DATA PROTECTION POLICY

Revision History		
Revision reference	Date	Description of changes
V.01	June 2021	- Initial Draft
V.02	Sept 2021	- Review post re-domiciliation
V.03	February 2023	- No changes
V.04	August 2024	- Expanded on the applicability of the Data Protection Policy – clause 2 - Enhanced the responsibilities of the DPO – clause 3 - Made minor amendments to the commitment of Grit under Actions – clause 6 - Enhanced our data protection obligations by adding responsibilities if a data controller and data processor – clause 7 - Enhanced our data protection principles within the policy – clause 8 - Revised how we transfer data and the rights of data subjects – clause 9 - Added a new clause 13 on updating this policy - Expanded on the glossary of terms.

grit

Contents

1. INTRODUCTION

Grit Real Estate Income Group Limited (the "Company" or "Grit") handles the personal data of its clients, staff, intermediaries, supplier contacts and other third parties. This data consists of information that relates to and identifies a living individual and may be stored physically or electronically. Personal data includes special categories of data, particularly sensitive data which warrants extra protections. Personal data does not include information relating to solely corporate entities or other vehicles. However, there may be corresponding duties of confidentiality in respect of corporate information and in these circumstances, we will adopt an appropriate similar standard of protection.

The protection of personal data is of paramount importance and a critical responsibility that we take seriously at all times. Grit may be exposed to regulatory action, fines and reputational damage for failure to comply with the provisions of applicable data protection legislation.

With this Data Protection Policy (the "Policy"), Grit ensures that data including personal data and special categories of personal data) (the "Data") are collected, gathered, held, stored, processed, and handled electronically, manually, or otherwise (fairly, transparently, with respect towards individual rights of Data Subjects (as defined below) and in accordance with applicable data protection legislations).

A glossary has been made available at the end of this Policy which provides explanation of some of the key terms used in the Policy.

2. APPLICABILITY

This Policy (and its related policies and procedures in place from time to time) applies to the Grit Group of Companies across all jurisdictions in which Grit has a presence, even where the legislation of that jurisdiction does not specifically provide for data protection or where its data protection rights are lesser than the standard set by the data protection legislation.

Employees of the Company and of any of its subsidiaries, as well as contractors, consultants, partners, and any other external entity of the Company and of any of its subsidiaries (the "Stakeholders") are required to follow this Policy. Generally, this Policy applies to anyone Grit collaborates with or who acts on its behalf and may need occasional access to Data.

The Stakeholders are required to comply with this Policy when processing personal data on behalf of Grit and to attend training on its requirements. This Policy sets out what Grit expects from its Stakeholders, including the employees of the Grit group of companies, in order for Grit to comply with the data protection legislations and to ensure compliance with this Policy.

Key messages set out in the Policy for Stakeholders, but not limited to, are as follows:

- If any data subject seeks to exercise any rights (e.g. right of access, rectification, erasure), he or she must immediately inform the Data Protection Officer of the Company and/or of its relevant subsidiary or affiliate (the "DPO") and not take any action without consulting the DPO; Stakeholders must comply with this Policy.

No changes, rectification, erasures nor any amendments in any kind shall be made to any data pertaining to data subjects without consultation of the DPO. Any such approved amendments to data of data subjects must be made in writing and signed by the DPO.

- Be familiar with the "Privacy Policy" – if a data subject or stakeholder thinks that Grit is processing data outside the terms of its Privacy Policy, he or she should alert the DPO.
- Personal data must be collected for explicit, specified and for legitimate purposes; and such data must not be processed in an incompatible way with those purposes. Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- If a data subject or stakeholder identifies any instances where he or she needs to process large scales of personal data, transfer it to another jurisdiction or the data is particularly sensitive, then the DPO must be consulted, and an action plan must be agreed to process such requests.
- Always ensure compliance with the information security measures at Grit to ensure the data we hold is kept as securely as possible.
- If any data subject or stakeholder notices that data is somewhere where he or she does not think it should be, then the DPO must be informed immediately.

Stakeholders must interpret and act in accordance with this policy as well as with other such related policies and procedures available, which enhance this Policy.

This Policy (and its related policies and procedures) is an internal document. It must not be shared with clients, regulators or other third parties without the approval of the DPO.

