CORPORATE POLICY

Privacy Policy

Version: 1.0 | Issue Date: 7 November 2025

Table of Contents

Purpose and Scope	2
Application	2
What is personal information	2
What types of personal information do we collect?	3
How do we collect and hold your personal information?	4
Providing personal information through MicroSourcing or Beepo website	6
What happens if we are unable to collect your personal information?	6
For what purpose do we collect, use and disclose your personal information?	7
To whom do we disclose your personal information?	9
Direct marketing materials	10
How can you access and request correction of your personal information?	10
Rights under GDPR	11
Data Subject Rights under Philippine Data Privacy Act of 2012	11
How to complain	12
Data Subject Rights under Colombian Data Protection Regulation	12
Do we disclose your personal information to anyone overseas?	14
Storage, Retention and Disposal	15
Security	15
Links	16
Credit Reporting Privacy Policy - Australia Only	16
Contacting us	17
Changes to our Privacy Policy	18
Annexure	18
Document Information	19

Purpose and Scope

MicroSourcing and Beepo protect the rights and rights of individuals in relation to their personal information. From time to time, MicroSourcing and Beepo may collect and process personal information of existing and prospective customers of our clients and potential, existing and former employees and contractors. This Policy identifies how MicroSourcing and Beepo collect and manage personal information. MicroSourcing and Beepo aim to handle personal information in an open and transparent manner consistent with the objectives of Philippine, Australian and Colombian Privacy Principles.

MicroSourcing and Beepo may be subject to the Philippine Data Privacy Act of 2012, the Australian Privacy Act 1988 (Cth) including the Australian Privacy Principles, the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the New Zealand Privacy Act 2020, Colombian Laws 1581 of 2012, 1266 of 2008, Decree 1377 of 2013, and the South Africa Protection of Personal Information Act 2013, as applicable. This Policy explains how and why MicroSourcing and Beepo collect, use, hold and disclose personal information. We may refer to these acts and regulations, as may be applicable, as "Data Protection Legislation" in this Privacy Policy.

Application

This Policy applies to all employees of MicroSourcing and Beepo, and all its related entities, as well as to any data subject whose personal data are processed, including but not limited to, Beepo Support Services Pty Ltd ACN 167 554 967, MicroSourcing International Ltd, MicroSourcing Philippines Inc., MicroSourcing Colombia SAS, and Beepo, Inc.

Where the words 'MicroSourcing and Beepo', 'MicroSourcing', 'Beepo', 'MS', 'we', 'us' and 'our' is used, it applies equally to all MicroSourcing and Beepo related entities. Where the word 'employee(s)' is used it applies equally to agency workers and contractors.

What is personal information

When used in this Policy, the term 'personal information' means any information or opinion (regardless of whether it is true) about an identifiable individual or an individual who is reasonably identifiable from the information or opinion. This may include an individual's name, address, telephone number, email address, credit card details, account number, and profession or occupation. If the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information. This Policy explains how we process 'personal data' in the Philippines, Australia, European Union (EU), UK, Colombia as required under the Philippine Data Privacy Act of 2012, Australia Privacy Act, GDPR, UK GDPR and Colombian Laws.

What types of personal information do we collect?

MicroSourcing and Beepo may collect the following types of personal information:

- name;
- signature;
- mailing or street address;
- email address and telephone and fax number;
- age or birth date;
- system access passwords for employees;
- profession, occupation or job title;
- your government-issued identification cards, social security numbers, and other government issued numbers.
- where you are our employee, your personnel records including your employment agreement, pay records, leave records, tax status, criminal record checks, superannuation records, educational qualifications, training records, and performance and disciplinary records;
- where you are our client, details of the products and services you have purchased from us or our other clients (on whose behalf we may provide products or services) or which you have enquired about, together with any additional information necessary to deliver those products and services and to respond to your enquiries;
- where you are a customer of our client and we are verifying your identity, your name, residential address and date of birth;
- where you are a customer of our client and we are discussing overdue debts, details of your employment and bank account details;
- credit card details;
- details of your creditworthiness and credit history;
- any additional information relating to you that you provide to us directly through our websites or indirectly through use of our websites or online presence, through our representatives or otherwise;

We may collect the following information deemed to be sensitive:

- Health information relating to an employee or a customer of our client where directly relevant to the goods or services acquired;
- Racial or ethnic origin where you are our employee; and
- Administrative and criminal record checks where you are our employee or a prospective employee.

