ARUP

Potential Recruits Privacy Notice

Asia Pacific (APAC)

January 2026

ARUP

Document Information

Prepared By	Reviewed By	Approved By	Next Review Date
Harry Smith	APAC People Talent Team	Stephanie Emmitt	January 2027

Revision History

Version	Date of Change	Status	Revised By	Summary of Change
1.0	February 2026			Updated to new document format. Minor language changes, additional information added.

ARUP

Contents

ARUP

Potential Recruits Privacy Notice

1. Purpose

Thank you for your interest in working at Arup. This privacy notice sets out how Arup Group Limited and its group companies use your personal information when you apply for a job with us, to join our talent communities or sign up to receive job alerts.

Arup Group Limited, and the group company to which you apply, (together "Arup") will be the "controller" (or equivalent role under applicable data protection laws) of your personal information under relevant data protection laws and will therefore be responsible for the use of your personal information.

To find out how Arup uses personal information generally, please see our website privacy notice.

2. Scope

This notice applies to Arup's career website visitors and individuals engaged in the recruitment process, whether directly with Arup or where you enter our recruitment process via a third party, such as a recruitment agency.

This notice applies when you apply for a role in the Asia Pacific region, including Australia, Mainland China, Hong Kong, Macau, Taiwan, South Korea, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, Thailand and Vietnam. Additional locations may be included where Arup undertakes recruitment activity in the region.

The notice also applies where you join one of our Talent Communities and/or choose to receive notifications about relevant vacancies.

You can view the recruitment section of our website and search for jobs without directly providing any personal information about yourself to us, we do however use cookies on our website that allow certain data to be gathered (e.g. what pages were viewed) when you browse our website (see our cookies policy for further information).

3. How We Acquire Your Personal Data

- When you apply directly for a job or submit your CV/Résumé to us
- When you apply for a job and link the application to your professional networking platform profile
- When you apply for a job via an agency
- Where you create a profile/account on our recruitment website
- Where you register to become a member of our Talent Communities

- Where you sign up to receive notifications about relevant vacancies

The information we may collect includes:

- Name
- Address (including postcode);
- Telephone number;
- Email address;
- Age range;
- Citizenship or residency status;
- Evidence of "right to work" in the country in which you are applying for a role;
- Employment history;
- Qualifications;
- Language spoken; and
- Diversity information such as your gender identity, the gender you were assigned at birth and any disabilities you may have. We use this information to monitor equal opportunities within our business and will not use it during the selection process (this information is not mandatory and is anonymised if you do choose to provide it). All diversity and equality information is held by Arup in strict confidence.

We will also collect any information that you choose to include on your CV or application form. Please do not include any sensitive information in this document, e.g., about racial or ethnic origin, political opinions or affiliations or health.

Where we collect diversity or equality-related information (for example, to support our inclusion initiatives or to comply with local reporting requirements), we only do so where permitted or required by applicable law and, where necessary, with your consent. We use this information in a strictly controlled manner and do not use it to make individual hiring decisions.

4. How We Use Your Personal Data

We will use your personal data for the following purposes:

- to assess your suitability for employment with us and in any subsequent interviewing process. Copies of the information you submit, and any further correspondence will be retained to progress your job application, as a record of our employment and fair access processes; and
- to maintain your profile within our recruitment systems, you can manage your details at any time by logging into your profile, or by emailing at APACprivacy@arup.com

- to send you job alerts of current vacancies. You can update your preferences or deactivate at any time by logging into your profile, or by emailing us at APACprivacy@arup.com

- to manage your Talent Communities membership, you can use the 'unsubscribe' option to stop receiving emails. To update or withdraw your membership, please email us at

APACtalent@arup.com

- For internal research and analysis, for example, on the effectiveness of our recruitment campaigns and methods.

We may use email or telephone to contact you to discuss your application and if you are successful in your application, we may request references from you and their contact information (including name, address and contact number). We will contact your referees to obtain references for you, but we will only do this with your prior permission.

If you are offered a role, then pre-employment checks may also be conducted dependent on the job and location to which you are applying. These will include, but not be limited to, checking your credit history, academic qualifications, and employer references, as well as conducting criminal records checks and address validation, subject always to local law limitations.

Jurisdictional Variations in Pre-Employment Checks:

• Australia: Pre-employment checks may include Australian Federal Police (AFP) checks or state-based police checks and are subject to the requirements of the Privacy Act 1988 (Cth) and relevant spent convictions legislation.

