DATA PROTECTION POLICY

Version: 3.0
Effective Date: 31 January 2024
Last Reviewed:1 January 2024

1. Introduction and Purpose

This policy sets out how Demerara Associates ("we", "us", "our") handles the collection, storage, processing, and transfer of personal data so as to comply with the Data Protection Act 2023 of Guyana and the GDPR (where applicable). We are committed to protecting the rights and privacy of data subjects and to processing personal data in a lawful, fair and transparent manner**.**

2. Scope

This policy applies to all personal data processed by us, whether belonging to customers, clients, employees, contractors, suppliers or other individuals ("data subjects"). It covers all processing activities carried out by or on behalf of Demerara Associates, in Guyana and in any other jurisdiction.

Under the Guyana Act, the law "applies to … the processing of personal data in the context of the activities of a data controller or a data processor established in Guyana; and … the processing of personal data of data subjects in Guyana by a data controller or data processor".

Under the GDPR, the law applies to organisations processing personal data of individuals in the EU/EEA (or offering goods/services to them).

3. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person. (Aligning with the Guyana Act and GDPR.)

"Sensitive Personal Data" (or "Special Categories" under the GDPR) refers to personal data revealing e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, health data, sexual orientation, etc. The Guyana Act covers "sensitive personal data" in specific provisions.

"Data Subject" means the identified or identifiable natural person to whom the personal data relates.

"Data Controller" means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Data Processor" means a person or organisation which processes personal data on behalf of the controller.

"Processing" means any operation or set of operations on personal data (collection, storage, use, disclosure, erasure etc.).

"Data Protection Officer (DPO)" means the person designated by us to monitor compliance with data protection laws (if applicable).

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signify agreement to the processing of

personal data. (GDPR standard)

4. Principles of Processing

We commit to adhere to the following principles, which reflect both the Guyana Act and the GDPR:

Lawfulness, fairness and transparency – personal data shall be processed lawfully, fairly and in a transparent manner. (Guyana Act: "must be processed lawfully, fairly and in a transparent manner.")

Purpose limitation – collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data minimisation – adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy – personal data shall be accurate and, where necessary, kept up to date. Every reasonable step to ensure that inaccurate personal data are erased or rectified without delay (GDPR Article 5).

Storage limitation – personal data shall not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are processed.

Integrity and confidentiality (security) – personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability – the data controller is responsible for, and must be able to demonstrate compliance with these principles.

By design and by default – data protection considerations shall be built into processing activities from the outset. (GDPR)

Rights of the data subject – we will respect the rights granted to data subjects under applicable laws (see Section 6).

5. Roles and Responsibilities

Demerara Associates is the Data Controller for the processing of personal data as described in this policy.

All employees, contractors and third-party processors must adhere to this policy and any related procedures.

6. Data Subject Rights

We recognise the following rights under the GDPR and the Guyana Act:

The right of access by the data subject (to obtain confirmation of whether personal data is being processed, and access to that data)

The right to rectification of inaccurate personal data.

The right to erasure ("right to be forgotten") under certain conditions.

The right to restriction of processing.

The right to data portability (receive data in a structured, commonly used and machine-readable form, and transmit it to another controller)

The right to object to processing in certain circumstances.

The right to object to automated individual decision-making (including profiling) under certain circumstances.

The right to withdraw consent at any time (where consent is the basis for processing) without affecting the lawfulness of processing before withdrawal.

We shall have processes in place to respond to data subject requests in accordance with legal time-limits and verify the identity of the requestor as required.

7. Lawful Basis for Processing

Where the GDPR applies, we will ensure that any processing of personal data is based on one or more of the lawful bases set out under the GDPR (consent; contract; legal obligation; vital interests; public task; legitimate interests).

Under the Guyana Act, processing must satisfy the conditions provided in the legislation and any regulations.

We will document which lawful basis applies for each processing activity.