3. COMPLIANCE WITH LAWS

This Policy issued by Grit, in respect of Grit and any of its affiliated entities and subsidiaries (together "Grit Group"), refers to Grit's commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

Grit, registered in Guernsey, is listed on the London Stock Exchange and on the Stock Exchange of Mauritius and has subsidiaries in different jurisdictions. Accordingly, it has to comply with applicable data protection legislation, *including but not limited to* the Mauritian Data Protection Act 2017 (the "DPA") together with any successor legislation or regulations, the Data Protection (Bailiwick of Guernsey) Law, 2017 ("Guernsey DPL"), the General Data Protection Regulation EU 2016/679 (as amended or replaced from time to time) (the "GDPR") ("Applicable Data Protection Legislations") and the Data Protection Act 2018 (DPA 2018).

Stakeholders must comply with this Policy, even where local law is less onerous. Where local law is more onerous, Stakeholders must comply with those laws in addition to this Policy. Where there is, or may be, a conflict, the Stakeholder should consult the Head of Risk & Compliance and the DPO.

4. Data Protection Officer

Grit has appointed a DPO with responsibility for overseeing this Policy and, as applicable, developing related policies and procedures. The responsibilities of the DPO are:

To work independently, and report to the highest management level with adequate resources and information in order to meet obligations set out in the Data Protection Act.

- To review all data protection procedures and related policies, in a timely manner.
- To duly inform and advise GRIT as well as all employees about the obligations to comply with the DPA and other such data protection laws.
- To advise data subjects on their rights under the data protection legislation and organize necessary training as and when required.
- To handle data protection queries from those covered by this Policy.
- To address any questions arising as to the implementation of this policy document; or on the data protection law; or address any particular concern which stakeholders may have relating to adherence to this Policy.
- To be the first point of contact for the Data Protection Office and for any individuals whose personal data are processed.

The current DPO is Dhanalaksmi (Tina) Gopaul, who can be reached at tina@grit.group.

5. SCOPE

This Policy refers to all identified or identifiable living individuals (including employees, agents, nominees, trustees, préposés, directors, shareholders, beneficial owners, job applicants, customers, investors, potential investors, suppliers, consultants, professional advisors, sponsors) (together the "Data Subjects" and each a "Data Subject") who provide any Data or information to us.

The Company shall only process the Data in accordance with the instructions and consent of the Data Subject and/or their ordinary professional activities (including the fulfilment of its legal, administrative, or regulatory obligations), or to conduct research about the use of our website.

A Data Subject may withdraw their consent at any time.

6. POLICY ELEMENTS

As part of our ordinary professional activities and operations, we need to collect, store, retain, process, and share Data. This Data includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, tax identification number, financial data, electronic identifying data, etc.

Our Company collects this Data in a transparent way and only with the full cooperation and knowledge of interested parties. Once this Data is available to us, the following rules apply.

Our Data will be:

- Accurate and kept up to date.
- Collected fairly and for explicit, specified, legitimate or lawful purposes only, and will not be processed in a manner incompatible with those purposes.
- Processed by the Company in accordance with the rights of the Data Subjects.
- Protected against any unauthorised or unlawful access and processing by internal or external parties.

Our Data will not be:

- communicated informally.
- kept longer than is necessary for the purpose for which the Data is processed.
- transferred to organizations, states or countries that do not have adequate data protection policies in relation to the processing of Data in accordance with applicable laws; and
- distributed to any party other than the ones agreed upon by the Data Subject (exempting legitimate requests from law enforcement authorities).

In addition to the above ways of handling the Data, the Company recognises its obligations towards people to whom the Data belongs. Accordingly, the Company undertakes to:

- Inform Data Subjects, on what data of theirs' is being collected.
- Inform Data Subjects about how and why the Company will process their Data.
- Inform Data Subjects about who has access to their information.
- Make adequate provision for case of lost, corrupted, or compromised Data; and
- Allow people to access their Data or request that we modify, erase, reduce, or rectify Data in relation to them contained in our databases, subject to relevant laws or policies relating to the retention of Data.

7. ACTIONS

To exercise data protection, Grit is committed to:

- Restrict and monitor access to Data.
- Develop transparent Data collection procedures.
- Train employees about online privacy and security measures.
- Implement appropriate physical, technical and organisational measures and build secure networks to reasonably protect online Data from unauthorised access or cyberattacks.
- Establish clear procedures for reporting privacy breaches or Data misuse.
- Ensure that all agreements are provisioned with a data protection clause, including, how data will be handled and processed.
- warrant that every stakeholder submits to equivalent obligations with respect to Data which are imposed on the Company under this Policy and under applicable laws.
- Identify all reasonably foreseeable internal and external risks as to Data under its control.
- Ensure safeguards are continually updated to respond to new risks or deficiencies; and
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.).