MicroSourcing and Beepo have set out in the Annexure to this Policy some more details about the information we may collect and hold in respect of each of our key businesses. Please read this carefully.

We may also collect information that is not personal information because it does not identify you or anyone else For example, we may collect anonymous data or aggregated information about how users use our websites.

Where relevant for the purposes of the applicable Data Protection Legislation, if we are acting as a Data Controller, we will process your personal information based on your consent and our legitimate interest. If we are acting as a Data Processor, acting on behalf of companies that employ our services, the legal basis for processing your data is based on the performance of a contract. Therefore, we will not store, process or transfer your data unless we have an appropriate lawful reason to do so. Please contact the company about further information about how they process your personal information.

How do we collect and hold your personal information?

We collect personal information directly from an individual unless it is unreasonable or impracticable to do so. When collecting personal information from an individual, we may collect in the following ways:

- through your access and use of our website;
- through your use of telephone and mobile communication (including but not limited to fixed line IVR services);
- through your use of electronic devices including tablets, supplied by us to you, or otherwise connecting to our systems in order to facilitate and enable you to perform your duties or to provide services to us;
- during conversations between you and our representatives;
- during correspondence between you and our representatives, including electronic correspondence;
- when you engage with us via social media or other online platforms; or
- when you complete an application, contract or purchase order.

Some of the personal information we collect is not collected by us directly from you. Since Microsourcing and Beepo provide digital customer experience solutions, managed outsourcing services, and operate customer contact centres on behalf of many companies globally, from retailers to banks and other institutions, much of the data and personal information it collects is provided to it by its clients.

Often it is impracticable for us to collect information directly from you when we are acting as the ‘agent’ or service provider of our client, as our client has already collected the relevant information from you (or another third party), and our client has provided it to us for our use in providing services to or on behalf of our client. For example, we act on behalf of many clients in sending email communications. To enable us to do so we may use the details which our client has supplied to us.

In respect of personal information which is provided to us by our clients, we do seek client assurances that all such personal information has been collected lawfully and in compliance with applicable Data Protection Legislation and that all required consents have been obtained, and disclosure statements provided, in respect of the intended uses and disclosures of that personal information. Details on how this personal information is managed will be in accordance with the relevant client's privacy management requirements that will be in addition to this Policy. A client's privacy policy should also be referenced separately regarding personal information management for these client services and should in most circumstances be available publicly on a client's website, or from their privacy officer directly.

We may also collect personal information from third parties who are not our clients including, for example, from third party companies such as data providers, credit reporting bodies, law enforcement agencies and other government entities.

If you apply for a job or contract with us, we will collect personal information about you from your referees. With your consent we may also use a third party service to ensure your employment, educational and identity records are valid, and may conduct an administrative or criminal record check. We may also check some details about our suppliers from publicly available sources, such as the Australian Business Register and ASIC databases.

For the Philippines, if you apply for a job or contract with us, we will also collect personal information about you from job portals, third-party placement vendors or referral channels, by attending consultations, interviews, signing-up and filling out our online job application portals, through your submitted resume, from former employees, work colleagues, educational institutions, professional or industry associations, registration or regulatory bodies, or appropriate government agencies when we conduct Background Investigation or profile verification or checking.

We collect limited information about users of our websites, for diagnostic and analytic purposes. This information may include:

- the location from which you have come to the site and the pages you have visited; and
- Technical data, which may include IP addresses, the types of devices you are using to access the website, device attributes, browser type, language and operating system.

We use cookies and gather IP addresses to do so, but we do not trace these back to individual users. A cookie is a small text file that the website may place on your device to store information. We may use persistent cookies (which remain on your computer even after you close your browser) to store information that may speed up your use of our website for any of your future visits to the website. We may also use session cookies (which no longer remain after you end your browsing session) to help manage the display and presentation of information on the website. You may refuse to use cookies by selecting the appropriate settings on your browser. However, please note that if you do this, you may not be able to use the full functionality of the website.

Providing personal information through MicroSourcing or Beepo website

Where an individual is required to provide personal information directly via MicroSourcing or Beepo website, you and accept that:

A. We may transfer your personal information to our related organisations overseas that includes Philippines, Colombia, Australia, New Zealand, South Africa and the United States of America.

