
The
Signal
Group

PRIVACY POLICY

WHEN DOES THIS POLICY APPLY?

This policy sets out the principles that Mulpha Signal Group Pty Limited and its subsidiaries (**Mulpha/we/us/our**) adopt in the conduct of our business in order to protect your personal information. A number of our subsidiaries engage in activities under other brands.

Mulpha is committed to providing you with exceptional service, and this includes protecting your privacy and being open and transparent about what we do with your personal information. In abiding with the Australian Privacy Principles and the *Privacy Act 1988 (Cth)*, we take steps to ensure information about you, is not disclosed to or accessed by unauthorised persons.

THIS POLICY

This privacy policy explains when and why we collect personal information, how we use it, and how and to whom we disclose that information and we maintain the quality and security of your personal information. It also provides details about how you may access and seek correction of the personal information that we hold about you, and what you can do if you are not satisfied with how we have dealt with your personal information.

WHAT TYPES OF PERSONAL INFORMATION DO WE COLLECT?

Personal information means any information about an individual from which that person can be reasonably identified. It does not include data where your identity has been removed or which is not associated with or linked to your personal information (anonymous data).

What personal information we obtain on you depends on the reason it is being collected, but may include your:

- Name
- Address
- Email address
- Telephone number
- CCTV image
- Photograph
- Video footage
- Internet Protocol (IP) address (when you visit our website)
- Card details (when making a payment to us)
- Financial details including sort code, bank account number and name on account (if you are providing services to us)
- Cookies (when you visit our website)
- Activity on our website, including the pages you visited, documents downloaded, and searches made, including whether you have accessed third party sites
- Correspondence with us
- WIFI at our centres
- Government identifiers (TFN)
- Nationality
- Country of birth
- Professional memberships
- Employee salary and due diligence data
- Police Checks to satisfy human resources requirements

As part of our recruitment processes for employees and contractors the personal information we obtain depends on the role and requirements but may include:

- Name
- Addresses
- Dates of birth
- Financial information
- Citizenship
- Employment references
- Regulatory accreditation and professional memberships
- Directorships
- Property ownership
- Identification documents.
- Government identifiers (such as TFN)
- Nationality
- Country of birth
- Family court orders
- Police Checks to satisfy human resources requirements.

Generally, we will seek consent from you in writing before we collect your sensitive information.

We only collect personal information about you that is necessary for us to carry on our business functions. The information we collect about you depends upon the nature of our dealings with you. Generally, we only collect personal information from you, unless it is not reasonable or practical to do so in which case, we may also collect personal information about you from third parties.

HOW DO WE COLLECT PERSONAL INFORMATION FROM YOU?

We may collect personal information which you give us, or that we collect independently, in one of the following ways:

- When you communicate with us by email or phone.
- When you make an enquiry about our properties, products or services, or visit our properties.
- When you access and interact with our website.
- When you access our WIFI.
- When you make a reservation with us or have an event with us.
- When you visit one of our events as a ticket holder or exhibitor.
- When an application is made by you or on your behalf to attend one of our events or take part in one of our activities
- When you have asked to receive information from us (such as event updates and mailing lists)
- When you enter a competition with us
- When you complete surveys that we use for research purposes, although you do not have to respond to them when we send them to you
- When you become a member of one of our clubs or provide your details for our mailing lists.
- When you purchase our services or products online.
- When you propose to provide or provide goods or services to us or our customers.
- When you receive goods or services from us or agree to receive goods or services from us.
- When you make an application to invest with us.
- When you make an application for finance from us.
- When you or another individual is injured during your interaction with us
- When you or another individual makes a complaint or where there has been a threat or damage to personal property.

We may collect information based on how you use our website. We use ''cookies'' and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website. This information is collected to analyse and improve our website, marketing campaigns and to record statistics on web traffic.

If you access your account with us online through a secure area of our website, we will collect your personal information using cookies. This is designed to track the use of our website and to allow our customers to effectively access their account information. This information is collected for security purposes and to protect the integrity of account details.