• Singapore: Pre-employment checks are subject to the Personal Data Protection Act and Ministry of Manpower guidelines. Criminal record checks require explicit consent.

• China: Pre-employment checks are subject to the Personal Information Protection Law and Labour Contract Law. Background checks are typically conducted through authorized agencies.

• New Zealand: Criminal record checks are subject to the Criminal Records (Clean Slate) Act 2004 and the Privacy Act 2020.

• Malaysia: Pre-employment checks are subject to the Personal Data Protection Act 2010 and Employment Act 1955.

• Other APAC jurisdictions: We observe and follow local requirements regarding the scope and conduct of pre-employment checks.

4.1 Talent Communities:

You can register your interest in future vacancies with Arup by accepting an invitation to join one of our Talent Communities. The information we collect through the online registration process is determined by the talent community you are interested in joining.

You can update your Talent Community details as you progress through your career, or if you no longer wish to be a member by email us at APACtalent@arup.com

4.2 Job Alerts

Register for job alerts to be informed of vacancies in desired sectors and locations. We will use the preferences you have specified to send details of matching vacancies to your registered email address. You can update your job alert requirements and manage your preference to receive or not receive these alerts in your profile.

5. Special Category Data

During the application process, we ask you to provide us with special category information for diversity monitoring purposes as described above. Providing this information is completely voluntary, and it is not used during the selection process. Where you supply it, the information is anonymised and aggregated to enable us to obtain measurable data.

Special categories of personal data include details relating to your health, race, or ethnic background, medical, sex and gender. Beyond the diversity section we ask you not to provide any special category information to us unless we specifically ask you to, for example, where we seek to make reasonable adjustments to facilitate an interview for individual needs.

Jurisdictional Note on Special Category Data:

The definition and treatment of special category or sensitive personal data vary across APAC jurisdictions:

- Australia: Under the Privacy Act 1988 (Cth), "sensitive information" includes information about racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal records, and health information. Collection requires consent unless an exception applies.

- Singapore: The Personal Data Protection Act requires organizations to obtain consent before collecting, using or disclosing sensitive personal data, and to notify individuals of the purposes for which the data is collected.

- China: The Personal Information Protection Law classifies certain data as "sensitive personal information" including biometric data, religious beliefs, health information, financial accounts, and location tracking. Separate consent is required for processing such data.

- New Zealand: The Privacy Act 2020 does not have a separate category for sensitive information but imposes general privacy principles on all personal information collection and use.

- Malaysia: The Personal Data Protection Act 2010 defines "sensitive personal data" to include information relating to physical or mental health, political opinions, religious beliefs, and criminal convictions.

6. Lawful Basis for Processing

Depending on your location and applicable data privacy legislation, we may process your personal/special category data for one or more or of the following purposes:

- You have consented to the processing, or,
- We have a legitimate interest in doing this (such as contacting you with details of relevant vacancies and telling you how your application is progressing), or
- We must do so by law, or

- We need to do this to enter a contract with you or so we comply with such a contract, or
- You have received notification (this notice) detailing how your personal data will be used.

Jurisdictional Variations in Legal Basis:

- Australia: Under the Privacy Act 1988 (Cth), we primarily apply Australian Privacy Principles 3 (collection), 6 (use and disclosure), and consent where required for sensitive information.

- Singapore: Under the Personal Data Protection Act, we apply consent, contractual necessity, or legitimate interests (where applicable under the Act).

- China: Under the Personal Information Protection Law, we apply consent, contractual necessity, or legal obligations. Separate consent is required for sensitive personal information.

- New Zealand: Under the Privacy Act 2020, we apply collection principles and lawful purposes for processing.

- Malaysia: Under the Personal Data Protection Act 2010, we primarily apply consent, with some exceptions for processing necessary for entering or performing a contract.

- Other APAC jurisdictions: We observe and follow the specific legal basis required under applicable local data protection laws.

Where we rely on your consent as the basis for processing your personal information, you may withdraw that consent subject to applicable law. If you do withdraw consent, we will no longer rely on it for future processing, but this will not affect the lawfulness of processing that took place before the withdrawal.

7. Sharing Your Personal Data

When you apply for a job with Arup, your application will be processed by the Arup recruiting team and Arup group company situated in the country in which you are applying to work. Your details will also be accessible to recruiting teams in other Arup locations.
We may use people or companies outside of the Arup Group to provide services as part of the recruitment process.
We make sure that all our Third-party suppliers have appropriate security in place to protect your personal data in line with our standards.

