PRIVACY POLICY AND COLLECTION STATEMENT
Griffin Projects Group Pty Ltd (ABN 39 151 840 041)

('*Privacy Policy*')

1. Introduction

Griffin Projects Group Pty Ltd (ABN 39 151 840 041) (referred to as **'Griffin'**, ***'we'***, ***'our'***, ***'us'***) is a Corporate Authorised Representative (CAR No. 001255188) of SMATS Consortium Pty Ltd (ABN 30 603 784 452) who holds an Australian Financial Services Licence (No. 480476).

Griffin is bound by the *Privacy Act 1988* (**Privacy Act**), including the Australian Privacy Principles (**APPs**), and recognises the importance of ensuring the confidentiality and security of your personal information. A copy of the APPs may be obtained from the website of the Office of the Australian Information Commissioner at https://www.oaic.gov.au/.

To the extent that it is necessary to do so, Griffin also complies with the requirements of the EU General Data Protection Regulation (**GDPR***)* as adopted by EU Member States. The APPs and the GDPR share many common requirements. Where an obligation imposed by the APPs and the GDPR are the same, but the terminology is different, Griffin will comply with the terminology and wording used in the APPs, and this will constitute Griffin's compliance with the equivalent obligations in the GDPR.

If the GDPR imposes an obligation on Griffin that is not imposed by the APPs, or the GDPR obligation is more onerous than the equivalent obligation in the APPs, Griffin will use reasonable endeavours to comply with the GDPR, if required.

We use reasonable endeavours to make all third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by Griffin, aware of this Privacy Policy and Collection Statement (**Privacy Policy).**

Griffin makes this Privacy Policy available free of charge and can be downloaded from its website at https://griffin-group.com.au/privacy-policy/.

In this Privacy Policy:

- ***Disclosure*** of information means providing information to persons outside of Griffin;
- ***Personal information*** means information or an opinion relating to an individual, which can be used to identify that individual;
- ***Privacy Officer*** means the contact person within Griffin for questions or complaints regarding Griffin's handling of personal information;
- ***Sensitive information*** is personal information that includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences and criminal record, and also includes health information; and
- ***Use*** of information means use of information within Griffin.

2. What kind of personal information do we collect and hold?

We may collect and hold a range of personal information about you to provide you with our services, including:

- name;
- address;
- phone numbers;
- email addresses;
- occupation;

- bank account details;
- driver's licence and or passport details (photographic identification);
- financial information, including details of:
    - assets, liabilities, income and expenses;
    - credit reference information including credit card/banking details;
    - personal, company and trust Tax File Numbers (TFNs);
    - your investments;
    - your insurance policies;
    - superannuation (incl. SMSFs) and pension funds;
    - estate planning strategies;
    - taxation information; and
    - health information.

3. How do we collect personal information?

We generally collect personal information directly from you. For example, personal information will be collected through our application processes, forms and other interactions with you in the course of providing you with our products and services, including when you visit our website, use a mobile app from us, call us or send us correspondence.

We may also collect personal information about you from a third party, such as electronic verification services, referrers and marketing agencies. If so, we will take reasonable steps to ensure that you are made aware of this Privacy Policy. We may also use third parties to analyse traffic at our website, which may involve the use of cookies. Information collected through such analysis is anonymous.

We will not collect sensitive information about you without your consent, unless an exemption in the APPs applies. These exceptions include if the collection is required or authorised by law, or necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct.

If the personal information we request is not provided by you, we may not be able to provide you with the benefit of our services, or meet your needs appropriately.

We do not give you the option of dealing with us anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, not permissible for Griffin to deal with individuals who are not identified.

We may also collect statistical information about visitors to our website using web analytics and session recording technology provided by third party service providers such as Google Analytics. These services use Cookies to assist us in understanding how visitors access and utilise our site. Generally, this information cannot be used to identify particular individuals. However, in some circumstances it may include a visitor's internet protocol (IP) address, which could be linked to an individual.

