DATA PROTECTION AND PRIVACY POLICY
(RSA-POPIA / UK-GDPR / EU-GDPR)

Trusted Partners is committed to protecting personal information and personal data processed in the course of our advisory services and business operations. We recognise that robust privacy governance is integral to ethical conduct, professional integrity, sound risk management and maintaining the trust of clients, counterparties and stakeholders. This Policy sets out the standards, responsibilities and controls Trusted Partners applies to ensure that personal information is managed lawfully, fairly and transparently, and that appropriate security safeguards are implemented to protect confidentiality, integrity and availability throughout the information lifecycle.

This Policy applies to all Partners, Associate Partners, employees, secondees, associates, sub-consultants and sub-contractors acting for or on behalf of Trusted Partners ("Representatives"). It applies at all times and in all locations in which Trusted Partners operates, including where services are delivered cross-border or where Trusted Partners uses cloud-based or third-party systems to support service delivery. Where local laws, client contractual requirements or regional regulatory expectations impose a higher standard than set out here, Trusted Partners will comply with the higher standard, and this Policy will apply as a minimum baseline.

1 Policy Statement

Trusted Partners is an Environmental & Social Risk Management advisory firm operating across multiple jurisdictions and routinely handling information that may identify individuals, including client representatives, counterparties, associates, and stakeholders engaged during assignments. Trusted Partners is committed to embedding privacy and data protection into the way we work. We will process personal information only for legitimate business purposes connected to professional service delivery and firm administration, and we will implement proportionate safeguards to prevent loss, misuse, unauthorised access, or unlawful disclosure.

Trusted Partners' approach is grounded in accountability and practicality. Data protection is treated as an operational discipline, not a purely legal exercise. We require our Representatives to understand the sensitivity and consequences of personal information handling, to apply good judgement, and to comply with this Policy without limitation or constraint. Every Representative has a duty of care to protect personal information they handle, to prevent avoidable exposure, and to contribute to a culture of confidentiality, secure working practices and ethical decision-making, consistent with the firm's reputation and values.

2 Who is covered by this Policy

This Policy applies to all Representatives of Trusted Partners. It also applies to any person or entity granted access to Trusted Partners systems, records, or data under the firm's authority, including temporary staff and outsourced service providers, to the extent that they process personal information under Trusted Partners' control or instruction. Where Trusted Partners engages third

parties who process personal information on our behalf, we require appropriate contractual commitments, confidentiality provisions, and security controls that are consistent with this Policy and with applicable legal requirements.

Trusted Partners expects its Representatives to lead by example, to implement this Policy in daily practice, and to ensure that anyone reporting to them or working under their direction understands the expectations set out herein.

3 What personal information we process

Trusted Partners processes personal information that is necessary to operate the firm and to deliver professional advisory services. The types of information processed will vary depending on the engagement and context, but typically include identity and contact details, organisational affiliation and role information, professional correspondence, engagement records, billing and financial administration data, and recruitment or contracting information for associates and staff. In some assignments, particularly those involving stakeholder engagement, labour and working conditions, grievance mechanisms, incident investigations, or social baseline work, Trusted Partners may process information relating to community members or workers that is provided by, or processed on behalf of, a client.

Trusted Partners seeks to avoid processing sensitive or special category information unless it is genuinely required for the defined purpose of an assignment or legal compliance. Where such information is necessary, it is handled using heightened safeguards, strict access limitation, and strong confidentiality controls.

4 Email archiving & retention statement

All email correspondence transmitted, received or stored through the Trusted Partners' email systems and archived within the Mimecast environment shall be retained for a fixed period of ninety-nine (99) years in terms of the Company's records retention, legal preservation, compliance and information governance requirements.

