PRIVACY POLICY AND STATEMENT

POLICY OWNER People & Culture
LAST UPDATED February 2024

1. PURPOSE

This Privacy Policy explains how we collect, hold, use and disclose personal information in the course of providing our professional services, through interactions on our website and through our employment and marketing activities.

This policy applies to the following entities within the RSM Australia Group (the **Firm**, **we**, **us**, **our**)

- RSM Australia Pty Ltd (ACN 009 321 377);
- RSM Financial Services Australia Pty Ltd (ACN 009 176 354; AFSL 238 282);
- RSM Australia Partners (ABN 36 965 185 036);
- RSM Digital Australia Pty Ltd (ACN 619 724 551);
- RSM Australia Tax Law Pty Ltd (ACN 151 764 877);
- RSM Corporate Australia Pty Ltd (ACN 050 508 024);
- RSM Australia CPG Pty Ltd (ACN 665 127 337);
- RSM Australia Group Finance Pty Ltd (ACN 654 994 171).

The Firm is a member of the global RSM Network. Each member of the RSM Network is an independent accounting and consulting firm, each of which practices in its own right.

The Firm endeavours to take all reasonable steps to comply with the *Privacy Act 1988* (Cth) (the '**Act**'), the Australian Privacy Principles (**APPs**) and any applicable State or Territory privacy laws, and to otherwise protect the privacy of the personal information that the Firm collects and holds.

We have also taken steps to ensure that, if you tell us you are located in the European Union and advise us that you wish to exercise the additional rights available to you under the General Data Protection Regulation, we will endeavour to meet those requests subject to the terms of this policy.

2. PERSONAL INFORMATION COLLECTED BY THE FIRM

The Firm collects and holds personal information pertaining to its clients, prospective clients, prospective employees, employees, referral sources, alumni, contractors, subcontractors, and other individuals with whom the Firm has dealings.

The Firm collects and records personal information that is necessary to: the recruitment and selection process; the provision of services by the Firm or a contractor or subcontractor; and for marketing activities. Personal information is collected when a person:

- contacts the Firm;
- participates in our recruitment processes;
- engage us to provide services;
- attends events, and information sessions conducted by the Firm; and/or
- offers services as a contractor with the Firm.
- Is part of the RSM Australia Group, from any other member of that Group.

Where possible, the Firm will collect the information directly from you. In some cases, we may collect information directly from your third-party representative or publicly available sources.

Personal information may also be collected where the Firm is required to do so by law (for example, via education, child protection, work health and safety laws, charitable collections, medical treatment, or other legislation in Australia).

Personal information that the Firm collects may include:

- name, date of birth, home and business address and Tax File Number declaration; and/or
- all information that you provide to us to enable us to provide our services to you or to comply with legislative requirements. As an example, the Firm may on occasion require bank account details, details of directorships and investments;
- if you apply to work with us as an employee or contract, records necessary to establish and maintain that relationship; and/or
- all other personal information required for the management of the relationship an individual has with the Firm.

If it is reasonably necessary in the circumstances, the Firm may also collect sensitive information (which is a type of personal information) such as a person's medical history or medical health checks, membership of a professional organisation or criminal record.

3. USE AND DISCLOSURE OF PERSONAL INFORMATION

The Firm uses and discloses personal information in accordance with this policy. Where requested by a person whose personal information is held by the Firm, the Firm will provide details of this activity.

3.1 Why Does the Firm Collect Personal Information?

The Firm collects, holds, uses, and discloses personal information for the purposes of:

- providing our services to you;
- communicating with you;
- assessing your job application;
- obtain services from you;
- to notify clients and alumni of events and services;
- to keep clients and alumni informed on any developments; and/or
- for internal business administration requirements.

3.2 Use and Disclosure – General

As part of our business processes, to back up our information or to obtain certain services, the Firm may use the services of a third party. As a result, personal information collected about an individual may be disclosed to third parties in these circumstances.

We also disclose personal information (this may include sensitive information as outlined above, contact details, financial information about business entities and information about your relationship with the Firm) to other entities within the RSM Australia Group.

3.3 Use and Disclosure – Recruitment

Unsuccessful applications will be retained for any future opportunities. Personal information may also be retained after that time in reports created during the selection and through the application process.

Applicants may be required to provide their written consent to check records maintained by state and/or federal police, the Department of Immigration and Citizenship and the relevant state Road Authority as a part of the selection process. At the Firm’s request, applicants may be required to undertake a medical or health check.