You can find out more information on how the below third parties use data:

- How Google uses data when you use Standards Australia's sites or apps at https://www.google.com/policies/privacy/partners/;
- How Cookiebot, our Cookie app in the form of a pop up message required for GPDR compliance, uses data at https://www.cookiebot.com/en/privacy-policy/; and
- How CompleteEmpire, our Business Management Software, uses data at https://www.empiresoftware.com.au/Privacy-Policy/.

4. Unsolicited personal information

We may receive unsolicited personal information about you. We destroy or de-identify all unsolicited personal information we receive, unless it is relevant to our purposes for collecting personal information. We may retain additional information we receive about you if it is combined with other information we are required or entitled to collect. If we do this, we will retain the information in the same way we hold your other personal information.

5. Who do we collect personal information about?

The personal information we may collect and hold includes (but is not limited to) personal information about:

- clients;
- potential clients;
- service providers or suppliers;
- prospective employees, employees and contractors; and
- third parties with whom we come into contact.

6. Website collection

We collect personal information when we receive completed online generated forms from our website.

We may also use third parties to analyse traffic on our website, which may involve the use of cookies.

To use our website, you consent to our use of cookies. You can withdraw or modify your consent to our use of cookies at any time. If you no longer wish to receive cookies, you can use your web browser settings to accept, refuse and delete cookies. To do this, follow the instructions provided by your browser.

Please note that if you disable cookies in your browsers, our website may not operate optimally, or at all.

Cookies are small text files that are transferred to a computer's hard disk through your web browser for record keeping purposes. Cookies do not contain personal information.

We will endeavour to delete all data obtained through cookies every few months. We may also use analytics on the site. We do not pass any personally identifiable information through this function, however, the data we collect may be combined with other information which may be identifiable to you.

7. Why do we collect and hold personal information?

We may use and disclose the information we collect about you for the following purposes:

- provide you with our products and services;
- review and meet your ongoing needs;
- provide you with information we believe may be relevant or of interest to you;
- let you know about other products or services we offer, respond to your queries, feedback, surveys, send you information about special offers or invite you to events;
- consider any concerns or complaints you may have;
- comply with relevant laws, regulations and other legal obligations;
- help us improve the products and services offered to our customers and enhance our overall business;
- to provide you with investment information, distribution information and tax information;
- to conduct business processing internally or with third parties, suppliers, contractors and service providers;
- analyse and improve aspects of our business, including development processes, business systems, outcomes, communication, website engagement and performance;
- to access the performance of the website and improve the website operation;
- for administrative, marketing, planning, product & service development, quality control, survey and research purposes, and employees;
- to update records and keep your contact details up to date; and

- to comply with any law (for example the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)), rule, regulation, lawful and binding determination, decision, direction, or a regulator, or in co-operation with any government authority of any country (or political sub-division of a country).

We may use and disclose your personal information for any of these purposes. We may also use and disclose your personal information for secondary purposes which are related to the primary purposes set out above, or in other circumstances authorised by the Privacy Act.

Sensitive information will be used and disclosed only for the purpose for which it was provided (or a directly related secondary purpose), unless you agree otherwise, or an exemption in the Privacy Act applies.

8. Who might we disclose personal information to?

We may disclose personal information to:

- a related entity of Griffin;
- SMATS Consortium Pty Ltd (ABN 30 603 784 452) as licensee (AFSL No. 480476) or a related entity of SMATS Consortium Pty Ltd;
- an agent, contractor or service provider we engage to carry out our functions and activities, such as our lawyers, accountants, debt collectors or other advisers;
- organisations involved in a transfer or sale of all or part of our assets or business;
- organisations involved in managing payments, including payment merchants and other financial institutions, such as banks;
- regulatory bodies, government agencies (in any country), law enforcement bodies and courts;
- financial product issuers (such as SMATS Consortium Pty Ltd);
- property professionals, ID verification providers, web hosting providers, cloud or web-based storage ;
- providers, IT systems, administrators, mailing houses, couriers, payment processors, data entry service providers, electronic network administrators, debt collectors, government related bodies and agencies in any country (or political sub-division of a country); and
- anyone else to whom you authorise us to disclose it or is required by law.