We may also share your personal data with other organisations when required by law, to prevent or detect crime, or to protect someone's rights, property, or safety. These organisations include the police, law enforcement agencies, and fraud prevention agencies.

Third parties with whom we may share your personal data include:

• Arup Group Companies globally
• Recruitment agencies and talent acquisition service providers
• Background check and verification service providers

• Occupational health professionals (where pre-employment health assessments are required)
• IT service providers supporting our recruitment platforms
• Professional advisers (including lawyers and auditors)
• Government agencies and regulatory authorities (where required by law)

All third-party service providers are required to maintain appropriate security measures and confidentiality obligations in accordance with applicable data protection laws.

8. Cross Border Data Transfers

Arup has operations throughout the world. As such, the personal information that we hold may be transferred to, and stored at, a country outside of your country of residence, including countries outside of the APAC region.

We apply the appropriate level of safeguards required by the laws of the country your data originates from. Transfers are protected either by formal safeguards or supported by specific local law provisions for legitimate business operations. The legal mechanisms for transferring personal data in relation to the recruitment process vary by jurisdiction.

Additionally, where we use service providers that are based outside of your country of residence; we will ensure that any such service provider complies with strict obligations of confidentiality and security.

We will ensure that binding legal agreements and/or appropriate safeguards are in place.

9. Data Retention

Career Profile/Account

We take all reasonable steps to retain personal information only for as long as we need to process your job application. We may retain your details after a decision has been reached regarding your suitability for current jobs in case alternative vacancies become available in the future.

Arup provides career pathway options for both early careers and experienced hires. Our internship and other early careers processes often span academic years. For early careers candidates we will retain your data for a maximum of 2 years, for experienced hire candidates, for a maximum of 1 year.

You may deactivate your careers account or withdraw from the process at any time by logging into your profile. Please be aware that personal data, limited to name and contact details, may be held within our recruitment administration and tracking records and will be deleted in line with our retention processes.

Talent Community

Accounts are deleted where you do not reconfirm consent after 1 year of inactivity, as we understand that your job seeking requirements are likely to have changed at this time. If you would like to update talent community details, for example, your experience and/or qualifications please contact APACtalent@arup.com

Talent Community /Job Alert Emails

We will ask you to confirm your consent again after 1 year. If you do not provide permission for us to continue, you will no longer receive these types of email communications.

10. Security

We are committed to ensuring that any personal information you provide to us when applying for a job is kept secure and any details you give us remain confidential.

Please ensure that you keep your password and profile login details confidentially and do not share them with anyone. Please contact us at APACprivacy@arup.com if you believe that your candidate profile account may have been compromised.

11. Your Rights

As a Data Subject, you may have the following rights under the Data Protection Laws:

- the right of access to Personal Data relating to you;
- the right to have the Processing of your Personal Data restricted;
- the right to object to the Processing of your Personal Data;
- the right not to be subject to decisions based solely on automated Processing of your Personal Data;
- the right to have inaccurate Personal Data corrected;
- the right to have Personal Data erased.

Jurisdictional Variations in Rights:

The availability and scope of these rights vary across APAC jurisdictions:

Australia: Under the Privacy Act 1988 (Cth), you have the right to:

• Access your personal information
• Correct inaccurate or incomplete personal information
• Make a complaint about privacy breaches

Note: The rights to erasure, data portability, and restriction of processing are not generally available under Australian privacy law, except in specific circumstances.

Singapore: Under the Personal Data Protection Act, you have the right to:

• Access your personal data

• Correct inaccurate or incomplete personal data
• Withdraw consent (though this does not affect the lawfulness of processing prior to withdrawal)
• Data portability (for data provided with consent or under a contract, in certain circumstances)

China: Under the Personal Information Protection Law, you have the right to:

• Access to your personal information
• Correction of inaccurate or incomplete personal information
• Deletion of personal information in specified circumstances
• Data portability
• Withdrawal of consent
• Right to request explanation of personal information processing rules
• Right to refuse automated decision-making in certain circumstances

New Zealand: Under the Privacy Act 2020, you have the right to:

• Access your personal information
• Request correction of personal information
• Object to certain types of processing

Malaysia: Under the Personal Data Protection Act 2010, you have the right to:

• Access your personal data
• Request correction of personal data
• Withdraw consent for processing
• Limit processing of personal data

Other APAC jurisdictions: Rights vary by jurisdiction. Please contact the APAC Privacy Team for information specific to your location.