B. MicroSourcing or Beepo websites also provide links to third party websites. Where you provide your personal information directly to these third party organisations the use of your personal information by them is not within our control and, therefore, we cannot accept responsibility regarding the use of your personal information by these organisations. It is recommended that you review the privacy policies of these organisations prior to providing your personal information.

What happens if we are unable to collect your personal information?

If you do not provide us with your personal information described above, some or all of the following may happen:

- we may not be able to provide the requested products or services to you, either to the same standard or at all, or we may not be able to supply services to our clients which may prevent our clients to do the same; or
- we may not be able to provide you with information about products and services that you may want, including information about discounts, sales or special promotions, or we may not be able to information to our clients which may prevent our clients to do the same; or
- we may be unable to tailor the content of our websites to your preferences; or
- if you are a prospective employee, we may not be able to hire you; or
- if you are a contractor to us, you may not be able to provide your services to us.

For what purpose do we collect, use and disclose your personal information?

MicroSourcing and Beepo collect, use and disclose personal information primarily so we can perform our business activities and functions. This includes for the following purposes, in each case, either on our own behalf or when acting on behalf of a client:

- to provide products and services to you (including our clients' products and services) and our clients, and manage our relationship with you;
- to send communications requested by you and/ or our clients;
- to identify and tell you about other products or services that we think may be of interest to you, or to answer enquiries and provide information or advice about existing and new products or services;
- to assess the provision of, and provide credit, to you;
- to undertake debt collection services on behalf of our clients;
- for the administrative, marketing (including direct marketing), planning, product or service development, quality control and research purposes of Probe, its related bodies corporate, or clients;
- to provide your updated personal information to our related bodies corporate, clients, contractors or service providers;
- to update our records and keep your contact details up to date;
- to contact you, including to process and respond to any queries or complaints made by you, or if we need to tell you something important;
- to comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator, or any governmental authority;
- to process queries on our website and facilitate website access;
- to transfer Personal Data (to a controller and/or processor) in accordance with the applicable legal safeguards governing each of these operations.
- to control and prevent fraud and money laundering, including but not limited to consulting restrictive lists and obtaining all necessary information required under local AML systems.
- to manage Personal Data so that Probe, in its capacity as employer, may duly comply with its obligations (as applicable).
- for Colombia, to manage the personal data of the data subject and of his or her family group for the purpose of carrying out affiliation procedures with health promoting entities (EPS), family compensation funds, labor risk administrators (ARL), and any other entities as may be necessary for the Controller to fulfill its legal obligations, when applicable.
- to ensure proper management of the contractual relationship.
- specific for Colombia operations, to consult your Personal Data in credit information agencies in order to verify your financial performance and payment capacity;

- specific for Colombia operations, to report to such credit information agencies regarding the fulfillment or breach of your obligations;
- specific for Colombia operations, to provide said credit information agencies with data related to your commercial, financial, and, in general, socioeconomic relationships, among others.
- to comply with any other legal obligation applicable to Probe.
- to law enforcement agencies where required or authorised by law; or
- for other purposes with your consent, unless you withdraw your consent.

The 'lawful processing' grounds on which we will use personal information about you under Article 6.1 of the GDPR, where the GDPR applies to you, is where:

- You have given consent to the processing of your personal data for the specific purpose of acquiring goods and services (including to a MicroSourcing or Beepo client);
- Processing is necessary for the performance of a contract to which you are a party or in order to action a request you have made prior to entering into a contract (this includes a contract with a MicroSourcing or Beepo client); or
- Processing is necessary for compliance with a legal obligation to which either MicroSourcing or Beepo, or our client are subject; or
- Processing is in our legitimate interests, where such interests are not overridden by your interests or fundamental rights and freedoms.

From time to time, we may use de-identified data for the purpose of improving and enhancing our products and services, as well as those of our clients. Such activities may involve the use and implementation of generative artificial intelligence. Where we use data in this way, we will do so in compliance with applicable Data Protection Legislation and the primary way in which we will achieve compliance is through the de-identification of data prior to such use. Further information about our use of data can be found in our 'Responsible and Ethical Data and AI Use Policy'.

Where you are our employee, we may collect, use and disclose your personal information for all purposes connected with our employment relationship. This includes hiring you, training you, remunerating you, administering your personnel records (including pay and leave records), managing workers' compensation or similar insurance claims, and managing your performance and disciplinary investigations, proceedings or sanctions.

