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

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 data protection legislations).

There is a glossary 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 all Grit entities in 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 our company and of any of its subsidiaries are required to follow this Policy (the "**Stakeholders**"). 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 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;

- Be familiar with the privacy notice – if a data subject or stakeholder thinks that Grit is processing data outside the terms of its privacy notice, he or she should alert the DPO;
- Consider at all times when processing personal data whether it is necessary to include all elements of the personal data, and limit the personal data processed where the data subject or stakeholder can;
- If a data subject or stakeholder identifies any instances where he or she need to process large scales of personal data, transfer it to another jurisdiction or the data is particularly sensitive, consult with the DPO;
- 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, alert the DPO

Related policies and procedures are available to help Stakeholders interpret and act in accordance with this Policy. Stakeholders must also comply with all such related policies and procedures.

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**") and the General Data Protection Regulation EU 2016/679 (as amended or replaced from time to time) (the "**GDPR**") ("**Applicable Data Protection Legislations**").

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 Group Compliance Manager.

Data Protection Officer

Grit has appointed a DPO with responsibility for overseeing this Policy and, as applicable, developing related policies and procedures. The DPO is responsible for:

- Keeping the board of directors or other relevant teams updated about data protection responsibilities, risks, and issues.

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.

- Arranging data protection training and advice for the people covered by this Policy.

- Handling data protection queries from those covered by this Policy.

- Dealing with requests from data subjects to exercise their rights under the data protection legislation.

- Checking and approving, where necessary, any contracts or agreements with third parties whereby personal data may be transferred.

The current DPO is the Group Compliance Manager, who can be reached at compliance@grit.group.

Please contact the DPO in relation to any questions about the operation of this Policy or the data protection legislation or if any Stakeholder has any concerns that this Policy is not being or has not been followed.

4. 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 its 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 its consent at any time.

5. 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, social security numbers, 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, which of their data is 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.

6. 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;
- Conclude agreements in relation to the processing of Data or include contract clauses or communicate statements on how we handle Data;
- Procure that each sub-processor of Data enters into a written agreement in terms of which such sub-processor 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 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 provisions will appear on our website.

7. DATA PROTECTION OBLIGATIONS

Controller and processor

Grit and its group of companies is/are data controllers. In some instances, Grit Group may also be acting as a processor. 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.

Data protection principles

The data protection legislation imposes obligations on those handling personal data and requires them to process that data in accordance with the data protection principles. 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).

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: 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 is mentioned in our privacy notice. If a data subject approaches anyone within the Grit Group to withdraw their consent to the processing of their personal data, he or she 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 and because consent cannot be given or has been unreasonably withheld.

The purposes for which we process personal data are explained in the Grit Group privacy notice. If any Stakeholder is concerned that the processing which he or she is undertaking is not adequately captured in the privacy notice, 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 notice explaining the purposes for our processing can be found here https://grit.group/google-privacy-policy/. The privacy notice also explains to data subjects how and why we will use, process, disclosure, protect and retain personal data.

Whenever we collect personal data directly from data subjects, we must provide the data subject with the privacy notice 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 a privacy notice. A Stakeholder acting for 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.

The privacy notice is publicly available on our website. Amended or alternative privacy notices should not be provided without the approval of the DPO. If there is a concern that an appropriate privacy notice has not been provided, any Stakeholder should raise this with his/her line manager (in the case of an employee) in the first instance or the DPO.

There are certain exceptions when a privacy notice is not required to be provided. If there are any queries, the DPO should be consulted.

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.

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. Accordingly, excessive data should not be collected and at all times Stakeholders shall ensure that any personal data collected is adequate and relevant for the intended purposes.

In particular, personal data processed should be limited to that necessary to fulfil the legitimate business purpose and should not exceed that. 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.

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 use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. 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.

Storage limitation

Personal data must not be kept in identifiable form for longer than is necessary for the purposes for which the data is processed.

Stakeholders must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

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 a law requires such data to be kept for a minimum time. Stakeholders must comply with Grit Group's Record Retention Policy.

