

Privacy Policy



ive

1 PURPOSE & SCOPE

IVE Group Ltd (IVE) is Australia's largest diversified marketing company. Specialising in Creative & Content, CX & Data, eCommerce, Brand Activations, Merchandise, Uniforms & Apparel, Packaging, Print, Distribution and 3PL, we connect more than 2,800 clients with their customers every day.

This Privacy Policy (Policy) applies to IVE Group Limited and its Australian subsidiaries that handle personal information, excluding those subsidiaries that maintain and publish their own privacy policies, and including Guangzhou IVE Trading Company Limited which has an Australian link for the purposes of the Privacy Act 1988 (Cth) – collectively referred to as “IVE”, “we”, “us” or “our”.

This Policy explains how we collect, hold, use and disclose personal information and how you can contact us about privacy matters.

This Policy applies to personal information we collect in Australia through interactions with customers, suppliers, and their staff and contractors, job applicants, individuals and our eCommerce systems. This Policy also explains how cross-border disclosures are managed.

This Policy is required by, and complies with, the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). It explains how we meet our obligations to you under this legislation.

2 WHAT PERSONAL INFORMATION WE COLLECT AND WHAT WE USE IT FOR

IVE collects and uses the following types of information (that are subject to the obligations of the Privacy Act) for the purposes stated below:

<i>Purpose</i>	<i>Types of Personal Information</i>
To enable ordering and delivery of our products and services by customer staff and to carry out business services and communications with customers and suppliers	Names, email addresses, job titles, phone numbers, delivery addresses.
To respond to queries or complaints from members of the public or third parties including regulatory bodies or government agencies.	Names, email addresses, phone numbers and any personal information provided voluntarily.
To assess suitability of job applicants for employment.	Names, email addresses, home addresses, phone numbers, career history, personal references.
To approve contractors for engagement on projects.	Names, email addresses, business addresses, phone numbers, insurance and license information, financial, and banking information.
To authorise and record visitors to IVE sites	Names, job titles, phone numbers, email addresses, facial images
To manage our share registry through Automic Registry Services, who collects and holds shareholder information on our behalf	Shareholder information
To manage register of Directors, Company Secretaries and Officeholders	<ul style="list-style-type: none"> • Full name, date of birth, residential address • Contact details (email, phone) • Identification documents (e.g., for ASIC/ASX requirements) • Professional history, qualifications, and declarations • Conflict-of-interest disclosures • Fit-and-proper assessments • Remuneration details • Meeting attendance, committee memberships, performance evaluations • Any information required under the Corporations Act or ASX Listing Rules
To maintain ability to contact relevant support people in an emergency affecting staff members	Names, addresses, email addresses and phone numbers of emergency contacts provided by staff members

3 WHAT PERSONAL INFORMATION WE MAY RECEIVE OR ACCESS AND WHAT WE USE IT FOR

IVE may receive or access personal information as part of the services we provide for our customers. This personal information is collected by our customers or third parties, not by IVE. The type and amount of information involved is determined by each customer or third party provider of the information and is not controlled by IVE.

Types of personal information

Depending on the service and the customer's requirements, personal information may include:

- Contact details such as names, postal addresses, email addresses and phone numbers
- Financial information such as bank account details, credit card information or loyalty program identifiers
- Sensitive personal information, which may include information about health, age or other demographic details

How IVE uses this personal information

IVE uses this personal information only to provide services requested by our customers. This can include:

- Producing and delivering personalised communications on behalf of customers, where content is determined by the customer and delivered through channels such as mail, email, SMS, social media or other digital platforms.
- Inbound scanning services, where IVE receives hard copy communications from our customers which include personal information they have collected. We convert this to digital formats and provide back to our customers
- Working within customer systems or environments, where IVE staff may be given controlled access to personal information for purposes such as executing communications, business analytics or consulting services. In these circumstances, customers determine what personal information IVE can access, how it can be used, and the limits on that access.
- Delivering goods to customers or their customers

Document archiving and hosted services

IVE also provides document archiving and information management services, where customers store business documents and information within applications hosted on IVE's network. These documents may contain personal information relating to the customer's employees, customers or other individuals.