If you are an employee or prospective employee of our operations in the Philippines, with your consent, we may collect, use and disclose your personal information for purposes of the implementation of the One Trust Link (OTL) Program of the Contact Center Association of the Philippines (CCAP).

We may also use your personal information for other purposes related to those described above, and/or for a purpose for which you would reasonably expect it to be used, as permitted by the applicable Data Protection Legislation.

Except as provided below, your personal information will not be shared, sold, rented or disclosed other than as described in this Privacy Policy. We do not disclose personal information we obtain when acting on behalf of one client, to any other client, unless directed by the client who has disclosed the personal information to us.

We sometimes handle personal information relying on exemptions under the applicable Data Protection Legislation. Under the Australian Privacy Act 1988 (Cth), these include exemptions in relation to:

- employee records;
- related bodies corporate;
- use or disclosure authorised by or under an Australian law or a court/tribunal order; and
- use or disclosure reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Any permitted handling of personal information under such exemptions will take priority over this Privacy Policy to the extent of any inconsistency.

To whom do we disclose your personal information?

We may disclose your personal information to:

- our employees, related bodies corporate, clients, contractors or service providers for the purposes of operation of our websites or our businesses, fulfilling requests by you, and to otherwise providing products and services to you and our clients including, without limitation, IT systems administrators, couriers, payment processors, data entry service providers, electronic network administrators, debt collectors, and professional advisors such as accountants, solicitors, business advisors and consultants;
- suppliers, field officers and other third parties with whom we have commercial relationships, for business,
- collection, marketing, credit reporting and related purposes; and
- any organisation for any authorised purpose with your consent.

We may combine or share any information that we collect from you with information collected by any of our related bodies corporate. Our clients may do likewise.

For prospective employees, personal information collected may be transferred to our related organisation in Colombia or Australia for the purposes of processing the application and stored on servers located in Australia, Philippines or Colombia.

Direct marketing materials

We may send you direct marketing communications and information about our products and services that we, or our clients, consider may be of interest to you. These communications may be sent in various forms, including email, in accordance with applicable marketing laws, such as the Consumer Act of the Philippines, Australian Spam Act 2003 (Cth), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Unsolicited Electronic Messages Act 2007 (NZ) and Law 2300 of 2023 in the case of Colombia.

At any time you may opt-out of receiving marketing communications from us by contacting us (see the details below) or by using opt-out facilities provided in the marketing communications and we will then ensure that your name is removed from our mailing list (or where we are using a mailing list provided by our client, we will pass your request on to our client).

We do not provide your personal information to other organisations for the purposes of direct marketing (see also our use of cookies). However, where we are engaged by our clients to act on their behalf in collecting personal information then we will pass that personal information on to our client for the purposes for which it was collected.

How can you access and request correction of your personal information?

You may request access to any personal information we hold about you at any time by contacting us (see the details below). Where we hold personal information, we will try to provide you with suitable means of accessing it (for example, by mailing or emailing it to you). We may charge you a fee to cover our administrative and other reasonable costs in making the information available to you and, if so, the fees will be $30 per hour of time spent. We will not charge for simply making the request and will not charge for making any corrections to your personal information.

Where you are an EU or UK resident, we will not typically charge you for exercising your data subject rights. However, we may charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive.

There may be instances where we cannot grant you access to the personal information we hold. For example, we may need to refuse access if granting access would unreasonably interfere with the privacy of others. If that happens, we will give you written reasons for any refusal.

If you believe that personal information we hold about you is incorrect, incomplete or inaccurate, then you may request us to correct it. We will consider if the information requires correction. If we do not agree that there are grounds for correction then as required by the applicable Data Protection Legislation we will, where requested by you, take reasonable steps to attach to or associate with the information a statement of the correction sought but not made, or a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

Rights under GDPR

Under the GDPR, as a data subject you have the right to:

- access your data;
- have your data deleted or corrected where it is inaccurate;
- object to your data being processed and to restrict processing;
- withdraw consent to having your data processed;
- have your data provided in a standard format so that it can be transferred elsewhere; and
- not be subject to a decision based solely on automated processing

We have processes in place to deal with Data Subject Rights requests. Our actions and responsibilities will depend on whether we are the controller or processor of the personal data at issue. Depending on our role as either a controller or processor, the process for enabling Data Subject Rights may differ, and are always subject to applicable law. Please refer to the Contact Details section of this policy if you would like to make a Data Subject Rights request or you have a specific need for assistance with a Data Subject Rights request.