Our data protection policy is shared on our website.

8. DATA PROTECTION OBLIGATIONS

8.1 Controller and processor

Grit Group of Companies are data controllers (can determine the purpose(s) and means of processing personal data) and in some instances, can also be data processors (can process personal data on behalf of the data controller), but in different contexts or different sets of data. Both controllers and processors are required to register/notify in certain jurisdictions in accordance with applicable laws. The DPO handles such registrations and maintains a register reflecting current registrations/notifications.

Where Grit Group is acting as a processor, appropriate processing terms must be agreed between Grit Group and the relevant client entity.

8.2 Responsibilities of a Data Controller:

- Determining the Purpose: The data controller decides why the data is being collected and how it will be used.
- Ensuring Compliance: The data controller must ensure that data processing activities comply with data protection laws, including obtaining consent where necessary and implementing appropriate security measures.
- Data Subject Rights: The data controller is responsible for enabling individuals (data subjects) to exercise their rights, such as accessing their data, requesting corrections, or having their data deleted.
- Data Breach Notifications: The data controller must notify the relevant authorities and affected individuals in the event of a data breach, where required by law.

8.3 Responsibilities of a Data Processor:

- Security: The data processor must implement adequate technical and organizational measures to ensure the security of the data.
- Data Breach Notification: The processor is required to notify the data controller without undue delay if a data breach occurs.
- Sub-Processing: If the data processor wishes to subcontract any part of the processing to another processor (sub-processor), it would need to get Grit's data controller's approval.

9. DATA PROTECTION PRINCIPLES

Grit's Data Protection Policy complies with the data protection obligations imposed by legislation on those handling personal data (data controllers and processors) and requires them to process that data in accordance with the applicable law. In summary, these principles require that personal data shall be:

- processed lawfully, fairly and in a transparent manner (lawfulness, fairness, and transparency).

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

- accurate and, where necessary, kept up to date (accuracy).

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (integrity and confidentiality).

9.1 Lawfulness, fairness, and transparency

Personal data must be processed fairly, lawfully and in a transparent manner in relation to the data subject. Grit Group may only collect, process, and share personal data fairly and lawfully, and for specified lawful purposes. Data protection legislation allows processing for specific purposes, some of which are set out below:

- The processing is necessary for performance of a contract: This basis may be relied on where the personal data collected and processed are required to fulfil our engagement with the data subject.

- To pursue our legitimate interests: If the processing of personal data is in the legitimate interest of Grit Group and is judged not to prejudice the interests or fundamental rights and freedoms of data subjects, this may be a lawful reason for processing. The legitimate reasons relied on by Grit Group are set out in the Grit Group privacy notice.

- The data subject has given his or her consent: Grit Group should bear the burden of proof for establishing a data subject consent to the processing of their personal data for a specified purpose. Consent is any freely given specific, informed, and unambiguous indication or the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his personal data relating to him being processed. Where there is no other reasonable basis for the processing, Grit Group will rely on consent for processing. The data subject's agreement to the processing must be indicated clearly either by a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not be sufficient. Data subjects must be easily able to withdraw consent, this forms part of our Privacy Policy. If a data subject approaches any internal stakeholder (Employee or Director) within the Grit Group to withdraw their consent to the processing of their personal data, the internal stakeholder must bring this to the immediate attention of the DPO. Unless we can rely on another legal basis, explicit consent is usually required for processing special category data and for cross border data transfers. Usually, we will be relying on another legal basis (and not require explicit consent) for most types of special category data. However, if consent is required, this should be evidenced, and appropriate records kept.

- To meet our legal compliance obligations: We may rely on this ground where we have a legal obligation to carry on the processing, other than an obligation imposed by contract.

- Vital interests of the data subject: We may process personal data without consent where that is necessary to protect the vital interests of the data subject or another natural person.

The purposes for which we process personal data are explained in the Grit Group Privacy Policy. If any Stakeholder is concerned that the processing which he or she is undertaking is not adequately captured in the Privacy Policy, he or she must bring this to the attention of the DPO and shall not continue processing that personal data without the approval of the DPO.

A copy of our Privacy Policy explaining the purposes for our data processing can be found here https://grit.group/google-privacy-policy/. The Privacy Policy also explains to data subjects how and why we will use, process, disclosure, protect and retain personal data.