While IVE is responsible for the security, integrity and availability of these systems and networks, customers control the content of the documents and how long the information is retained.

Legal basis for handling personal information

IVE relies on one or more lawful bases when handling personal information, including consent, performance of a contract or order, compliance with legal obligations, and our legitimate interests (where permitted by law).

4 DISCLOSURE AND CROSS-BORDER TRANSFERS

We may disclose personal information to:

- **Service providers and partners** who assist with execution of personalised communication projects on behalf of our customers.
- **Professional advisors and insurers**
- **Banks** in order to process payments to recipients
- **Regulators, law enforcement or courts** where required or authorised by law
- **Related entities and potential purchasers** in the course of corporate reorganisations or sale of business

Some recipients may be located overseas. When we disclose information outside Australia we take reasonable steps to ensure it is protected and managed in ways consistent with this Policy and the APPs, including contractual safeguards where appropriate.

Where we use overseas suppliers to assist in the delivery of electronic communication material on behalf of our customers, we assess their ability to comply with Australian privacy requirements prior to commencement of any work. We confirm their data security capability and gain their acknowledgement of their obligations under the Privacy Act and APPs. We also gain agreement from each customer for use of offshore suppliers.

5 DATA SECURITY AND RETENTION

We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure using administrative, technical, human and physical safeguards appropriate to the sensitivity of the information.

These measures include:

- Robust networks with strong technological defenses in place.
- Use of reputable third-party providers with privacy and security capabilities compatible with IVE's.
- Regular staff training in information security and privacy requirements.
- Secure platforms for receipt and transmission of information.
- Undertaking regular back-ups to ensure availability of information.
- Only retaining personal information as necessary for the purposes described, to meet legal obligations, and carry out normal business activities.

Retention periods vary depending on the type of information and its purpose and include:

- Where we receive personal information from customers to carry out personalised communications projects, or inbound scanning services we use a default retention period of 60 days for personal information held on the IVE network. Hard copy information received for scanning services is either returned to the customer or held in secure storage for an agreed period and then destroyed. This can also be varied via written agreement with individual customers.
- We seek consent from job applicants to retain their personal information for consideration for future work opportunities. Where consent is not provided, this information is deleted.
- We do not use the personal information of contractors or site visitors for purposes other than those disclosed when it is collected, without seeking their consent.
- Retention of information relating to shareholders, Directors, Company Secretaries and Officeholders is governed by ASIC and ASX regulations and statutory obligations.

6 ACCESS, CORRECTION AND COMPLAINTS

You may request access to the personal information we hold about you or request that we correct it. We will respond within a reasonable time and may charge a reasonable fee for access where permitted by law.

Where we have received your personal information from a customer (rather than collecting it directly) you should contact the customer that provided your information to us. We will assist you in this process if required.

If you wish to make a privacy complaint, contact our Privacy Officer (details below). We will investigate and aim to resolve complaints promptly. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC).

7 PRIVACY OFFICER CONTACT DETAILS

All queries should be directed to the Privacy Officer at:

Attention: The Privacy Officer
IVE Group
Locked Bag 555
SILVERWATER NSW 2128 AUSTRALIA

Or by email: privacy@ivegroup.com.au

8 REVIEW OF THIS POLICY

This Policy will be reviewed biennially, unless material changes necessitate an earlier review. Changes will be published on our website with an effective date. Significant changes will be notified to affected individuals where reasonably practicable.

9 DEFINITIONS

- **Personal information** means information or an opinion about an identified individual or an individual who is reasonably identifiable.
- **Sensitive information** is a subset of personal information that includes health, racial or ethnic origin, political opinions, religious beliefs, sexual orientation and the like; we only collect sensitive information when necessary and permitted by law.

Approved by



Matt Aitken
Managing Director

January 2026