Data Subject Rights under Philippine Data Privacy Act of 2012

If a Data Subject in the Philippines, we value and respect your rights as a data subject pursuant to the Philippine Data Privacy Act of 2012, which includes your:

- **Right to be informed.** We, through our Privacy Policy and this Consent Form, have informed you of whether your personal information shall be, are being, or have been Processed.
- **Right to Access.** You have the right to obtain confirmation on whether or not data relating to you are being processed.
- **Right to Object.** You have the right to object to the processing of your personal data where such processing is based on consent or legitimate interest.
- **Right to Erasure or Blocking.** You have the right to request for the suspension, withdrawal, blocking, removal or destruction of your Personal Data from our system upon discovery and substantial proof that your Personal Data are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or is no longer necessary for the purposes for which they were collected. In this case, we may notify third parties who have previously received your processed Personal Data.
- **Right to Rectify (or Update).** You may dispute an inaccuracy or error in your Personal Data and have us correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.

- **Right to Damages.** Right to be indemnified for any damages you may have sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of your Personal Data.
- **Right to Complain.** Right to file a complaint with the Philippine National Privacy Commission (NPC).
- **Right to Data Portability.**

You may exercise your data subject rights in the Philippines by contacting its Data Protection Officer at dpo@microsourcing.com, or dpo@beepo.com.au, depending on the entity that you are connected, related, or otherwise associated with.

Data Subject Rights under Colombian Data Protection Regulation

If you are a Colombian Data Subject, you have the right to:

- know, update, and rectify your personal data.
- request evidence of the consent granted to the data controller for processing, except in cases where your consent is not expressly required by law for processing.
- be informed about the use of your Personal Data.
- file claims with the Superintendence of Industry and Commerce (SIC) for violations of the law.
- revoke your consent and/or request the deletion of your Personal Data, when the Processing does not respect constitutional and legal principles, rights, and guarantees.
- access your Personal Data free of charge.

How to complain

If you believe that your privacy has been breached or otherwise have a complaint about the way we handle personal information, please contact us using the contact information below and provide details of the incident so that we can investigate it.

Our procedure for investigating and dealing with privacy breaches and complaints is to ascertain all relevant facts and correspond with those involved (including where relevant our clients), reach a view as to the existence, scope and cause of the issue, and where relevant and appropriate, implement corrective or rectification measures.

We will consider your complaint and determine whether it requires further investigation. We will notify you of the outcome of this investigation and any subsequent internal investigation.

A request for access to the personal information held by us concerning an individual can be made by that individual to our Privacy Officer on the numbers or address mentioned below or, in cases where we are acting on behalf of a client, to our client.

If you remain unsatisfied with the way in which we have handled a privacy issue, you may approach an independent advisor or contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au for guidance on alternative courses of action which may be available. If you are in the European Union, you can choose to instead lodge a complaint with your local Data Protection Authority (DPA). The list of DPAs is at https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

If you are a UK resident, you may lodge a complaint with the Information Commissioner's Office (the ICO). If you are a Philippine resident, you may lodge a complaint with the Philippine National Privacy Commission.

If you are a Colombian data subject, the following procedure applies to the handling of your inquiries and claims.

Inquiries Procedure - Colombia only

Inquiries:

Data Subjects who wish to make inquiries should take into account that we, as the Data Controller, will provide them with all the information contained in the individual record or related to the identification of the Data Subject. The inquiry shall be made through the channels enabled by us and will be addressed within a maximum period of ten (10) business days from the date of receipt of the request. When it is not possible to address the inquiry within that period, the interested party will be informed, stating the reasons for the delay and indicating the date on which their inquiry will be addressed. In any case, this date cannot exceed five (5) business days from the expiration of the initial period, without prejudice to the provisions contained in special laws or regulations issued by the National Government that may establish shorter terms, taking into account the nature of the Personal Data.

Claims:

Data Subjects who believe that the information contained in a our Database should be corrected, updated, or deleted, or who detect the alleged non-compliance with any of the duties established in the Applicable Law, may file a complaint with MicroSourcing or the Data Processor, which will be processed according to the following rules:

1. The complaint shall be made by means of a request addressed to the Data Controller or Data Processor, including the identification of the Data Subject, a description of the facts that give rise to the complaint, and the address, along with any supporting documents.