Stakeholders will take all reasonable and necessary steps to destroy or erase from our systems all personal data that we no longer require in accordance with our applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

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

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 size, scope and business, our available resources, the amount of personal data that Grit Group own or maintain 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 of our processing of personal data.

All Stakeholders are responsible for protecting the personal data Grit Group hold. 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 are able to access the personal data when they need it for authorised purposes.

Stakeholders must comply with all aspects of any information security policies and 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.

Privacy by design

Grit Group will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy and data protection issues, including the completion of one or more Data Protection Impact Assessments ("DPIA"). If you are commencing a new project or involved in changes to existing systems or arrangements, you (and your business area head) must engage with the DPO at an early stage to ensure and appropriate DPIA is undertaken.

8. TRANSFERS 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 notice. If Stakeholders are transferring to a third party which Stakeholders do not consider is covered by the privacy notice, Stakeholders must raise the matter with the DPO immediately.

Large transfers

In certain circumstances, we will need to transfer large amounts of personal data to a third party. Stakeholders must not do this without having first discussed the proposed transfer with the DPO, who will determine the necessary measures required prior to the transfer which may include:

- Conducting a DPIA.
- Carrying out an audit of the third parties' data protection policies and procedures.
- Putting in place an agreement with the third part setting out the basis of their instructions and responsibilities.

Appointment of processors

In the event that 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 business head and the DPO. The DPO will maintain oversight and responsibility for all such outsourcing arrangements.

International transfers

In the event that any transfer of personal data to a third party will result in that personal data being processed outside of the European Union or internationally, Grit Group must ensure that we meet with the relevant requirements of the data protection legislation before any transfer takes 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.

Where the transfer is to a jurisdiction in the European Economic Area ("EEA") (or a jurisdiction deemed adequate by the European Commission (see below)) the recipient may be subject to the same data protection standard adopted across Grit Group. Where the recipient is outside the EEA, Grit Group has an obligation to ensure the necessary obligations of the data protection legislation are met. Where Stakeholders are making the decision to transfer personal data this will include ensuring that the third parties to whom we are transferring personal data and who are located outside the EEA (and not otherwise an adequate jurisdiction) have in place policies and procedures in relation to the obtaining, processing, and storing of personal data which are at least equivalent to the standards under GDPR and that there is a contract in place confirming that. 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 or not they should transfer any personal data, they must discuss this with the DPO or the Group Compliance Manager as appropriate.

Adequate

Some jurisdictions may be designated as "adequate" by the European Commission such that personal data may be transferred to those jurisdictions with no or limited restrictions.

Where data is required to be held by a third party outside of an adequate jurisdiction [the DPO must be informed prior to processing any data or signing any agreements].

Data subject rights

Data subjects have rights to:

- Receive certain information about our processing activities;
- Request access to their personal data that we hold;
- Ask us to erase personal data if it is no longer necessary in relation to the purposes of which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- Restrict processing in 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 the EEA;
- 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.

Data breaches

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

Training

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

The Group HR department will ensure that data protection training or overview is provided to all new staff within [10] working days of the commencement of their relationship with us, so far as practicable.
Data protection training will be provided to all existing staff on an annual basis. Additional data protection training will be provided to any relevant staff when it is deemed appropriate to do so.

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.

9. 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. All business areas 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/Group Compliance Manager where appropriate.

10. 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.

11. 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: compliance@grit.group

Glossary of terms

consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or clear positive action, signify agreement to the Processing of personal data relating to them.

controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with data protection legislation.

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: a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

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

explicit consent: consent which requires a very clear and specific statement, not just action.

personal data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special category data and pseudonymised personal data but excludes anonymous data or data that has the identity of an individual permanently removed. Personal data can be factual (for example, name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

personal data Breach: any act or omission that compromise the security, confidentiality, integrity, or availability of personal data or the physical, technical, administrative or organisation safeguards that we or our third-party service providers put in place to protect it. The loss, or 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: a person or organisation responsible for processing personal data on behalf of a controller.

special category data: relates to particularly sensitive data including heath 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.