Privacy Policy

This policy sets out how **WMF Consulting Pte Ltd** ('WMF Consulting') UEN 202119531Z collects, uses, discloses, retains and manages your personal information and the personal information for Clients it works for and how we comply with our obligations under the Privacy Act 1988 (Cth) (Privacy Act).

WMF Consulting does not provide financial or credit services in its own right but instead is a consultancy company assisting global businesses with operational advice and support, with a focus on Australian-based financial services businesses. This Privacy Policy is specific to our Australian-based clients.
Therefore, the information we collect is done on behalf of each respective Australian financial services business that is a client of WMF Consulting. WMF Consulting is an offshore company registered in Singapore and although services are provided by virtual team members in various locations, we adhere to Australian Privacy Principles in the Privacy Act 1988. If we operate under and existing Personal Data Protection Policy or establish one in the future, this Australian-specific Privacy Policy applies to you if your personal information (within the meaning defined in this Addendum) is collected, used, held or disclosed by us in Australia and is governed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (Privacy Laws). Where there is an inconsistency between the terms of the Personal Data Protection Policy and the terms of this Australia Addendum, the terms of this Australia Addendum override the Personal Data Protection Policy.

Unless you advise us otherwise, you acknowledge and consent to us using your personal information as set out in this Privacy Policy or as otherwise permitted under the Privacy Act or other law.

1. What personal information do we collect?

A. When we are contacted or we provide our services, the personal information we collect may include a person's name, contact numbers, email address, residential or business address, financial details, insurance details, credit card details and other personal data. This may include sensitive information (as that term is used in the Privacy Act).

B. When our server/cloud storage is accessed, it automatically records information the browser sends when it connects to our website. This information may include:

• The accessing party's Internet Protocol (IP) address, domain name, browser type and language
• Information about usage and online activities (for example, by way of cookies) including when our website is accessed, other sites accessed from our website, content upload and download and usage of the services available on our website
• Information provided through use of any downloading facilities on our website.

C. Our website uses cookies. Cookies do not identify you personally, but they may link back to a database record about you. With most Internet browsers you can erase or block cookies or receive a warning before a cookie is stored. Refer to your Internet browser instructions for guidance on this.

2. How do we collect the personal information?

A. We collect personal information:

• From the individual
• From you, our clients when we provide services to them. This includes personal information about your customers and clients (Your Clients)
• Via a file-sharing arrangement with a client and when a client provides access to their customer relationship management (CRM) and software systems and third party websites to enable us to provide the services;
• When sent to us by email or other communication from third parties
• From publicly available sources of information
• When we are required to do so by law
• From our own records

B. We are committed to ensuring the information we have is accurate and up to date. We update personal information when we are advised there has been a change and at other times as necessary.

3. Provision of personal information to us by you and Your Clients

If you provide us with the personal information of another person (including Your Clients):

A. You must disclose to that person that you are providing personal information (including sensitive information) to us and that the information may be disclosed offshore

B. You represent and we accept it on the basis that you represent that Client and authorised to do so and that the relevant person has consented to the disclosure to us

4. How we use your personal information?

A. Generally, we will collect, use and hold personal information to:

• Provide our services, including services involving Your Clients
• Facilitate our internal business operations, including the fulfilment of any legal requirements
• Advise you of additional services or information which may be of interest
• Provide your contact details to our partners who have agreed to provide you with any services
• Analyze our services and customer needs with a view to developing and improving existing and new products and services
• Maintain and update our business infrastructure and systems;
• Compile statistical data
• Promote and advertise our business, products and services.

B. If we do not collect the personal information we will not be able to provide the services or provide any assistance requested.

C. If the personal information provided to us is incomplete or inaccurate, we may be unable to provide our services or our services may be adversely affected.