If we disclose your personal information to service providers that perform business activities for us, they may only use your personal information for the specific purpose for which we supply it. We will ensure that all contractual arrangements with third parties adequately address privacy issues, and we will make third parties aware of this Privacy Policy.

9. Sending information overseas

We may disclose personal information to related entities (such as SMATS Consortium Pty Ltd), data hosting and cloud computing providers, IT service providers that are located outside Australia in some circumstances. These recipients may be located in the following countries:

- Singapore;
- UAE;
- Hong Kong;
- United Kingdom; and
- United States of America.

We will not send personal information to recipients outside of Australia unless:

- we have taken reasonable steps to ensure that the recipient does not breach the Act and the APPs,
- the recipient is subject to an information privacy scheme similar to the Privacy Act; or
- the individual has consented to the disclosure.

If you consent to your personal information being disclosed to an overseas recipient, and the recipient breaches the APPs, we will not be accountable for that breach under the Privacy Act, and you will not be able to seek redress under the Privacy Act.

10. Management of personal information

We recognise the importance of securing the personal information of our customers. We will take steps to ensure your personal information is protected from misuse, interference or loss, and unauthorised access, modification or disclosure.

Your personal information is generally stored in our computer database including in the 'cloud' or by our third-party service providers (including but not limited to MailChimp and Microsoft Officer 365). Any paper files are stored in secure areas. In relation to information that is held on our computer database, we apply the following guidelines:

- passwords are required to access the system, and passwords are routinely checked;
- data ownership is clearly defined;
- we change employees' access capabilities when they are assigned to a new position;
- employees have restricted access to certain sections of the system;
- the system automatically logs and reviews all unauthorised access attempts;
- unauthorised employees are barred from updating and editing personal information;
- all computers which contain personal information are secured both physically and electronically;
- data is encrypted during transmission over the network; and
- print reporting of data containing personal information is limited.

Where our employees work remotely or from home, we implement the following additional security measures:

- two-factor authentication is enabled for all remote working arrangements;
- password complexity is enforced, and employees are required to change their password at regular intervals;
- employees only have access to personal information which is directly relevant to their duties;
- we use audit trails and audit logs to track access to an individual's personal information by an employee;
- we monitor access to personal information, and will investigate and take appropriate action if any instances of unauthorised access by employees are detected;
- employees must ensure that screens are angled so that they cannot be used by anyone else, and are locked when not in use;
- employees must ensure that no other member of their household uses their work device;
- employees must store devices in a safe location when not in use;
- employees may not make hard copies of documents containing personal information, nor may they email documents containing personal information to their personal email accounts; and
- employees may not disclose an individual's personal information to colleagues or third parties via personal chat groups.

11. Direct marketing

We may only use personal information we collect from you for the purposes of direct marketing without your consent if:

- the personal information does not include sensitive information; and
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing; and
- we provide a simple way of opting out of direct marketing; and
- you have not requested to opt out of receiving direct marketing from us.

If we collect personal information about you from a third party, we will only use that information for the purposes of direct marketing if you have consented (or it is impracticable to obtain your consent), and we will provide a simple means by which you can easily request not to receive direct marketing communications from us. We will draw your attention to the fact you may make such a request in our direct marketing communications.

You have the right to request us not to use or disclose your personal information for the purposes of direct marketing, or for the purposes of facilitating direct marketing by other organisations. We must give effect to the request within a reasonable period of time. You may also request that we provide you with the source of their information. If such a request is made, we must notify you of the source of the information free of charge within a reasonable period of time. You may submit a request to the Privacy Officer in writing to info@griffin-group.com.au.

