

PRIVACY POLICY

Pureprofile Business Account

ABOUT US

Pureprofile is a global data and insights organisation providing industry-leading online research solutions to agencies, marketers, researchers, brands and businesses.

Pureprofile captures and delivers insights which enable businesses to gain the ability to segment, target and engage with their audiences for the purpose of research, marketing and advertising. In exchange, our panellists receive value for their data, both as an immediate reward and through the delivery of preferred, more relevant content and personalised experiences.

INTRODUCTION

Pureprofile understands the importance of privacy and is committed to protecting personal data collected in the course of our work. This Privacy Policy explains which personal data we collect and how we use it, along with your privacy rights and how the law protects you.

Use by our business customers

This Privacy Policy is based on the following principles:

- You can request to access, update or change your data at any time;
- You may opt-out of the Service at any time;
- We use online technologies and good industry practice to protect all personal data from unauthorised physical and electronic access and interference; and
- We do not disclose your information to any third parties, other than the organisations detailed in this Privacy Policy. Such disclosure is necessary to enable us to provide our services to you and these organisations are required to respect and maintain our commitments to your privacy and the security of your data.

1. IMPORTANT INFORMATION AND WHO WE ARE

Purpose of this Privacy Policy

This Privacy Policy (henceforth, "**policy**") aims to give you information on how Pureprofile collects and processes your personal data. You should read this policy alongside any collection notice we may provide when we are collecting or processing your personal data so that you are fully aware of how and why we are using your data. This policy supplements such notices and is not intended to override them.

Pureprofile Group

The Pureprofile Group ("**Group**") is made up of different legal entities. This policy is issued on behalf of the Group so when we mention "**Pureprofile**", "**we**", "**us**" or "**our**", we are referring to the relevant company in the Group responsible for processing your data. The entities within the Group include:

- Pureprofile Australia Pty Ltd, ABN 99 093 819 713 of 263 Riley Street, Surry Hills, 2010, NSW, Australia;
- Pureprofile NZ Limited, Company number: 5862635 of Level 3, Building E, Union Square, 192 Anglesea Street, Hamilton, 3204, New Zealand;
- Pureprofile Singapore Pte Ltd, UEN 202212468H of 3 Phillip Street #14-05, Royal Group Building, Singapore 048693; and
- Pureprofile UK Limited, Company number: 04077299 of 3rd Floor, Unit 3b, Zetland House, 5-25 Scrutton Street, London, England, EC2A 4HJ.

Controller, Joint Controller or Processor

This section applies where the General Data Protection Regulation (“**GDPR**”) or UK GDPR applies to the processing of your personal data.

Where we determine the purposes and means of processing, we act as the controller (“**controller**”). The Pureprofile entity acting as controller is determined by: (i) the entity through which you register, purchase or interact with; or (ii) failing that, your country of residence. We will confirm the specific entity acting as controller in the collection notice or terms provided to you when we first collect your personal data. Where more than one Group entity jointly determines the purposes and means of processing (i.e. **joint controllers**), we will identify the arrangement between us in accordance with Article 26, GDPR.

Where you or another entity is the controller and we process personal data on your behalf and in accordance with your instructions, we act as the processor (“**processor**”). For example, if you use a Pureprofile Tool such as Datarubico Insights Creator, we act as processor. Where we act as processor, our processing is governed by our [data processing agreement](#) which is consistent with Article 28, GDPR.

Data protection officer

We have appointed a data protection officer (“**DPO**”) who is responsible for overseeing questions in relation to this policy. If you have any questions about this policy, including any requests to exercise your legal rights, please email dataprotectionofficer@pureprofile.com.

UK and European representatives

We have appointed representatives to act on our behalf regarding our compliance with the GDPR and UK GDPR. If you are based in the UK or EEA, you may contact the relevant representative regarding data protection matters relevant to you:

Our EU / EEA Representative is Rickert Rechtsanwalts-gesellschaft mbH, - Pureprofile -, Colmantstraße 15, 53115 Bonn, Germany, art-27-rep-pureprofile@rickert.law

Our UK Representative is: Rickert Services Ltd UK, - Pureprofile -, PO Box 1487, Peterborough, PE1 9XX, United Kingdom, art-27-rep-pureprofile@rickert-services.uk

Your right to make a complaint

We aim to respond to all complaints directly. If for any reason you remain unsatisfied with our response, you have the right to make a complaint at any time to the Information Commissioner's Office (“**ICO**”), the UK regulator for data protection issues (www.ico.org.uk).