5. Disclosing your information

We can disclose personal information we have about you to third parties in certain circumstances including:

• If you or Your Client agree to the disclosure;

• To employees, contractors and service providers, who assist us in operating our business and providing our services and those service providers of yours that you require us to work with;
• If you or Your Client would reasonably be expected to consent to information of that kind being passed to a third party;
• Using it for the purposes we collected for which it was (e.g. to provide our services or respond to a query);
• Where disclosure is required or permitted by law;
• To our related entities;
• If disclosure will prevent or lessen a serious and imminent threat to someone's life or health; or
• Where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of public revenue.

6. Disclosure of personal information off-shore

A. We provide services to you and Your Clients under our Client Services Agreement. These services are performed by our Singapore based company, WMF Consulting Pte Ltd. We may disclose your information overseas, including countries where WMF Consulting has operations (such as Singapore, The Philippines and Thailand), or countries where WMF Consulting has investments or receives outsourced services. If we do this, we make sure there are arrangements commensurate to the Australian privacy laws in place to protect your information. If you have provided your consent to us disclosing your personal information to overseas recipients without complying with APP 8.1, to the extent allowed by the APP, we may disclose your information to overseas recipients without taking reasonable steps to ensure the overseas recipient does not breach the APPs

B. Services include (but is not limited to):

• All services outlined in your Service Agreement

C. To provide our services we, WMF Consulting, receive personal information from you about Your Clients. This may include sensitive information.

D. We have security processes in place for the protection of that personal information, including supervising staff, specialist security software, disabling USBs, staff training, use of password protection, employee investigation software.

E. WMF Consulting will do all things necessary to ensure that as recipient of personal information, is subject to and complies with its obligations under the Privacy Act and Australian Privacy Principles, which include in particular, Australian Privacy Principle 8 – cross-border disclosure of personal information.

7. Considerations when you send information to us

A. While we do all we can to protect your privacy and the privacy of Your Clients, including investing in specialist security software, no data transfer over the Internet is 100% secure.

B. If you or Your Clients provide personal information to us electronically, there are ways you and Your Clients can help maintain the security of the information. These include:

• Always close your browser when you have finished your user session
• Do not provide personal information by using a public computer
• Never disclosing your user name and password to another person
• Not sending information to a WMF Consulting employee's email or other web-based mail account, or any other means of transferring client information other than through file sharing applications (e.g. Dropbox, Google Drive) specifically provided and approved by WMF Consulting

C. You are responsible for all actions taken using your username, email or password. If at any time you believe your username or password have been compromised, change your password and contact us immediately.

D. If we suspect that there is a data breach leading to the protection of personal information stored or held by us being compromised, we will implement a data breach response plan, which will include:

• Notifying you and Your Clients that may be affected by such a breach

• If necessary, notifying the relevant regulatory authorities of a suspected breach, which may include the Office of the Australian Information Commissioner (OAIC) and the Australian Federal Police.

• Undertaking appropriate remedial action, depending on the type, amount and nature of the personal information that is at risk. In the implementation and carrying out of the data breach response plan, we will refer to the OAIC's Data breach notification: a guide to handling personal information security breaches publication. Our Privacy Officer will be primarily responsible for developing and implementing such response plan and may require the assistance of WMF Consulting staff, its agents and external assistance in doing so, depending on the nature, extent and impact of the suspected breach.

8. How your information is stored

A. We take reasonable steps to securely store personal details and information. This includes electronic and physical security measures.

B. When the personal information that we collect is no longer required, we destroy or delete it in a secure manner.

9. How you can update, correct, or delete your personal information

A. You and Your Clients have a right to request access to personal information which we hold about you and Your Clients and to ask us to correct it if you believe it is inaccurate or out of date.

B. You and Your Clients may request the source of any information we collect from a third party. We will provide this at no cost, unless under the Privacy Act or other law there is a reason for this information being withheld.

C. You or Your Clients may request access to your personal information or correct any inaccurate or out of date information by contacting our Privacy Officer at privacy@wmfconsulting.online

D. If there is a reason under the Privacy Act or other law for us not to provide you or Your Clients with information, we will give you or Your Clients a written notice of refusal setting out

• The reasons for the refusal except to the extent it would be unreasonable to do so
• The mechanisms available to you to complain about the refusal

E. You or Your Clients should also contact us immediately if:

• Someone has gained access to you or Your Client's personal information
• We have breached our privacy obligations or your or Your Client's privacy rights in any way
• You or Your Clients would like to discuss any issues about our privacy policy.