Where third parties are involved in the recruitment, selection or promotion of the Firm's personnel, applicants' personal information may be collected and/or held by that third party for that purpose. The applicant or the Firm may provide personal information to the third party for this purpose. Where such personal information is collected or held by the third party, it will be managed, de-identified and/or destroyed in accordance with the third parties' privacy policy.

3.4 Use and Disclosure - Marketing

The Firm may use and disclose an individual's personal information in order to inform them of products and services that may be of interest. This includes sharing of personal information to other entities within the RSM Australia Group for marketing and customer relationship management purposes.

In the event a person does not wish to receive such communications, they can opt-out by contacting the Firm marketing team or through any opt-out mechanism contained in a marketing communication to you.

4. PRIVACY ON OUR WEBSITE

Individuals do not have to reveal their identity or otherwise provide us with any personal information if they visit our website. However, if a person remains anonymous or goes by a pseudonym, the Firm may be unable to efficiently respond to a request.

Cookies may be used in some areas of the website to improve the navigation use by visitors.

If you are concerned about Cookies, most browsers recognise when a cookie is offered and allow the user to opt out. If a person does this, they can still navigate on our website.

The Firm's website contains links to third party websites which a user can access if they wish. By clicking and accessing these links the user will be subject to the third party's privacy policy and not that of the Firm. The Firm is not responsible for the privacy policies or practices of those website and for any consequences of a person's use of those websites.

The Site is an Australian based website, and it is not intended to provide services to EU residents, and its terms may not be fully consistent with the General Data Protection Regulation. If you are an EU resident and you choose to use the Website then you do so at your own risk, and on the terms of the Site.

5. STORAGE AND DATA SECURITY

All reasonable steps are taken to protect the security of personal information held by the Firm. This includes appropriate measures to protect electronic materials and materials stored and generated in hard copy. The Firm may engage a third party for the storage of personal information, including cloud storage and will take reasonable steps to ensure that the personal information is protected by the third party, including by requiring the third party to itself comply with the Act and the APPs and any applicable State or Territory privacy laws in relation to personal information passed to it by the Firm. The Firm will permanently destroy or de-identify personal information the Firm holds about an individual if the Firm no longer needs it for any purpose, including the purposes set out in this Privacy Policy. Appropriate de-sensitisation of data is practiced, and information is destroyed using secure means.

6. ACCESS ARRANGEMENTS

Individuals can access personal information held about them by the Firm in a prompt and confidential manner by making a request to the Firm. The Firm treats all requests for access seriously and any request to access personal information will not negatively impact the individual's existing obligations or affect any arrangement between them and the Firm.

Clients of the Firm can gain access to the information the Firm holds about them by contacting the Manager/Principal/Partner responsible for providing their services.

All requests will be dealt with in a timely manner and the Firm will endeavour to respond within 30 days. Individuals who find that the personal information the Firm holds about them is inaccurate, incomplete, or out-of-date are asked to contact the Firm immediately via the contact details below and the Firm will correct it.

An individual's right to access their personal information is not absolute. The Firm may deny access to personal information if:

- the request does not relate to the personal information of the person making the request;
- the request is frivolous or vexatious;
- providing access would pose a serious and imminent threat to life or health of a person;
- providing access would create an unreasonable impact on the privacy of others;
- the request relates to existing or anticipated legal proceedings;
- providing access would prejudice negotiations with the individual making the request;
- access would be unlawful;
- denial of access is authorised or required by law;
- access would prejudice law enforcement activities;
- access discloses a 'commercially sensitive' decision making process or information; and/or
- any other reason that is provided for in the APPs set out under the Act.

If the Firm denies access personal information, the Firm will provide the person seeking access with written reasons. Where possible, the Firm will respond to each request within 30 days of a request being received; or where the request is not complicated or does not require access to a large volume, information will be provided as soon as reasonably practical.

There is no charge for making a request for access to personal information. However, individuals will be required to pay all reasonable costs imposed by the Firm for the provision of the requested personal information. Fees will be charged for accessing, photocopying and any delivery charges for personal information stored off-site and access to electronic databases.

7. DATA INTEGRITY

The Firm endeavours to maintain accurate and up to date information. From time to time, the Firm may request individuals to provide an update of their personal information, and at times this is to aid in meeting the Firm's obligations under the APPs.

8. NOTIFIABLE DATA BREACHES SCHEME

In the event of a data breach, the Firm will review the breach and notify affected individuals in accordance with the requirements of the Privacy Act.

9. DISCLOSURE OF PERSONAL INFORMATION OUTSIDE OF AUSTRALIA

There are several circumstances in which the Firm may disclose personal information outside of Australia.