If you are based in the EEA, you have the right to make a complaint at any time to a supervisory authority in the country in which you live or work. You can locate a supervisory authority on the European Data Protection Board website (https://edpb.europa.eu/about-edpb/about-edpb/members_en).



If you are based in Australia, you have the right to make a complaint at any time to the Office of the Australian Information Commissioner (“**OAIC**”), the Australian regulator for data protection issues (www.oaic.gov.au).

If you are based in New Zealand, you have the right to make a complaint at any time to the Office of the Privacy Commissioner (www.privacy.org.nz).

Notwithstanding these rights, we would appreciate the chance to deal with your concerns before you approach ICO, or the relevant supervisory authority, the OAIC or the Office of the Privacy Commissioner, so please contact us, or, if applicable, our UK or European representative, in the first instance.

For more information on other rights you may have, please see paragraph 8 (*Your Legal Rights Under the GDPR*).

Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

Our website at <https://www.business.pureprofile.com/> (“**Website**”) may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy policies. When you leave our Website, we encourage you to read the privacy policies of other websites you visit.

2. INFORMATION FOR WEBSITE VISITORS

How is your personal data collected?

We use different methods to collect data from and about you including through:

- Automated technologies or interactions. We may collect, use, store, analyse and transfer personal data we obtain from you via our Website such as internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the Website (“**Website Visitor Data**”). The Website is not intended for children, and we do not knowingly collect data relating to children.
- Third parties or publicly available sources. We may receive Technical Data about you from various third parties and public sources such as analytics providers.
- Communicating with us through correspondence, chats, email, or when you share information with us from other social applications, services or websites;
- Interacting with our sites, services, content and advertising; or
- Investing in our business or enquiring as to a potential purchase of our business.

We may create, collect, use and share **Aggregated Data** such as statistical or demographic data using Website Visitor Data. Aggregated Data may be derived from your personal data but is not considered personal data in law as it does not directly or indirectly reveal your identity. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly



identify you, we treat the combined data as personal data which will be used in accordance with this policy.

We do not collect any sensitive data or Special Categories of Personal Data, such as details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, health or genetic information, or biometric data. Nor do we collect any information about criminal convictions and offences.

If we fail to collect personal data from you and this data is required by us to provide services to you or is required under a contract, we may not be able to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel a service you have with us, but we will notify you if this is the case at the time.

Legal basis for processing

The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

- **Legitimate interests:** The term “legitimate interest” means our interest in conducting and managing our business to enable us to give our clients the best service / product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you, unless we have your consent or are otherwise required or permitted to by law. If you would like further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities, please contact us by emailing dataprotectionofficer@pureprofile.com
- **Legal obligation:** We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to.
- **Performance of a contract with you:** Where we need to perform a contract we are about to enter or have entered with you.
- **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example if you subscribe to an email newsletter.

We use Website Visitor Data to support the operation of our Website. We may on occasion also use it to detect or prevent fraud or crime. We have a legitimate interest in using Website Visitor Data for this purpose where your interests and fundamental rights do not override those interests. We may also use Website Visitor Data to comply with a legal obligation to which we are subject.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Change of purpose

If you are in Australia, we will only use your personal data for the purposes for which we collected it (the “primary purpose”), unless we reasonably consider that we need to use it for another reason (the “secondary purpose”) and it is compatible with the primary purpose. If you wish to get an explanation as to how the processing for the secondary purpose is compatible with the primary purpose, please contact us. If we need to use your personal data for another purpose, we will notify you and we will explain the legal basis which allows us to do so or obtain your consent.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.



3. INFORMATION FOR BUSINESS CLIENTS

Our role as a controller

We act as the controller in relation to the personal data we collect and process when you submit your details via the "Contact Us" form on our Website. We will only process your data for the purpose(s) you have consented to, which may include:

- responding to an enquiry you have submitted via the "Contact Us" form;
- keeping you updated with Pureprofile news, research, studies and product updates (you can unsubscribe at any time).

You may receive marketing communications if you have signed up for our newsletter, purchased our services or consented to receiving updates. We may also collect and process your preferences about receiving marketing from us and our partners and affiliates, and your communication preferences.

You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you, or by contacting us.

We will obtain your express consent before we share your personal data with any third party for marketing purposes. You can withdraw your consent at any time by contacting us at privacy@pureprofile.com, which will stop further sharing of your data for this purpose. You may also ask third parties to stop sending you marketing messages directly by following the opt-out links on any marketing message sent to you by them.