10. Your authority and opting out

A. By using our services and providing us with personal information, you consent to us maintaining, using and disclosing your personal information in the way described in this Privacy Policy.

B. We do not use personal information of Your Clients for marketing purposes.

C. If at any time you no longer wish to receive any additional marketing material from us or do not want your information disclosed for direct marketing purposes, email info@wmfconsulting.online and we will remove your details from our marketing database.

D. If you close your account or opt out, we will remove or de-identify personal information as soon as reasonably possible. We may, however, retain personal information for as long as is necessary to comply with any applicable law, for the prevention of fraud, for insurance and governance purposes, in our IT back-up, for the collection of any monies owed and to resolve disputes.

11. Limitation of liability

A. To the extent permissible by law and subject to our obligations under the Privacy Act, we will not be liable to you or to any third party for any loss or damage (including but not limited to consequential loss or loss of profits) or claim arising from our collection, disclosure, management and use of personal information in accordance with this policy.

B. Where liability is not able to be excluded by law, to the extent allowed by law and without limiting your rights under Australian Consumer Law, our liability to you in any circumstances will be limited to re-performance of any services we have provided to you.

C. Links on our website or websites we set up for you may take you outside our network. These links are provided in good faith. However, we are not responsible for third party sites and accept no responsibility for the content, accuracy, security or function of third party sites.

12. Changes to our Privacy Policy and Complaints Handling Procedure

A. This document sets out our current Privacy Policy.

B. Our Privacy Policy will be updated from time to time. You should review our Privacy Policy each time you visit our website or provide us with personal information.

C. If you would like further information on our Privacy Policy or if you have any concerns or complaints over the protection of or the handling of the information you have given to us or that we have collected from others or if you believe that we have not dealt with your personal information in accordance with an Australian Privacy Principle, please contact our Privacy Officer by email at privacy@wmfconsulting.online. We endeavour to ensure that any complaints about privacy breaches will be dealt with quickly, seriously and confidentially. To help us investigate your complaint quickly and efficiently we will ask you or Your Client(s):

• Put your complaint in writing
• Provide us with your name and contact details, the nature of the complaint, any information that may assist with the complaint, any copies of any documentation which supports your complaint and the outcome(s) that you seek.

D. Our Privacy Officer is able to:

• Acknowledge receipt of and read your complaint;
• investigate your complaint, having regard to the information you have provided us and any other information which may be available, that could
• assist us in investigating your complaint, including requesting further information from you;
• notify you of our findings and any actions we may have taken or propose to take in regards to your complaint;

• if possible, discuss options to resolve the problem or dispute arising; and
• provide you with information on how to make a complaint to the OAIC if you are unhappy with the outcome of the investigation.

13. Privacy Officer

WMF CONSULTING has nominated a Privacy Officer to handle any queries or issues related to Privacy. This person has been nominated at a senior level and has access to the Board.

Name: Luke Mellar
Phone: +61 480 009 812
Email: privacy@wmfconsulting.online
Post: 5001 Beach Road, #04-03 GOLDEN MILE COMPLEX SINGAPORE 199588

We take our client's privacy seriously and will address your concerns through our complaints handling the process. All complaints will be given fair consideration and will aim to be resolved within 45 days. We encourage you to submit your complaint to the Privacy Officer (details above) either via email to post. Where it is found that we are unable to finalise the investigation of your complaint within 45 days, we will contact you to request an extension.

If you believe you did not receive a satisfactory resolution to your concern, you may contact the Office of the Australian Information Commissioner. You are able to do so by:

Visiting http://www.oaic.gov.au and submitting an online form;
Obtaining a hard copy form at http://www.oaic.gov.au/about-us/contact-us;
Phone: 1300 363 992;
Fax: 02 9284 9666;
Email: enquiries@oaic.gov.au