

Third-Party Privacy Notice - Mainland China

1. Purpose and Scope

In the regular course of business, AECOM, its subsidiaries and affiliates (collectively, "AECOM") acquires Personal Information by interaction and communication with potential, current or past job applicants, alumni, talent networks, clients, vendors, contractors, sub-contractors and other third parties. AECOM takes seriously its obligations to protect such Personal Information. As evidence of its commitment to privacy, AECOM has established this Privacy Notice about how AECOM collects, uses, processes and stores your Personal Information.

AECOM will only process your Personal Information in accordance with this Privacy Notice unless otherwise required by applicable law. The organization takes steps to ensure the Personal Information collected about you is adequate, relevant, not excessive, and processed for limited purposes.

This Privacy Notice does not cover aggregate data, data rendered anonymous or data that has been deidentified. Aggregate data relates to a group or category of individuals, from which individual identities have been removed. Data is rendered anonymous if individual persons are no longer identifiable. Deidentified data is data that has had identifiable elements removed, and cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual.

You are under no obligation to provide Personal Information to AECOM. However, if you do not provide the information, AECOM may not be able to provide the requested service to you.

We may revise this Privacy Notice from time to time, and when we do so, we will update the "Revision" date. If we make material changes to this Privacy Notice, we will notify you by email or by posting a notice on our website and we will obtain your consent again, if required by applicable law. We encourage you to periodically review this Privacy Notice to stay up to date on our privacy practices.

2. Privacy Notice

When you choose to contact us, sign up for newsletters, visit our website, apply for employment, submit a bid or tender, become a supplier, vendor, or subcontractor, or otherwise engage with us, we will process some Personal Information about you. We may also receive your Personal Information through clients for purposes of conducting surveys or collecting your opinion concerning certain projects.

Based on your interaction and relationship with us, as described above, we process your Personal Information for the following purposes:

1. Communicate with you, or inform you about products or services, consistent with your choices.
2. Communicate with alumni, talent networks, job applicants, clients, vendors, contractors, sub-contractors and other third parties concerning AECOM employment opportunities, projects and business operations.
3. To review your education, qualifications, and past and current job experience.
4. To verify identity and administer background/clearance checks, right-to-work checks, legal due diligence/anti-corruption screening, denied or restricted party screening, quality reviews, and occupational health and safety standard checks.
5. Incident response and emergency communications.
6. Recording of working time and timesheet records for contractors and sub-contractors.
7. Administration of safety and protection of our employees, resources, and workplaces.

8. Invoicing and payment for services.
9. Accounting/government tax and auditing business purposes for vendors, contractors and sub-contractors.
10. Administration of equal opportunities monitoring or meeting requirements for reporting on diversity and equality.
11. System access and authentication.
12. Administration of safety and protection of AECOM systems for recording and monitoring network activity for the purpose of identifying, predicting, and preventing the entry of malicious activity onto or the release of Data from AECOM network and computing resources.
13. Reporting of worksite safety incidents or Occupational Health surveillance requirements related to individual's functional ability and fitness for specific work, with any advised restrictions, and to make reasonable adjustments based on disability.
14. To administer quality, safety and compliance checks and reviews to qualify third party contractors for performing work in accordance with applicable quality standards such as ISO 9001 and NQA-1, including use of individuals who are required to maintain specific qualifications or certifications.
15. To manage our business, comply with our legal obligations, resolve disputes, or enforce our agreements.
16. Identification purposes for physical site access security and administration to ensure access to correct areas are granted for customer staff, vendors, contractors, and subcontractors.
17. As otherwise stated at or about the time your Personal Information is collected from you.

Table 1 lists the categories of Personal Information AECOM may collect and process about you based on the requirements stated herein.

Table 1. Personal Information Collected and Purpose for Collection

Ways of Processing	Personal Information Processed	Purposes for Processing Personal Information
'Contact Us' website form submission, emailing us directly, or signing up for email communications	Name, email address, phone number, and other voluntary data	The above-described purposes: 1, 17
Job outreach campaigns Resume submission, career or job inquiry	Name, email address, mailing or home address, telephone number, qualifications, education, experience	The above-described purposes: 1, 2, 3, 17
Pre-hire of staff and business partners	Name, email address, mailing or home address, telephone number, date of birth, social security number or national identification, nationality, citizenship, immigration status, country of birth, photograph/facial recognition, references, credit or criminal background checks	The above-described purposes: 1, 3, 6, 13, 14, 15, 17
Post-hire/onboarding of staff and business partners	Name, email address, mailing or home address, telephone number, date of birth, tax identification number, social security number or national identification, nationality, citizenship, immigration status, gender, country of birth, photograph, fingerprint scanning, emergency contacts/next-of-kin, banking information, username and password, and where applicable:	The above-described purposes: 1, 3, 4, 6, 7, 8, 10, 11, 13, 14, 15, 17

Ways of Processing	Personal Information Processed	Purposes for Processing Personal Information
	automobile insurance and/or professional liability insurance.	
Worksite incident or safety reporting	Name, email address, telephone number, medical or incident details	The above-described purposes: 12, 14, 15, 17
Physical site access administration	Name, email address, telephone number, National Identification Number, photo	The above-described purposes: 5, 7, 16, 17

Some of the types of information set out above may constitute Sensitive Personal Information. It is necessary for us to process your Sensitive Personal Information for the purposes described in this notice. We will only process Sensitive Personal Information only if strict protection measures are put in place and there is sufficient necessity to justify the processing.