Whenever Grit collects personal data directly from data subjects, the data controller and/or data processor must provide the data subject with the Privacy Policy when the data subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source) we must also provide the data subject with the Privacy Policy. A Stakeholder acting on behalf of Grit Group must also check that the personal data was collected by the third party in accordance with the data protection legislation and on a basis which contemplates our proposed processing of that personal data.

9.2 Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. No Stakeholder can use personal data for new, different, or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consent where necessary.

9.3 Data minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purpose for which it is processed. Personal data may only be processed when performing as part of the requirements of the duties of a Stakeholder. Personal data cannot be processed for any reason unrelated to duties under the role of a Stakeholder.

Stakeholders should also keep in mind that personal data may be disclosable (including expressions of opinion) and so care should be taken in recording it.

Stakeholders must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Grit Group's Record Retention Policy.

When handling personal data, regard should be given to any contractual terms or policies regarding information security.

9.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

Stakeholders will ensure that the personal data Grit Group uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it has been collected. Stakeholders must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Stakeholders must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

9.5 Storage limitation

Personal data must be kept in a form which allows identification of data subjects for no longer than is necessary for the purposes for which such personal data are processed. The latter procedure must be followed by stakeholders.

Grit Group will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless an applicable law requires such data to be kept for a minimum time. Stakeholders must comply with Grit Group's Record Retention Policy. The latter procedure must be followed by stakeholders.

Data subjects are informed of the period for which data is stored and how that period is determined in our Privacy Policy.

9.6 Integrity and confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

Grit Group will develop, implement, and maintain safeguards appropriate to our company size, scope and business, our available resources, the amount of personal data that Grit Group owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). Grit Group will regularly evaluate and test the effectiveness of those safeguards to ensure security around how we process personal data.

All Stakeholders are responsible for protecting the personal data Grit Group holds. Grit Group must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Stakeholders must exercise particular care in protecting special category data from loss and unauthorised access, use or disclosure.

Stakeholders must follow all procedures and technologies which Grit Group puts in place to maintain the security of all personal data from the point of collection to the point of destruction. Grit Group will only transfer personal data to third-party service providers who agree to put adequate measures in place, as requested. Before transferring personal data to a third-party service provider, Stakeholders must consider any data protection implications associated with that transfer and liaise with the DPO to ensure that the transfer is permissible and appropriately documented.

Stakeholders must maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users can access the personal data when they need it for authorised purposes.

Stakeholders must comply with all aspects of any information security policies and must not attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain in accordance with our data protection obligations and relevant standards to protect personal data.

10.TRANSFER OF DATA

As part of our business activities, Grit Group commonly transfer personal data to third parties. The list of potential recipients of data is set out in the Grit Group Privacy Policy. If Stakeholders are transferring data to a third party which do not align with the Privacy Policy, the stakeholders must promptly inform the DPO.

10.1 Large transfers

Often, large amount of personal data is required to be transferred to third parties. In such circumstances, stakeholders must first discuss the proposed transfer with the DPO, who will set out necessary measures which are required prior to the transfer. This may include the below:

- Carry out an audit of the third parties' data protection policies and procedures.
- Put in place an agreement with the third party setting out the basis of their responsibilities.

10.2 *Appointment of processors*

If Grit Group appoints a third party to process data on its behalf, that third party is likely to be a processor. Any such arrangement must be appropriately documented by putting in place a written agreement with that third party. Such agreement must contain certain provisions and must be prepared in conjunction with the appropriate head of businesses and the DPO. The DPO will maintain oversight and responsibility for all such outsourcing arrangements.

10.3 International transfers

If any transfer of personal data to a third party will result in that personal data being processed internationally, Grit Group must ensure that we meet with the relevant requirements of the data protection legislation before any such transfers take place. Transfers can only be made where a lawful basis for processing has been determined and there

is adequate protection for the rights and freedoms of individuals in relation to the processing of information about them.

Grit Group has a duty to ensure the necessary obligations of the data protection legislation of the concerned jurisdiction are met. In other instances, Grit Group may rely on the fact that the data subject has consented to the transfer (i.e. where we have been asked to appoint an external lawyer or the transfer is necessary for the purposes of obtaining legal advice).

If Stakeholders are unsure about whether they should transfer any personal data or not, they must discuss this with the DPO or alternatively with the Head – Risk and Compliance.