12. Identifiers

We do not adopt identifiers assigned by the Government (such as drivers' licence numbers) for our own file recording purposes, unless one of the exemptions in the Privacy Act applies.

13. How do we keep personal information accurate and up-to-date?

We are committed to ensuring that the personal information we collect, use and disclose is relevant, accurate, complete and up-to-date.

We encourage you to contact us to update any personal information we hold about you. If we correct information that has previously been disclosed to another entity, we will notify the other entity within a reasonable period of the correction. Where we are satisfied information is inaccurate, we will take reasonable steps to correct the information within 30 days, unless you agree otherwise. We do not charge you for correcting the information.

14. Accessing your personal information

Subject to the exceptions set out in the Privacy Act, you may gain access to the personal information that we hold about you by contacting the Griffin's Privacy Officer. We will provide access within 30 days of the individual's request. If we refuse to provide the information, we will provide reasons for the refusal.

We will require identity verification and specification of what information is required. An administrative fee for search and photocopying costs may be charged for providing access.

15. Updates to this Privacy Policy

This Privacy Policy will be reviewed from time to time to take account of new laws and technology, and changes to our operations and the business environment. We reserve the right to change our Privacy Policy at any time by posting an updated version on our website.

16. Responsibilities

It is the responsibility of management to inform employees and other relevant third parties about this Privacy Policy. Management must ensure that employees and other relevant third parties are advised of any changes to this Privacy Policy. All new employees are to be provided with timely and appropriate access to this Privacy Policy, and all employees are provided with training in relation to appropriate handling of personal information. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

17. Non-compliance and disciplinary actions

Privacy breaches must be reported to management by employees and relevant third parties. Ignorance of this Privacy Policy will not be an acceptable excuse for non-compliance. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

18. Incidents/Complaints handling/Making a complaint

We have an effective complaint-handling process in place to manage privacy risks and issues. We also have an internal "Complaints Handling Policy" that outlines procedures and processes that are in place to ensure that Griffin (and our Representatives) have adequate dispute resolution procedures for its clients.

The complaints handling process involves:

- identifying (and addressing) any systemic/ongoing compliance problems;
- increasing consumer confidence in our privacy procedures; and
- helping to build and preserve our reputation and business.

You can make a complaint to us about the treatment or handling of your personal information by lodging a complaint with the Privacy Officer.

If you have any questions about this Privacy Policy, or wish to make a complaint about how we have handled your personal information, you can lodge a complaint with us by:

- writing – to Griffin Projects Group Pty Ltd at Unit G2, 204 Walcott Street MENORA WA 6050; or
- emailing – info@griffin-group.com.au.

If you are not satisfied with our response to your complaint, you can also refer your complaint to the Office of the Australian Information Commissioner by:

- telephoning – 1300 363 992;
- writing – Director of Complaints, Office of the Australian Information Commissioner, GPO Box 5288, SYDNEY NSW 2001;
- online submission – https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacycomplaint-with-us; or
- Fax – +61 2 6123 5145.

You may unsubscribe from our mailing/marketing lists at any time by contacting us in writing.

19. Contractual arrangements with third parties

We endeavour to ensure that all contractual arrangements with third parties adequately address privacy issues, and we inform third parties of our obligations under our Privacy Policy.

Third parties will be required to implement policies in relation to the management of your personal information in accordance with the Privacy Act. These policies include:

- regulating the collection, use and disclosure of personal and sensitive information;
- de-identifying personal and sensitive information wherever possible;
- ensuring that personal and sensitive information is kept securely, with access to it only by authorised employees or agents of the third parties; and
- ensuring that the personal and sensitive information is only disclosed to organisations which are approved by us.

20. Your rights

This Privacy Policy contains information about how:

- you may access the personal information we hold about you;
- you may seek the correction of your personal information;
- you may ask us to provide an alternative means of identity verification for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)*;*
- you may complain about a breach of the Privacy Act, including the APPs; and
- we will deal with a privacy complaint.