2. If the complaint is incomplete, the interested party will be required, within five (5) days following the receipt of the complaint, to rectify any shortcomings. If two (2) months have passed since the date of the request without the applicant submitting the required information, it will be considered that they have withdrawn the complaint.

3. If the party receiving the complaint is not competent to resolve it, they will forward it to the appropriate entity within a maximum period of two (2) business days and inform the interested party of the situation.

4. Once the complete complaint is received, a legend will be included in the Database within a maximum period of two (2) business days stating, “complaint in progress” and the reasons that led to it. This legend must be maintained until the complaint is resolved in depth.

5. The maximum period for addressing the complaint will be fifteen (15) business days, counted from the day following the date of its receipt. If it is not possible to address the complaint within this period, the interested party will be informed of the reasons for the delay and the date on which their complaint will be addressed, which may not, in any case, exceed eight (8) business days after the expiration of the initial term.

Do we disclose your personal information to anyone overseas?

We may disclose personal information to our related bodies corporate and third party suppliers and service providers located overseas for some of the purposes listed above. Some of our employees are located overseas.

Except where specific individual consent has been obtained, we take reasonable steps to ensure that the overseas recipients of your personal information do not breach the privacy obligations relating to your personal information.

We may disclose your personal information to entities located overseas, including the following:

- our related bodies corporate located in the Philippines, Colombia, Australia, New Zealand, and the United States of America;
- our data hosting and other IT service providers, located in the Philippines, Colombia, Australia, New Zealand and the United States of America; and not be subject to a decision based solely on automated processing.
- our clients and their related entities located in foreign countries, to the extent that we are acting on their behalf or at their direction in using, storing, or collecting your personal information. Applicable foreign countries include Philippines, Colombia, Australia, New Zealand, and the United States of America.

Storage, Retention and Disposal

MicroSourcing and Beepo retain a record of your personal information in accordance with our Data Retention Policy and aligned with appropriate Data Privacy Regulations, including the Philippine Data Privacy Act of 2012, Colombian Laws 1266 of 2008 and 1581 of 2012, and never retains your Personal Data for longer than is necessary, or reasonable to fulfill the purposes that justify its processing.

We may hold your information in either electronic or hard copy form. We store most information about you in computer systems and databases operated by either us or our external service providers. Some information about you is recorded in paper files that we store securely.

Destruction of hard copies of data must be conducted by secure shredding using the facilities located in Probe's offices. Destruction of electronic data is undertaken through secure means. Our manner of disposal shall ensure that the personal information shall no longer be retrieved, processed, or accessed by unauthorized persons.

Security

We take reasonable precautions to protect personal information from misuse, loss, theft, as well as against unauthorised access, modification or disclosure, alteration and destruction. In addition to electronic data protection through password access, data back-up and firewalls, these measures include:

- administrative processes;
- technical safeguards;
- physical infrastructure and site security;
- requiring all employees to comply with internal information security policies and keep information secure; and
- requiring all employees to complete training about privacy and information security.

We have comprehensive security policies and procedures in place to ensure the protection of personal information held by both us and our clients.

As part of our commitment to continuous process improvement, regular audits will be undertaken to ensure that these security practices are adhered to and remain current.

As our website is linked to the internet, and the internet is inherently insecure, we cannot provide any assurance regarding the security of transmission of information you communicate to us online. We also cannot guarantee that the information you supply will not be intercepted while being transmitted over the internet. Accordingly, any personal information or other information which you transmit to us online is transmitted at your own risk.

Links

Our website may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for informing you about their own privacy practices. Before providing your personal information, we advise you to examine the terms and conditions of using that website and its privacy policy.

Credit Reporting Privacy Policy - Australia Only

This Credit Reporting Privacy Policy describes our our practices in connection with information we collect and hold about individuals when providing commercial credit, in particular:

- information we collect and hold about individuals who are directors of a company, when providing commercial credit to that company;
- information we collect and hold about individuals who provide a personal guarantee to us in relation to commercial credit we provide to a company; and
- information we collect and hold about individuals who are obtaining that credit for their own business
- purposes as sole traders or partners in a partnership.

In this Credit Reporting Privacy Policy, “credit-related personal information” means one or more of “credit information”, “credit eligibility information”, “credit reporting information” or “regulated information”, as those terms are defined in the Australian Privacy Act 1988 (Cth).