10.4 Rights of Data Subjects

Data subjects have rights to:

- Receive certain information about our processing activities.
- Request access to their personal data that we hold.
- Request erasure of their personal data that we hold.
- Restrict processing under specific circumstances.
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest.
- Request a copy of an agreement under which personal data is transferred outside of their jurisdiction of residence.
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else.
- Be notified of a personal data breach which is likely to result in a high risk to their rights and freedoms.
- Make a complaint to the supervisory authority.
- Receive or ask for their personal data to be transferred to a third party.

Stakeholders must immediately forward any data subject request that they receive to the DPO.

10.5 *Data breaches*

If a personal data breach occurs, it must be notified to the applicable regulator(s) and, in certain instances, to the data subject.

Grit Group has put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where Grit Group is legally required to do so.

If Stakeholders know or suspect that a personal data breach has occurred, they should not attempt to investigate the matter but should immediately record and report the matter to the DPO.

Stakeholders should preserve all evidence relating to the potential personal data Breach.

10.6 *Training*

To manage the personal data processed by Grit Group and to ensure Grit Group is acting in accordance with obligations, all staff are required to undertake data protection training.

The Human Capital department will ensure that data protection training or overview is provided to all new staff within [10] working days, so far as practicable, of the commencement of their employment with Grit Group

Data protection refresher training will be provided to all existing staff annually.

Attendance at training is mandatory (whether that training is online or in person) unless the employee is told otherwise and attendance will be monitored, with status reports sent to compliance. Failure to undertake any mandatory training may result in disciplinary action.

11.SPECIFIC DUTY OF EMPLOYEES

Each member of the staff (the "Employee") has a duty to assist Grit in complying with its obligations under the applicable Data Protection legislations. Employees must ensure that whenever handling personal data, they are doing so in accordance with the applicable Data Protection legislations, and all applicable policies and procedures at Grit Group. All Businesses Units have the responsibility of ensuring that appropriate practices, processes, and controls are put in place to ensure compliance.

If any Employee is unsure about any aspects of this Policy or what actions he/she should take in relation to personal data, he/she should discuss this with his/her line manager and involve the DPO/Head – Risk and Compliance appropriately.

12. DISCIPLINARY OR OTHER CONSEQUENCES

All principles described in this Policy must be strictly followed. A breach of data protection guidelines by any employee, agent, nominee, trustee, préposé, director, shareholder and/or beneficial owner of the Company will result in disciplinary and possibly legal, regulatory, arbitral, or administrative action.

13. CONTACT DETAILS

If any Stakeholder has any comments, questions or concerns about any of the information in this Policy, or any issues relating to the processing of Data by the Company, please contact the Company's client service contact on: tina@grit.group or compliance@grit.group

14.UPDATING THIS POLICY

This policy will be reviewed annually or as and when any changes to it are required.

Glossary of terms

Consent: Means any freely given specific, informed, and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmation action, by which they signify their agreement to personal data relating to them being processed.

Controller: the person or organisation that determines when, why and how to process personal data. They are responsible for establishing practices and policies in line with data protection legislation. Means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision-making power with respect to the processing.

data protection legislation: all applicable laws and regulations relating to the processing of personal data including but not limited to the Mauritian Data Protection Act 2017 (the "DPA"), together with any successor legislation or regulations, the General Data Protection Regulation 2016/679 (GDPR), the Data Protection (Bailiwick of Guernsey) Law 2017 ("Guernsey DPL") and any statutory instrument, order, rule or regulation made thereunder, as from time to time amended, extended, re-enacted, or consolidated.

data subject: Means an identified or identifiable individual, by reference to an identifier such as a name, an identification number, a location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

DPO (Data Protection Officer): the person appointed with responsibility for data protection compliance.

personal data: Means any information relating to a data subject.

Pseudonymisation: Means the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

Personal Data Breach: any act or omission that compromise the security, confidentiality, integrity, or availability of personal data or the physical, technical, administrative, or organisational safeguards that Grit Group or its third-party service providers have put in place to protect it. The loss, unauthorised access or disclosure of personal data is a personal Data Breach.

process: any operation or set of operations performed on personal data such as collection, recording, storage, adaptation, alteration, retrieval, disclosure, dissemination, restriction, erasure, or destruction.

processor: Means a person who, or public body which, processes personal data on behalf of a controller.

special category data relates to particularly sensitive data including health data, biometric data, genetic data, data relating to racial or ethnic origins, political opinions, sex life, sexual orientation, religious beliefs, and information relating to criminal convictions or alleged criminal activity.

staff: all partners, employees, directors, consultants, contractors, and other persons engaged by Grit Group.