First, in some circumstances, as part of the delivery of the Firm's services, the Firm may be required to disclose personal information to other members of the RSM Network or their representatives overseas. The full list of countries where RSM members firm are located is available here.

Second, the Firm may disclose personal information to third party service providers of the Firm which are located overseas.

The Firm will take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the personal information disclosed to it. Any such transfer of personal information does not change any of the Firm's commitments to safeguard the privacy of personal information and to comply with the Firm's obligations under the Act.

10. COMPLAINTS AND FURTHER INFORMATION

If you have any questions about this policy or would like to make a complaint in relation to the collection, use, disclosure, quality, security of and access to your personal information may be made to the Firm Privacy Officer at:

Director, People & Culture
RSM Australia Pty Ltd
Level 13, 60 Castlereagh Street Sydney NSW 2000
GPO Box 5138 Sydney NSW 2001

The Firm will respond to each complaint within a reasonable period and try to resolve the complaint.

If a person is dissatisfied with the Firm's response to their complaint, they can contact the Office of the Australian Information Commissioner (OAIC). See www.oaic.gov.au for how to make a complaint.

The Firm may amend this Privacy Policy from time to time by publishing an updated version on this website.

11. EUROPEAN RESIDENTS

If you are a resident of the European Union, you have the following data protection rights, which you can exercise at any time by contacting the Privacy Officer listed above.

- The right to opt-out of marketing communications we send you at any time.
- The right to access, correct, update or request deletion of your Personal Data.
- Where you request that we delete your personal data, this will be done in accordance with Australian Laws. For example, we are required to hold some personal data for a period of seven (7) years.
- The right to object to or restrict the processing of your personal information in certain circumstances, except for when processing is required for legal reasons.
- You may revoke your consent for us to process your personal information. In some cases, we may continue to process your data when processing is required for legal reasons.
- You have a right to complain to your local supervisory authority should you feel our processing of your data infringes your European Regulation.

DATA BREACH RESPONSE PLAN

The Firm endeavours to take all reasonable steps to comply with the Notifiable Data Breaches (NDB) scheme, which is in effect through the *Privacy Amendment (Notifiable Data Breaches) Act 2017.* The NDB scheme sets out obligations to notify individuals and the Office of the Australian Information Commissioner (OAIC) about any eligible data breaches which are likely to result in serious harm.

What is an eligible data breach?

An eligible data breach refers to a data breach involving personal information that is likely to result in serious harm to any affected individual, and arises when the following criteria are also satisfied:

- There is unauthorised access or unauthorised disclosure of personal information, or a loss of personal information. ***Unauthorised access*** occurs when personal information that an entity holds is accessed by someone who is not permitted. This includes unauthorised access by an employee, an independent contractor or an external third party (such as by hacking). Unauthorised disclosure occurs when an entity releases information outside of its effective control, whether intentionally or unintentionally, which is not permitted by the Privacy Act. Accidental or inadvertent loss is likely to result in unauthorised access or disclosure ; and
- Remedial action has not been able to prevent the likely risk of serious harm.

Identifying Serious Harm

In deciding whether serious harm is likely to result from a data breach, the following is to be considered.

a) The type(s) of personal information involved in the data breach. Examples of information more likely to cause an individual serious harm if compromised are outlined below:

- Sensitive information, such as information about an individual's health;
- Documents typically used for identity fraud. This includes Medicare card, drivers' licence, and passport details;
- Financial information and/or
- A combination of several types of personal information, which allows more to be known about an individual than what the information is about.

b) The circumstances of the data breach. The following may be considered:

- The individuals whose personal information has been involved;
- Number of individuals involved;
- The extent that the circumstances affect the sensitivity of the personal information;
- Length of time the information has been accessible;
- The adequacy of security measures used to protect the information; and/or
- The parties who have gained or may gain unauthorised access to the personal information.

c) The nature of the harm that may result from the data breach. Examples may include:

- Identity theft;
- Significant financial loss by the individual;
- Threats to an individual's physical safety;
- Loss of business or employment opportunities;
- Humiliation, damage to reputation or relationships; and/or
- Workplace or social bullying or marginalisation.

Preventing Serious Harm with Remedial Action

Where there is any data breach, you are to take all reasonable positive steps to address any data breach in a timely manner, for the purposes of preventing the data breach from being likely to result in serious harm to any individual.

For data breaches where information has been lost, remedial action is adequate if it prevents unauthorised access and disclosure of personal information.