INFORMATION WE COLLECT FROM OTHERS

We collect personal information about you from third parties such as:

- Our service providers. For example, when you make an enquiry about our properties, products or services to our service provider who assists us in providing our products or services to you.
- Booking agents. For example, when you enquire or make a reservation through a third-party booking agent to dine or stay with us, or have an event with us.
- Other goods or service providers, and our clients. For example, when you provide a trade or finance reference as part of entering into an agreement with us and you have agreed for your personal information to be shared with us.
- Your financial advisor, accountant, agent, or third-party intermediaries and you have agreed for your personal information to be shared with us.
- Someone that is appointed as your personal representative, attorney or legal representative.
- Third parties to whom you have provided your personal information and consented for that information to be shared with us.

SENSITIVE INFORMATION

We only collect sensitive information if it is:

- Required by applicable laws or rules.
- Reasonably necessary for one or more of our business functions or activities, and we have your consent.
- Necessary to lessen or prevent a serious threat to life, health or safety.

USING YOUR INFORMATION

We only use your personal information for:

- The reasons we collected it, that is where it is reasonably necessary for one or more of our business functions or activities (the primary purpose).
- A related secondary purpose that would be reasonably expected by you.
- The purposes set out in this policy.
- An activity or purpose to which you have consented.

We use your personal information so we can, amongst others:

- Establish and verify your identity.
- Provide, manage and administer the provision of our goods and services to you.
- Process a payment, including credit card payment.
- Assess your application for any financial product or finance (including where you have consented to act as a guarantor).
- Contact you and manage our relationship with you.
- Identify and tell you about other products or services that we think may be of interest to you (unless you tell us not).
- Conduct, manage and improve our business and our customers experience.
- Design, price and administer our products and services.
- Manage our risks and identify and investigate illegal activity, such as fraud, bribery or corruption; and
- Comply with our legal obligations such as under the such as under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act and AML/CTF Rules) and assist government and law enforcement agencies or regulators.

We may also collect, use and exchange your information in other ways where permitted by law.

DIRECT MARKETING

If you don't want to receive direct marketing, you can tell us by emailing us and telling us which list you would like to be removed from at **marketing@mulpha.com.au** or write to us at Level 9, 117 Macquarie Street Sydney, NSW 2000 Australia.

USING GOVERNMENT IDENTIFIERS

If we collect government identifiers, such as your tax file number, we do not use or disclose this information other than required by law. We will never use a government identifier in order to identify you.

EXCHANGING YOUR INFORMATION

We may exchange (ie, collect from and disclose to) your personal information with the following parties for the following purposes:

- Any of our associates, related entities or contractors.
- Agents and persons who assist us to provide our products or services to you.
- Our product and service providers who provide or assist us to provide, manage or administer our properties, products or services on our behalf.
- Consultants and contractors and their sub-contractors who provide services to us.
- Our representatives, associates, joint venture partners, partners, agents.
- Our professional advisors.
- Those to whom we outsource certain functions, for example, postage, marketing, printing, accounting, administration, debt recovery and IT support.
- Referees provided by you to us.
- Insurers and re-insurers.
- Auditors.
- Any person considering acquiring an interest in our business or assets.
- Any organisation providing verification of your identity (including information you have told us as part of AML/CTF Know Your Customer checks), or bank account, credit card or other payment information.
- Claims-related providers, such as assessors and investigators, who help us with claims.
- Financial institutions, for example so that we can process a claim for mistaken payment.
- Government and law enforcement agencies or regulators.
- Any industry body, tribunal, or court.
- Entities established to help identify illegal activities and prevent fraud; and
- Any person where we are required by law to do so.

SENDING INFORMATION OVERSEAS

We may send your information overseas, but only directly to our own offices or agents in an overseas location, and to service providers or other third parties who operate or hold data outside Australia. Where we do this, we make sure, as far as reasonably possible, that appropriate data handling and security arrangements are in place. Please note that Australian law may not apply to some of these entities.