AECOM may need to collect Sensitive Personal Information. Where required under applicable local law, such Sensitive Personal Information will be processed with consent. Where required by applicable local law, consent to transfers or uses of Sensitive Personal Information will be opt-in

3. How Data is Collected

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

- a. **Direct Interactions:** You give us your Personal Information when contacting us through candidate profiles, through interviews, or in response to surveys, jobs, projects, bids, through quality and compliance questionnaires, proposals or other means. This includes Data you provide when you submit your CV/resume or contact details through our website, email, and via our alumni or talent networks.
- b. **Third Parties or Publicly Available Sources:** AECOM may obtain Personal Information about you from a representative of your company (if we are sub-contracting services), publicly available online records, background check providers, criminal records check, or past or current professional references you supply to us. The organization will seek Personal Information from third parties only once a job offer, or business opportunity has been made, and will inform you or your company representative that it is doing so.

We do not undertake automated decision making or profiling on Personal Information or Sensitive Personal Data.

4. Legal Basis for Processing

For AECOM to process Personal Information we must have a lawful basis for doing so and at least one of the following must apply:

- a. **Consent:** an individual must give clear consent for us to process their Personal Information and then only for a specific purpose.
- b. **Contract:** the processing is necessary for a contract that AECOM has with an individual, or because we have asked the individual to take specific steps before entering into a contract.
- c. **Legal Obligation:** the processing is necessary for AECOM to comply with the law.
- d. **Vital Interests:** processing is necessary to protect someone's life.
- e. **Public Information: where you have publicly disclosed your** Personal Information and it is used for processing within a reasonable scope.

5. Minimum Necessary Collection and Use

AECOM adheres to the following guidelines to ensure that its collection of Personal Information is fair and lawful. Specifically, AECOM:

- a. Collects only as much Personal Information as is required by law or needed for reasonable and legitimate business purposes.
- b. Collects Personal Information in a non-deceptive manner.
- c. Where appropriate, informs individuals which Personal Information is required, and which is optional at the time of collection.
- d. Collects Personal Information from individuals consistent with local legal requirements.

6. Use and Retention

AECOM uses, stores, retains, and otherwise processes Personal Information only for reasonable business purposes and for only as required for that business purpose or as authorized.

AECOM does not disclose Personal Information to third parties for direct marketing purposes, nor does it sell Personal Information. Processing of Personal Information will comply with contractual, regulatory, and local legal requirements.

AECOM stores and destroys Personal Information based on AECOM data retention policies and procedures. AECOM retains the data for as long as it serves the purpose of processing for which it was collected or subsequently authorized.

Job candidates may remove their profile at any time through the AECOM Careers website or by sending a request to the Privacy Office at privacyquestions@aecom.com.

7. Data Privacy Rights

AECOM uses, stores, retains, and otherwise processes Personal Information only for reasonable business purposes and for only as required for that business purpose or as authorized.

AECOM does not disclose Personal Information to third parties for direct marketing purposes, nor does it sell Personal Data. Processing of Personal Information will comply with contractual, regulatory, and local legal requirements.

AECOM stores and destroys Personal Information based on AECOM data retention policies and procedures. AECOM retains the data for as long as it serves the purpose of processing for which it was collected or subsequently authorized.

- a. **The right to request access.** You have the right to request AECOM for copies of your Personal Information.
- b. **The right to request rectification.** AECOM relies on you to ensure the information you provide to AECOM about you is accurate, complete and current. If any Personal Information is inaccurate or incomplete, you may request that your Personal Information be corrected or completed. AECOM will correct or delete Personal Information as required by applicable law. You may also request to correct, amend, or delete Personal Information that has been processed in violation of applicable data protection law.
- c. **The right to request erasure.** You have the right to request AECOM delete your Personal Information under certain conditions.
- d. **The right to withdraw consent.** Where you have provided written consent (or positive opt-in) to the collection, processing, or transfer of Personal Data, you may have the legal right to withdraw consent. Where we have processed your Personal Information with written consent (or positive opt-in), you can withdraw that consent at any time. Note - withdrawing consent will not affect the lawfulness of any processing we conducted prior to

withdrawal nor will it affect the processing of the Personal Information conducted in reliance on a lawful basis other than consent.