For the duration of the applicable retention period, such archived email records shall constitute official business records of Trusted Partners and shall be maintained in a manner designed to preserve their integrity, authenticity, accessibility and evidential value. Owing to the configuration and operation of the Mimecast archival system, archived email correspondence subject to this retention rule cannot be deleted, expunged, amended or otherwise removed by end users and, except where required by law or authorised through formally approved system-level legal or regulatory processes, shall not be capable of deletion before expiry of the prescribed retention term.

This retention requirement applies irrespective of whether the underlying email has been deleted from an individual user mailbox and includes, where applicable, attachments and associated metadata retained as part of the archived record. Access to retained records shall be restricted to duly authorised persons on a need-to-know basis and in accordance with applicable law, Trusted Partners' internal policies, and any relevant legal, regulatory, investigatory, audit or litigation-related requirements.

All employees, contractors and other users of Trusted Partners' email systems shall be deemed to have been notified that email communications may be subject to long-term retention and may

remain recoverable, reviewable and disclosable for lawful business, compliance, legal and evidentiary purposes throughout the full retention period.

5 How and why we use personal information

Trusted Partners processes personal information for defined, legitimate purposes that support service delivery and business administration. These purposes include responding to enquiries, developing proposals, onboarding clients and associates, delivering contracted advisory services, managing projects and quality assurance processes, maintaining records required for governance, audit and professional accountability, meeting legal and tax obligations, maintaining system security and preventing fraud, and administering recruitment and contracting processes.

Where Trusted Partners processes personal information as part of delivering services to clients, the purpose and scope of processing are governed by the client mandate and the agreed terms of engagement. In such cases, Trusted Partners will process personal information only in a manner consistent with the client's instructions, the agreed scope of work, applicable law, and the confidentiality requirements of the engagement.

6 Lawful processing and privacy principles

Trusted Partners processes personal information on a lawful basis appropriate to the context. Depending on the circumstances, processing may be necessary to perform a contract, to take steps at the request of a prospective client prior to entering a contract, to comply with a legal obligation, to protect legitimate business interests in a manner that does not override individual rights and freedoms, or because consent has been obtained where consent is required.

In applying lawful processing, Trusted Partners is committed to the following operational principles. We process personal information fairly and transparently, and we provide appropriate notices where required. We limit processing to a specific purpose and avoid function creep. We apply data minimisation by collecting and using only what is necessary. We take reasonable steps to ensure accuracy where accuracy matters for the purpose. We retain personal information only for as long as it is needed and dispose of it securely when it is no longer required. We protect information using security safeguards proportionate to risk. We maintain accountability through governance, training and oversight, and we document key decisions where necessary to demonstrate responsible practice.

7 Disclosure, sharing and confidentiality

Trusted Partners does not sell personal information and does not permit unauthorised use of personal information for third-party marketing or unrelated purposes. We share personal information only where it is necessary, lawful, and appropriately controlled. This may include sharing with clients and client representatives for purposes of service delivery; with vetted service providers supporting business systems (for example, email, secure storage, document management, accounting and IT services) where processing is governed by confidentiality and appropriate contractual controls; with professional advisers where necessary for legitimate administration; and with regulators, courts, law enforcement or other competent authorities where disclosure is required by law or necessary to protect rights or to comply with lawful process.

All Representatives are required to maintain strict confidentiality in relation to Trusted Partners information, including personal information, client confidential information, and commercially sensitive data. Representatives may not release information externally on behalf of Trusted

Partners without appropriate authorisation and without ensuring that disclosure is lawful, necessary and properly safeguarded.

8 Cross-border processing and international transfers

Trusted Partners operates across jurisdictions and may process personal information across borders, including through international client engagements and the use of reputable cloud-based service providers. Where cross-border transfers occur, Trusted Partners ensures that personal information continues to receive an appropriate level of protection. This is achieved through risk-based safeguards that may include contractual protections, confidentiality undertakings, transfer-related governance controls, access restrictions, and technical security measures. Trusted Partners also considers client requirements and any transfer-related legal constraints applicable to the information being processed.