How to Exercise Your Rights:

To exercise any of your rights, please contact us at:

• Email: APACprivacy@arup.com
• For Early Careers specific queries: APACtalent@arup.com

We will respond to your request within the timeframe required by applicable, typically 30 days but this varies by jurisdiction.

12.Automated Decision-Making

Currently, Arup does not make solely automated decisions that produce legal effects or similarly significantly affect candidates without human intervention. Where we use automated tools to assist in the recruitment process (such as application tracking systems or initial screening tools), these operate with human oversight and review.

Final decisions regarding your application are always made by human recruiters and hiring managers.

If you have concerns about any automated processing that affects you, please contact us at APACprivacy@arup.com

13. Delete your careers account

If you wish to withdraw an application for a specific role, please access your candidate profile and follow the relevant steps. This will not delete your personal information, just the specific application.

If you wish to delete your account, select "My Profile" > Select "Delete profile". Please note that the account deletion will instigate the following actions:

• Any applications are set to "Removed at candidate's request"
• Any offers are set to "withdrawn"
• Any interviews are set to "withdrawn"
• The profile is disabled, archived, and marked for permanent deletion (This deletion should happen within 48 hours and cannot be undone)
• You will be logged out of the candidate portal

Please be aware that personal data, limited to name and contact details, may be held within our recruitment administration and tracking records and will be deleted in line with our retention processes.

14. Contact

If you have any questions about your personal data, you can contact our APAC Privacy Team at the following address:

Harry Smith, APAC Data Privacy Manager
APACprivacy@arup.com

Stephanie Emmitt, Global Data Privacy Manager
privacy@arup.com

Supervisory Authorities and Complaint Mechanisms:

You have the right to complain to the applicable supervisory authority if you believe we have not met our legal duties, but please speak to us first so we can attempt to address your concerns.

Australia:
Office of the Australian Information Commissioner (OAIC)
Website: https://www.oaic.gov.au/
Complaint portal: https://www.oaic.gov.au/privacy/privacy-complaints

New Zealand:
Office of the Privacy Commissioner
Website: https://www.privacy.org.nz/
Complaint portal: https://www.privacy.org.nz/your-rights/making-a-complaint/

Singapore:
Personal Data Protection Commission (PDPC)

Website: https://www.pdpc.gov.sg/
Complaint portal: https://www.pdpc.gov.sg/Help-and-Resources/How-to-Comply/If-You-Have-a-Data-Protection-Query-or-Complaint

Indonesia:
Ministry of Communication and Informatics (KOMINFO)
Website: https://www.kominfo.go.id/

Malaysia:
Personal Data Protection Commissioner
Jabatan Perlindungan Data Peribadi (JPDP)
Website: http://www.pdp.gov.my/
Email: pdpa@pdp.gov.my

Indonesia:
Ministry of Communication and Informatics (KOMINFO)
Website:

Mainland China:
Cyberspace Administration of China (CAC)
Website: http://www.cac.gov.cn/
For complaints, please contact your local network information department or the CAC through official channels.

Hong Kong:
Office of the Privacy Commissioner for Personal Data (PCPD)
Website: https://www.pcpd.org.hk/
Email: communications@pcpd.org.hk

Japan:
Personal Information Protection Commission (PPC)
Website: https://www.ppc.go.jp/
Email: https://www.ppc.go.jp/news/opinion/

Macau:
Office for Personal Data Protection, Macao (GPDP)
Website: https://www.gpdp.gov.mo/

Philippines:
National Privacy Commission (NPC)
Website: https://www.privacy.gov.ph/
Email: info@privacy.gov.ph

South Korea:
Personal Information Protection Commission (PIPC)
Website: https://www.pipc.go.kr/
Email: webmaster@pipc.go.kr

Taiwan:
Personal Data Protection Commission (PDPC)
Website: https://www.ndc.gov.tw/en/

Thailand:
Personal Data Protection Committee (PDPC)
Ministry of Digital Economy and Society
Website: https://www.mdes.go.th/

Vietnam:
Department of Cybersecurity and High-Tech Crime Prevention
Ministry of Public Security (MPS)
Website: https://mps.gov.vn/

Other jurisdictions: For information on complaint mechanisms in other APAC countries/locations where Arup operates, please contact the APAC Privacy Team APACprivacy@arup.com.

Changes to This Notice

Any changes to this privacy notice will be posted here, so please check back regularly when you visit this website. The date of the most recent revision will be indicated at the top of this notice.

We appreciate your interest in joining Arup.