For any data breach, you are required to notify your People and Culture (P&C) representative and your Manager / Partner as soon as practicable.

Examples of remedial action that may prevent serious harm may include, but are not limited to, the following:

- Where an incorrect recipient is sent a data file, the sender contacts the recipient to check whether they have accessed the data and asks them to permanently delete the data. The recipient confirms in writing that they have not copied the data and have permanently deleted the file, and the recipient is also well known to the sender, to the point they regard the recipient as reliable and trustworthy.
- An employee leaves a work mobile device on public transport and contacts the National IT team to remotely delete information on the device. Because of the security measures on the device, National IT are confident its content could not have been accessed in the short period between when it was lost and when its contents were deleted.

Where remedial action does not prevent the likelihood of serious harm and it is believed there has been an eligible data breach, you and your Manager / Partner will work with your P&C representative to promptly notify affected individuals and the OAIC of the data. Please refer to section 8.4 below for further information on this.

Where remedial action does not prevent the likelihood of serious harm and there is suspicion there may have been an eligible data breach, you and your Manager / Partner will work with your P&C representative to conduct an assessment which is reasonable and expeditious. Please refer to the following section for further information on this.

At any time, including during an assessment, you should continue to take steps to prevent serious harm with remedial action. If remedial action is successful in preventing serious harm to affected individuals, then notification to the individuals and to the OAIC is not required.

Assessment of Suspected Eligible Data Breaches

An assessment will occur as a three-stage process, as outlined below:

a) **Initiate:** This involves deciding whether assessment is necessary, and identifying who will be responsible for undertaking this;
b) **Investigate:** This is where relevant information about the suspected eligible data breach is promptly gathered. Such information includes, for example, what personal information is affected, who may have had access to the personal information and any likely impacts; and
c) **Evaluate**: This is where a decision is made based on the investigation, to identify whether the breach is an eligible data breach.

The assessment process and outcome will be documented and kept on record by the Firm.

All reasonable steps will be undertaken to complete the assessment within 30 calendar days from the date an eligible data breach was suspected. Where an assessment cannot be reasonably completed within this timeframe, this will be documented and kept on record by the Firm for the purposes of being able to demonstrate the following:

- That all reasonable steps have been taken to complete the assessment within 30 days;
- The reasons for the delay; and
- That the assessment was reasonable and expeditious.

Notification of Eligible Data Breaches

Notification of an Eligible Data Breach involves notifying the Commissioner of the Eligible Data Breach under the NDB scheme, as well as notifying the affected individuals.

All notifications will include the following information:

- Identity and contact details of the Firm;
- Description of the eligible data breach;
- Types of information involved; and
- Recommendations about the steps individuals should take in response to the eligible data breach.

A statement will be provided to the OAIC as soon as practicable, to notify them of the Eligible Data Breach. Further information in relation to this can be found here on the OAIC site.

In terms of notifying individuals of the Eligible Data Breach who are at risk of serious harm, they will be notified through one of the following three options depending on what is most practicable:

1. **Notify all individuals:** This option may be appropriate, for example, where it cannot be reasonably assessed which individuals are at risk of serious harm.
2. **Notify only those individuals at risk of serious harm:** This option is appropriate where a particular individual, or set of individuals, can be identified as being at risk of serious harm.
3. **Publish notification:** This option is appropriate if neither option 1 nor 2 above are practicable. As part of this option, a copy of the statement must be published on the relevant organisation's website if it has one, and all reasonable steps must be undertaken to publicise the contents of the statement. This statement will be available and published for a period of at least six months.

Prevention of Future Breaches

Once steps as outlined above are taken to address any breaches, you and your Manager / Partner together with your P&C representative will work with any other relevant parties to investigate the cause of the breach and whether to review the existing prevention plan or, where there is no prevention plan in place, to develop one.

A prevention plan should suggest actions that are proportionate to the significance of the breach. It should also consider whether it was a systemic breach or an isolated event. This plan may include, but is not limited to:

- Conducting a security audit of physical and technical security;
- Review of policies and procedures, and incorporate any changes to reflect any lessons learned from the breach or the associated investigation. Ensure regular reviews thereafter;
- Review employee training practices;
- Enhancing transparency of the plan;
- Review service delivery partners, including any offsite data storage providers; and/or
- A requirement for an audit at the end of the process of reviewing a prevention plan, to ensure the plan continues to be implemented and adhered to.

Summary of NDB Scheme

A flowchart that summarises the NDB scheme requirements described above can be found on the OAIC website. A link to this is provided here.