PROFIT RISE

CONSULTING

PUBLIC · EXTERNAL-FACING

Data Protection & Privacy Policy

Hong Kong · Greater Bay Area · Asia-Pacific

Document title	Data Protection & Privacy Policy
Document reference	**PRC-DP-001**
Version	**1.0**
Status	**Approved**
Owner	**Data Protection Officer / Privacy Lead**
Approver	**Managing Director**
Effective date	**12 September 2026**
Next review date	**12 September 2027**
Classification	**Public (external-facing)**

This document is uncontrolled when printed or downloaded. The current version is published at profitriseco.com.

1. Introduction

Profit Rise Consulting ("Profit Rise", "PRC", "we", "us", "our") is committed to protecting the privacy of the individuals whose personal data we handle. As a consultancy delivering AI governance, information security, and digital-transformation services across Hong Kong, the Greater Bay Area, and the Asia-Pacific region, we recognise that privacy is not only a legal obligation but a foundation of the trust our clients, partners, and associates place in us.

This Policy explains how we collect, use, retain, disclose, and protect personal data, and the rights available to individuals. It applies to personal data we process as a data user or controller in the course of our own business (for example, data about clients, prospective clients, suppliers, and website visitors). Where we process personal data on behalf of a client as a data processor, the client's scope of work and our data-processing agreement govern that processing, and this Policy describes our baseline commitments.

2. Scope and application

This Policy applies to all personal data processed by Profit Rise Consulting in any form (electronic, paper, or otherwise) and to all personnel acting for or on behalf of the company, including directors, employees, contractors, and subcontractors.

3. Definitions

- **Personal data** — information relating to an identified or identifiable natural person (a "data subject").
- **Sensitive personal data** — data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, or sexual orientation, and (where the law so provides) biometric or genetic data.
- **Processing** — any operation performed on personal data, including collection, recording, storage, use, disclosure, alteration, transmission, and erasure.
- **Data user / controller** — the person or entity that controls the purposes and means of processing.
- **Data processor** — an entity that processes personal data on behalf of a data user / controller.
- **DPO** — Data Protection Officer / Privacy Lead.
- **PDPO** — the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486).
- **PIPL** — the Personal Information Protection Law of the People's Republic of China.
- **GDPR** — the EU General Data Protection Regulation.
- **PDPA** — the Singapore Personal Data Protection Act 2012.

4. Our privacy principles

We process personal data in accordance with the following principles, which reflect the data protection principles of the PDPO and the principles of the PIPL, GDPR, and PDPA:

1. **Lawfulness, fairness, and transparency** — We process personal data for lawful purposes, fairly, and with clear notice to data subjects.
2. **Purpose limitation** — We collect personal data for specified, explicit, and legitimate purposes and do not process it in a manner incompatible with those purposes.
3. **Data minimisation** — We collect only personal data that is adequate, relevant, and limited to what is necessary.
4. **Accuracy** — We take reasonable steps to keep personal data accurate and up to date, and correct or erase inaccurate data without delay.
5. **Storage limitation** — We retain personal data only for as long as necessary for the purposes for which it was collected, or as required by law.
6. **Integrity and confidentiality** — We protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage using appropriate technical and organisational measures.
7. **Accountability** — We are responsible for, and able to demonstrate, compliance with these principles.

5. What personal data we collect

Depending on our relationship with you, we may collect:

- **Identity and contact data** — name, job title, employer, business email address, telephone number, and postal address.
- **Engagement data** — records of correspondence, meeting notes, proposals, and project-related information.
- **Billing and payment data** — invoicing information and (through our payment providers) payment details.
- **Technical data** — internet protocol (IP) address, browser type, device identifiers, and log data collected when you use our website.
- **Professional data** — information you include in a CV or proposal, where you provide it to us.

We do not intentionally collect sensitive personal data unless you provide it voluntarily and it is necessary for a specific engagement, in which case we will obtain your consent or rely on another lawful basis as required by law.

6. How we use personal data

We use personal data for the following purposes:

- To deliver and administer consulting, assurance, training, and advisory services.
- To communicate with you about engagements, proposals, and events.
- To manage our client and supplier relationships, including contracts and billing.
- To comply with legal, regulatory, and professional obligations (for example, anti-money-laundering or conflict checks).

- To improve our website, services, and security (using aggregated or de-identified data where possible).
- To send you information you have requested or consented to receive.

Where we market our services by direct means, we will ensure a lawful basis and provide an opt-out in every communication.

7. Lawful bases for processing

We process personal data on one or more of the following lawful bases, as appropriate to the jurisdiction and circumstances:

- The performance of a contract with you or steps you have asked us to take before entering a contract.
- Compliance with a legal or regulatory obligation.
- Our legitimate business interests, where these do not override your rights and freedoms.
- Your consent, where we have asked for it, which you may withdraw at any time.

8. Disclosure of personal data

We disclose personal data only as necessary and appropriate:

- To our personnel who need it to deliver services, under obligations of confidentiality.
- To trusted service providers and subcontractors who process data on our behalf under a written data-processing or confidentiality agreement (for example, cloud-hosting, email, accounting, or payment providers).
- To professional advisers (legal, accounting, insurance) under confidentiality.
- To regulators, law enforcement, courts, or other authorities where we are lawfully required or permitted to do so.
- To third parties in connection with a merger, acquisition, or restructuring, subject to appropriate confidentiality and data-protection terms.