8. Consent

Where we rely on consent as the lawful basis for processing, we will ensure that consent is:

- Freely given, specific, informed and unambiguous;
- Given by a clear affirmative action;
- Easy for the data subject to withdraw at any time.
- We will keep records of consents obtained (GDPR standard).

9. Data Transfers Outside Guyana / Outside the EEA

Guyana Act

The Guyana Act sets specific conditions for the transfer of personal data outside Guyana.

GDPR (when applicable)

When transferring personal data outside the EU/EEA, we will ensure that appropriate safeguards are in place (e.g., adequacy decision, standard contractual clauses, binding corporate rules) or that another legal exemption applies.

10. Security of Personal Data

We will implement and maintain appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Measures may include (but are not limited to):

- Encryption and pseudonymisation where possible;
- Access controls and authentication mechanisms;
- Regular data backups, secure storage, and disaster recovery plans;
- Employee awareness training and role-based access;
- Secure disposal of personal data when no longer required;
- Periodic security risk assessments and audits.
- We will review and update our security measures regularly.

11. Data Breach Notification

In the event of a personal data breach, we will:

Investigate the breach promptly;

Assess whether the breach is likely to result in a risk to the rights and freedoms of data subjects;

If required by the GDPR, notify the relevant supervisory authority within 72 hours of becoming aware of the breach, unless the notification is delayed because it is unlikely to result in a risk to individuals' rights and freedoms.

Notify affected data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

Under the Guyana Act, comply with any national breach-notification requirements as may be prescribed (and maintain records of all breaches).

Keep records of all data breaches, regardless of whether notification is required.

12. Retention and Disposal

We will retain personal data only for as long as necessary to fulfil the purposes for which it was collected (and to satisfy legal, regulatory or contractual obligations). We will establish retention schedules and/or criteria, and securely dispose of or anonymise personal data when no longer needed.

13. Third-Party Processors and Contracts

Where we engage third-party processors (i.e., organisations that process personal data on our behalf), we will:

- Carry out due-diligence to ensure the processor is capable of implementing appropriate data protection measures;
- Enter into a written contract (data processing agreement) setting out the processor's obligations (including security, confidentiality, data subject rights, breach notification, return or deletion of data) (GDPR Article 28 style)
- Monitor the processors' performance and compliance with this policy and applicable law.
- Ensure that where personal data is transferred internationally, the contractual arrangements include appropriate safeguards.

14. Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in high risk to the rights and freedoms of natural persons (for example large-scale processing of sensitive data, systematic monitoring, new technologies), we will carry out a DPIA in accordance with the GDPR and national requirements.

The DPIA will evaluate the risk of the processing, the measures to mitigate risk, and whether the processing should proceed.

15. Training and Awareness

We will provide regular training to employees, contractors and other relevant individuals on data protection principles, this policy, secure data handling and incident-reporting procedures. We will promote a culture of data protection and privacy awareness.

16. Accountability, Monitoring and Review

We will maintain records of our data processing activities (including purposes, categories, retention periods, third-party transfers, security measures). (GDPR Article 30 style)

We will monitor compliance with this policy and the relevant laws, conduct audits and reviews, and update this policy and related procedures on a regular basis (at least annually or when there is a significant change in our processing activities or applicable law).

17. Responsibilities for Violation

Breaches of this policy or the applicable laws may result in disciplinary action (for employees/contractors) and may expose the organisation to regulatory sanctions, reputational damage and legal liability. We reserve the right to take appropriate corrective action.

18. Contact and Complaints

If you have any questions about this policy, or would like to request access to your personal data or exercise any of your rights, please contact:

Rawl Prescott
Email: demeraraassociates@demeraraassociates.com
Phone: 592 668 3665

We will also provide a mechanism to permit complaints from data subjects about our processing of their personal data.

19. Policy Review

This policy will be reviewed at least once every [12] months, and/or whenever there are significant changes to our operations, regulatory environment or risks. Any revision will be documented and the version history updated.

End of Policy