SECURITY

We will take all reasonable steps to protect your personal information from misuse, loss, unauthorised access, modification or disclosure. We will destroy or permanently de-identify personal information we no longer need or which we are no longer required by law to retain. We have physical, electronic and procedural safeguards to protect your information which is held by us. Your information, both hard-copy and/or electronic records, are held at our secure office premises and at secure offsite premises using trusted third parties. Our office premises are protected against unauthorised access by electronic security passes which are held only by our staff, alarms and cameras. Access to information stored, including electronic records which require login and password authorisation, is restricted to our staff whose job purpose requires access. All our staff undertake information security and privacy training. We have firewalls, intrusion detection systems and virus scanning tools to protect against unauthorised persons and viruses accessing our systems.

CUSTOMER RIGHTS

Wherever it is lawful and practicable, we will give you the option of not providing information when entering into transactions with us. However, in most cases, if you do not provide the full and complete information requested we will be unable to provide our products or services to you.

RESPONDING TO DATA BREACHES

We will take appropriate, prompt action if we have reasonable grounds to believe that a data breach may have or is suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC).

If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

HOW DO YOU ACCESS YOUR INFORMATION?

You may ask us what personal information we hold about you, and you may make a request to access to this information at any time. You may make a request by us by contacting our PRIVACY OFFICER (see below contact details). We may ask you to complete a PERSONAL INFORMATION REQUEST FORM and will process your request within a reasonable time and try to make this information available within 30 days of your request. Before we give you the requested information, we will need to confirm your identity.

We generally will not charge you a fee in respect of such access, but reasonable administrative costs may be charged in some circumstances. If there is an access charge, we will give you an estimate first and ask you to confirm that you would like us to proceed, if you would like us to, we do require payment up front. Generally, the access charge is based on an hourly rate plus any other reasonable costs incurred by us such photocopying and postage. We do not need to provide access to your information in several circumstances; for example, the information is commercially sensitive, the request is frivolous or would unreasonably interfere with another person's privacy or be in breach of the law, or, where to provide access would pose a threat to health or public safety. If we refuse you access, we will advise you of our reasons for doing so.

HOW DO YOU CORRECT OR UPDATE YOUR INFORMATION?

You may ask us at any time to correct the information we hold about you or that we have provided to others us by contacting our PRIVACY OFFICER (see below contact details). We will process your request within a reasonable time and try to correct the information within 30 days. If it looks like it will take longer, we will let you know the reason for the delay and try to agree to an extended timeframe with you.

If we are able to correct your information because it is indeed inaccurate, we will inform you when it is so corrected.

If we disagree with you that the information is inaccurate and should be corrected, we will inform you in writing of our reasons. You may request that we attach a statement to that relevant information noting that you consider it is inaccurate misleading, incomplete, irrelevant or out-of-date. We will take reasonable steps to comply with such a request.

WHAT CAN YOU DO IF YOU HAVE A COMPLAINT?

If you are not happy in respect of how we have dealt with your personal information or in gaining access to it, please contact our PRIVACY OFFICER to discuss your concerns (see below contact details). If we do not resolve your complaint to your satisfaction or we are unable to resolve your complaint you have the right to refer the matter the Office of the Australian Information Commissioner – Privacy Hotline on 1300 363 992 or visit their website at www.oaic.gov.au or writing to GPO Box 5218 Sydney NSW 2001.

HOW TO CONTACT US:

PRIVACY OFFICER

Address: Mulpha Group Level 9, 117 Macquarie Street Sydney, NSW 2000 Australia

Phone: +61 2 9270 6186

Email: company.secretary@mulpha.com.au

REVIEW

This policy requires biennial Legal and Compliance and Board Review.

Document Control Log

Version	Document Owner	Author	Approval	Date
1.0	Legal and Compliance	Naomi McRae/ Lesley Stradling	SCSG Risk Management Committee	August 2023