GDPR matters: legal@headshotpro.com. Security questionnaires and reviews are handled at support@headshotpro.com.

What other compliance frameworks do you align with?

We are compliant with GDPR, UK GDPR, CCPA, and Singapore PDPA, and certified under SOC 2 Type II (Security). We do not currently claim ISO 27001 certification.

What logging and audit-trail capabilities do you have?

Every API request is authenticated and scoped to the signed-in user. Production console access and security-relevant events are logged and reviewed for anomalous activity; application health and errors are monitored continuously via Sentry.

What are your availability and recovery commitments?

A 99.9% monthly uptime target with service credits, an RTO of 2 hours and RPO of 1 hour, supported by hourly backups with point-in-time recovery and at least quarterly restoration tests.

Need something this document doesn't cover, or have a questionnaire of your own to complete? Email support@headshotpro.com.