The information we collect about you

We may collect the following types of Information:

- name;
- mailing or street address;
- email;
- your Business Account credentials;
- phone number and other contact details;
- any credit or banking details you provide;
- your activity on the Website, such as when you log in to your Business Account, use a Pureprofile Tool or when you send us Customer Service correspondence;
- your transaction history, including status of campaigns and paid/unpaid invoices;
- information about you that is available on the internet, such as from Facebook, LinkedIn, X and Google, or publicly available information that we acquire from service providers;
- personal data you provide to us through customer satisfaction surveys; and
- any other personal data we may require to facilitate your dealings with us.

How we use the data we collect about you

In addition to the uses identified elsewhere in this policy, we may use your personal data to:

- Provide our services to you or your organisation;



- Administer your Business Account, including in relation to payments;
- respond to your requests and contact you when necessary;
- improve our Website and services;
- improve and personalise your Pureprofile experience;
- send you important updates regarding your Business Account or the status of our services, including the Pureprofile Tools;
- send you marketing communications relating to our business;
- view and access your online accounts (if required); and
- improve the accessibility of Business Accounts and / or our Website.

We will never sell your personal data to any third party.

Cookies

We use cookies and similar technologies on our Website. When you first visit our Website, you will be asked to consent to non-essential cookies via our cookie banner. You may accept all, reject all (other than strictly necessary cookies), or select which categories to allow. No non-essential cookie is set until you have made a choice. For more information, please see our [Cookie Policy](#).

4. DISCLOSURES OF YOUR PERSONAL DATA

This section applies to all personal data covered by this policy.

We may share your personal data with the parties set out below for the purposes set out above – see “[How We Use Your Personal Data](#)”:

- Other companies within the Group, where such sharing is necessary for internal administrative purposes, to provide our services to you, or for the purposes set out in this policy;
- Our clients and advertisers, third party agents, service providers such as Amazon Web Services (AWS) and contractors. We work with service providers globally, therefore some of the recipients of your personal data are based overseas;
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in the UK and Australia who provide consultancy, banking, legal, insurance and accounting services;
- Regulators and other supervisory authorities in Australia, the UK and other countries where we operate who require reporting of processing activities in certain circumstances; and
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this policy.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We only disclose your credit card or banking details (if any) to the relevant payment service



provider for processing payments owing to us for our provision of the Service. This disclosure occurs in a secure and protected online facility.

5. INTERNATIONAL DATA TRANSFERS

This section applies to all personal data covered by this policy.

Whenever we transfer your personal data out of the UK or the EEA, we ensure an adequate degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- The country to which your personal data is transferred has been deemed to provide an adequate level of protection for personal data by the ICO or, if applicable, the European Commission; or
- The third party has entered into a contract with us which contains undertakings and assurances from them to give your personal data the same protection it has in the UK or, as applicable, the EEA.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK or the EEA.

6. DATA SECURITY

We have implemented appropriate security measures to prevent your personal data from being accidentally lost, used, accessed, altered or disclosed in an unauthorised way. Additionally, we limit access to your personal data to those employees, agents, contractors and other third parties who have a need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have also put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

We also use technology to encrypt the transfer of all personal data. All data collected and stored by Pureprofile is protected by firewalls and other intrusion protection and detection tools. Our internal control environment is continuously monitored, and we are ISO 27001 certified by external auditors.

7. DATA RETENTION

We may retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Where the GDPR and UK GDPR applies, you can ask that we delete your data in some circumstances (see the next section for further information).

In some circumstances, we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.



8. YOUR LEGAL RIGHTS UNDER THE GDPR / UK GDPR

Under certain circumstances, you have rights under data protection laws in relation to your personal data as described below:

- **Right to request access** to your personal data (commonly known as a "data subject access request" or "DSAR"). This enables you to request a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Right to request correction** of the personal data we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Right to request erasure** of your personal data (commonly known as the "right to be forgotten"). This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with applicable law. We may not always be able to comply with your request of erasure for specific legal reasons which, if applicable, will be notified to you at the time of your request.
- **Right to object** to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing as you believe it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- **Right to request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - You want us to establish the data's accuracy;
 - Our use of the data is unlawful but you do not want us to erase it;
 - You need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - You have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.
- **Right to portability** of your personal data. Where relevant, we will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Right to withdraw consent** at any time where we are relying on your consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please email dataprotectionofficer@pureprofile.com.



No fee usually required

You will not have to pay a fee to access your personal data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally, it may take us longer than one month if your request is particularly complex or you have made multiple requests. In this case, we will notify you and keep you updated.

Changes to this policy and your duty to inform us of changes

We keep this policy under regular review. This version was last updated on the date shown at the end of the policy. Historic versions can be obtained by contacting us.

1 September 2026