When you apply for or obtain or guarantee credit from us, the credit-related personal information that we collect from you includes information that identifies you, such as your name, postal address, email address and date of birth and your driver’s license number.

We may exchange credit-related personal information about you with credit reporting bodies (CRBs) for the purposes of assessing commercial credit applications from you or companies of which you are a director, and also to assess whether to accept a guarantee from you.

We may use the information we collect from and about you for account management and administrative purposes directly related to the provision or management of the commercial credit we provide to you or to companies of which you are a director.

We may also report defaults in payment terms or guarantee commitments in relation to commercial credit to CRBs. We may also disclose your credit-related personal information to any guarantor of your obligations to us.

We may also use the information we collect from and about you to:

- collect overdue payments;
- assign debts; and
- create assessments and ratings of your creditworthiness.

We may disclose your credit-related personal information to our related bodies corporate and third party suppliers and service providers located outside Australia, for the purposes set out in this Credit Reporting Privacy Policy.

Further details about such overseas disclosures are set out in the section “Do we disclose your personal information to anyone overseas?” of this Privacy Policy.

For information about the following topics in relation to our handling of credit-related personal information please refer to the applicable section of our Privacy Policy (of which this Credit Reporting Privacy Policy comprises a part):

- Access and Correction - see section “How can you access and request correction of your personal information?”;
- Complaints - see section “What is the process for complaining about a breach of privacy?”;
- Disclosure outside Australia - see section “Do we disclose your personal information to anyone overseas”; and
- Security - see section “Security”.

Contacting us

If you have any questions about this Privacy Policy, any concerns or a complaint regarding the treatment of your privacy or a possible breach of your privacy, please use the contact link on our website or contact the applicable Privacy Officer using the details set out below.

We will treat your requests or complaints confidentially. Our representative will contact you within a reasonable time after receipt of your complaint to discuss your concerns and outline options regarding how they may be resolved. We will aim to ensure that your complaint is resolved in a timely and appropriate manner.

Please contact our Philippine-based Privacy Officer at:

Att: Data Protection Officer
MICROSOURCING AND BEEPO
dpo@microsourcing.com, or
dpo@beepo.com.au

If you are a Colombia Data Subject, you may contact our Colombia-based Privacy Officer at:

Att: Privacy Officer
MICROSOURCING COLOMBIA SAS
Tax ID (NIT): 901.900.826-7
dpo@microsourcing.com
CARRERA 12 # 89 - 33 Floor 6, Bogotá D.C.
6017561220

Changes to our Privacy Policy

MicroSourcing and Beepo may change this Privacy Policy from time to time. A revised version of this Privacy Policy will be posted on our website.

This Privacy Policy was last updated on **7 November 2025.**

Annexure

Specific examples of personal information held by MicroSourcing and Beepo

Business Activity	Types of Personal Information held and/or collected
Contact centre services	• Name, address, contact details, date of birth, payment details including bank account details, credit card information, purchase history, purchase trends, enquiries, problems experienced, customer service issues, insurance policy details, referral advisor details, claim information, subscription details, email information, invoices, survey information. • Where we are given access directly to our clients systems, we have access to the personal information held in those systems. For example, we may operate a call centre of a bank, retailer , health provider etc.
Speech solutions	• Name, address, contact details, passwords, or other personal identifiers such as voice recognition details.
BPO and collections services	• Name, address, contact details, date of birth, payment details including bank account details, credit card information, purchase history, purchase trends, enquiries, problems experienced, customer service issues, customer debt and payment history and information regarding the customer's workplace and employment.
Physical site security	• Where we are given access directly to our clients systems, we have access to the personal information held in those systems.
Credit reporting in relation to commercial credit	• Help desk and other customer issues support as required.
Employees	• Surveillance camera data
Visitors to website	• See "Credit Reporting Privacy Policy" section of this Policy.

Document Information

© Copyright 2025. The information in this document is for the sole use of MicroSourcing and Beepo staff. It contains company confidential information. No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent. This document should not be circulated outside MicroSourcing and Beepo without the written consent of the Release Authority. Where no release authority is listed, a Senior Manager's written consent must be obtained before the document is circulated outside MicroSourcing and Beepo.

All hard copies of this document are uncontrolled.

microsourcing beepo®