We do not sell personal data.

9. Cross-border transfers of personal data

Because we operate across Hong Kong, the Greater Bay Area, and the wider Asia-Pacific region, personal data may be transferred to, stored in, or accessed from jurisdictions outside the one in which it was collected.

Where we transfer personal data across a border, we will do so only where appropriate safeguards are in place, such as:

- A legal adequacy decision, equivalence mechanism, or recognised transfer arrangement applicable to the jurisdiction.
- Written contractual clauses imposing data-protection obligations on the recipient.
- Consent, where legally valid and appropriate.

We apply the strictest applicable standard across the jurisdictions relevant to a given transfer, and we document cross-border transfers in our records of processing.

10. Data security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, disclosure, alteration, loss, or destruction. These are set out in our Information Security Policy and include access controls, encryption, network and endpoint protection, secure development, and staff training. Security measures are proportionate to the sensitivity of the data and the risk of harm.

Our personnel are subject to confidentiality obligations and receive privacy and security awareness training.

11. Data retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected and to satisfy legal, accounting, and regulatory requirements. Specific retention periods are maintained in our retention schedule and are guided by:

- The duration of the relevant client or supplier relationship.
- Any statutory retention requirements (for example, tax and companies legislation).
- The limitation periods applicable to potential claims.
- Any contractual obligations to a client.

When personal data is no longer required, we securely delete or anonymise it.

12. Your rights

Depending on the jurisdiction that applies to your personal data, you may have rights to:

- Be informed about how we process your personal data.
- Request access to, and a copy of, your personal data.
- Request correction of inaccurate personal data.
- Request erasure ("right to be forgotten"), where applicable.
- Object to, or request restriction of, processing.
- Request data portability, where applicable.
- Withdraw consent, where processing is based on consent.
- Lodge a complaint with a data-protection supervisory authority.

We will respond to valid requests within the periods required by applicable law (for example, within 40 days under the PDPO, or within one month under the GDPR, unless extended). We may need to verify your identity before acting, and we may charge a reasonable fee or refuse manifestly unfounded or excessive requests in accordance with law.

To exercise any of these rights, contact us using the details in Section 18.

13. Data protection impact assessments

Where a processing activity is likely to result in a high risk to the rights and freedoms of individuals — including the use of new technologies, large-scale processing, or the processing of sensitive data — we will conduct a data protection impact assessment (also known as a privacy impact assessment) before commencing the activity. The outcome, including any mitigating measures, is documented and reviewed by the DPO.

14. Personal data breach management

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- All suspected or confirmed breaches are reported immediately to the DPO.
- We assess the nature, scope, and risk of the breach and take immediate steps to contain and remediate it.
- We notify affected individuals without undue delay where a breach is likely to result in a high risk to their rights and freedoms.
- We notify the relevant supervisory authority where, and within the timeframes, required by applicable law (for example, within 72 hours under the GDPR), and we follow the Hong Kong Privacy Commissioner's breach notification guidance.
- We maintain an internal breach register and use post-incident learning to strengthen controls.

15. AI and automated decision-making

As a provider of AI-governance services, we hold ourselves to the standards we advise others to adopt:

- We use AI systems in our own operations only where lawful, transparent, and proportionate.
- We do not make decisions that produce legal or similarly significant effects on individuals based solely on automated processing unless permitted by law, with appropriate safeguards and a right to human intervention.
- We apply data minimisation and, where feasible, de-identification or pseudonymisation when using data in AI contexts.
- We do not use client data to train models without the client's prior written consent, and any such use is governed by data-processing terms and our AI governance commitments.

16. Roles and responsibilities

- **Managing Director** — ultimate accountability for privacy and data protection.
- **DPO / Privacy Lead** — day-to-day oversight of this Policy, maintenance of records of processing, handling of data subject requests and breaches, and advice to the business. Where a formal DPO is not required by law, this function is performed by a designated Privacy Lead.

- **All personnel** — comply with this Policy, complete privacy training, and report suspected breaches promptly.

17. Monitoring, audit, and review

We monitor compliance with this Policy through periodic internal review, and we review the Policy at least annually or sooner after a material change in law, client obligations, our processing activities, or an incident.

18. How to contact us

If you have any questions about this Policy, wish to exercise your rights, or wish to raise a concern about how we handle personal data, please contact:

Data Protection Officer / Privacy Lead

Profit Rise Consulting

Email: privacy@profitriseco.com

We will acknowledge and respond to privacy enquiries and complaints promptly and in accordance with law. If you are not satisfied with our response, you may lodge a complaint with the relevant supervisory authority for your jurisdiction (for example, the Office of the Privacy Commissioner for Personal Data, Hong Kong).

19. Changes to this Policy

We may update this Policy from time to time. The current version is published on our website, and material changes will be highlighted appropriately.

Approved by: Ron Ng, Managing Director, Profit Rise Consulting

Date: 12 September 2026