9 Information security safeguards

Trusted Partners maintains a risk-based security approach designed to protect personal information throughout its lifecycle, from initial collection through use, storage, transfer and disposal. Safeguards are implemented in a manner proportionate to risk and appropriate to the firm's operations. These safeguards include access control and permission management based on need-to-know principles; secure authentication practices; controlled use of portable devices; secure storage and handling of paper records; appropriate protective measures for digital systems and cloud platforms; and responsible information-sharing practices, including avoiding insecure transmission channels where confidentiality may be compromised.

Representatives are required to work securely and to promptly report any suspected loss, unauthorised access, inadvertent disclosure, malware incidents, or other information security concerns that could compromise personal information. Information security is treated as an operational responsibility for all Representatives, not solely an IT function.

10 Data subject rights and requests

Trusted Partners respects the rights of individuals in relation to their personal information. Where applicable, and subject to lawful limitations and appropriate verification, individuals may request access to personal information held about them, request correction of inaccurate data, and in certain circumstances request deletion, restriction of processing, or objection to processing. Where processing is based on consent, individuals may withdraw consent, and Trusted Partners will implement the withdrawal where legally applicable.

Trusted Partners will manage requests through a structured process designed to protect individuals, prevent unauthorised disclosures, confirm identity, maintain record integrity and comply with legal obligations. Where a request relates to information processed on behalf of a client, Trusted Partners may coordinate with the client as the primary decision-maker for that processing context.

11 Incident and breach management

Trusted Partners maintains internal processes intended to identify, manage and respond to suspected or confirmed personal information incidents. If an incident occurs, Trusted Partners will act to contain and assess the event, mitigate harm, secure systems and information, and implement corrective measures. Where notification to affected individuals, clients, or competent authorities is legally required or contractually mandated, Trusted Partners will take appropriate steps within the relevant timeframes and in coordination with the client where the client is the responsible decision-maker for the processing.

12 Accountability, training and communication

The Partners of Trusted Partners have overall responsibility for ensuring that this Policy is implemented and that Trusted Partners meets its legal and ethical obligations relating to personal information. The Partners also retain day-to-day responsibility for monitoring the effectiveness of the Policy, addressing queries, and ensuring that appropriate guidance and controls are maintained.

Trusted Partners commits to ensuring that Representatives receive relevant awareness and practical guidance on the secure handling of personal information. This includes communicating expectations at the outset of engagements with personnel, associates and service providers, and reinforcing secure working practices as appropriate over time.

13 Monitoring, risk assessment, and review

Trusted Partners treats data protection and privacy as an ongoing risk management discipline. As part of our internal risk assessment and governance processes, we periodically review the suitability, adequacy and effectiveness of our privacy controls and operational practices. Where gaps are identified, Trusted Partners will implement improvements that are proportionate to risk and appropriate to the firm's operations, client expectations, and legal requirements. Representatives are expected to support this process by raising concerns, disclosing suspected wrongdoing or weaknesses, and contributing to a culture of integrity and continuous improvement.

This Policy does not form part of any employee's contract of employment and may be amended at any time to reflect changes in operations, technology, service delivery, or legal requirements.

14 Policy review and effective date

This Policy is reviewed at least annually and additionally when material changes occur to Trusted Partners' operations, systems, service lines, client requirements, or applicable legal obligations. The most recent version remains in effect until it is formally updated and re-issued.

15 Contact

Any questions regarding this Policy, requests to exercise privacy rights, or concerns regarding the handling of personal information should be directed to **Trusted Partners**' designated privacy contact / Information Officer function using the contact details provided through the firm's official channels.

DATE OF APPLICABILITY	NEXT REVIEW
March 01, 2026	February 28, 2028

NAME	POSITION	DATE	SIGNATURE
Malcolme Logie	Partner	March 01, 2026	Malcolme Logie
Nishal Sewruttan	Partner	March 01, 2026	Nishal Sewruttan