- e. **The right to request portability.** You have the right to request AECOM transfer your Personal Information that we have collected to another organization, or directly to you, under certain conditions.
- f. **The right to restrict processing.** You have the right to request that AECOM restrict the processing of your Personal Data, under certain conditions.
- g. **The right to opt-out of email marketing.** You can opt-out of email marketing communications at any time by selecting the email's "Opt-out" or "Unsubscribe" link, or following the instructions included in each email subscription communication.
- h. **The right to file a complaint.** If you consider that your privacy rights have not been adequately addressed, you have the right to submit a complaint to the AECOM [Privacy Office](#) or with the supervisory authority in your country of residence.

You can submit a request to exercise these data privacy rights to the AECOM Privacy Office at privacyquestions@aecom.com. AECOM will request specific Personal Information to help confirm identity and rights.

AECOM will not discriminate against individuals for exercising any of their privacy rights allowed or required by applicable data protection law or regulation.

8. Sharing and Onward Transfer

AECOM shares Personal Information in the following ways:

- a. **Affiliates:** AECOM shares information among AECOM subsidiaries and affiliates for the purposes described in this Privacy Notice where consistent with applicable legal requirements.
- b. **Third-Party Suppliers:** AECOM shares Personal Information to selected affiliated or trusted third party suppliers to perform services on behalf of the organization. These trusted third-parties include, but are not limited to Data Technology Providers, Cloud Providers, Data Hosting Services, Denied and Restricted Party Screening Providers, Background Check Providers, and Data Storage Providers.
- c. **Clients:** AECOM shares certain Personal Information as part of our professional services under contract to our clients, including governmental agencies, for project-related work, security clearances or as required by security protocols.
- d. **Other Third Parties:** AECOM discloses certain Personal Information to other third parties:
 - i. where required by law or legal process (e.g., to tax and social security authorities);
 - ii. where AECOM determines it is lawful and appropriate;
 - iii. to protect AECOM's legal rights (e.g., to defend a litigation suit or under a government investigation or inquiry) or to protect its employees, resources, and workplaces; or
 - iv. in an emergency where health or security is at stake.
- e. **Public Security/Law Enforcement:** AECOM may be required to disclose Personal Information in response to lawful requests by public authorities, including meeting national security or law enforcement requirements.

These third parties provide hosting and other services for the Company and otherwise process your information for purposes that are described in this Privacy Notice or notified to you when we collect your Personal Information. If you want to know more information about these third parties, you may contact privacyquestions@aecom.com.

AECOM is a global company, with offices, Clients, and Suppliers located throughout the world. As a result, Personal Information may be transferred to other AECOM offices, data centers, and servers in Europe, Asia, South America, or the United States for the purposes identified. Any such transfer of Personal Information shall take place only under applicable law and/or the use of Standard Data Protection Clauses and data protection agreements, or other transfer mechanism as required by applicable law.

AECOM will take steps designed to comply with all applicable local laws when Processing Personal Data, including any local law conditions for and restrictions on the transfer of Personal Data.

AECOM may also protect data through other legally valid methods, including international data transfer agreements or Standard Contractual Clauses that have been recognized by the relevant Data Protection Authorities as providing an adequate level of protection to the Personal Information we process globally.

AECOM will ensure all transfers of Personal Information are subject to appropriate safeguards as defined by data protection laws and regulations.

9. Data Security

AECOM has adopted and maintains reasonable and appropriate Data security policies, processes and/or procedures to safeguard Personal Information from loss, misuse, unauthorized access, disclosure, alteration, destruction, and other Processing. However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. As such, we cannot promise, ensure, or warrant the security of any Personal Information that you may provide to us.

AECOM's Data security processes provide for the classification of data and the assignment of protection requirements and security controls based on the classification. The safeguards used to protect Personal Information is commensurate with the level of risk involved.

10. Exceptions

Under certain limited or exceptional circumstances, AECOM may, as permitted or required by applicable laws and regulations, process Personal Information without providing notice, access or seeking consent. Examples of such circumstances may include investigation of specific allegations of wrongdoing, violation of company policy or criminal activity; protecting employees, the public, or AECOM from harm or wrongdoing; cooperating with law enforcement agencies; auditing financial results or compliance activities; responding to court orders, subpoenas or other legally required disclosures; meeting legal or insurance requirements or defending legal claims or interests; satisfying labor laws or agreements or other legal obligations; collecting debts; protecting AECOM's Data assets, intellectual property and trade secrets; in emergency situations, when vital interests of the individual, such as life or health, are at stake; with respect to access requests, where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or the privacy interests of others would be jeopardized; and in cases of business necessity.

11. Complaints and Questions

If you feel that your rights have not been adequately addressed, you have the right to submit a complaint to the AECOM Privacy Office: privacyquestions@aecom.com or with the supervisory authority or regulator in your country of residence. You may click [here](#) to find your country regulator.

If you have any questions about this statement or our handling of personal Data, please contact the Privacy Office by e-mail at privacyquestions@aecom.com.

12. Terms and Definitions

- a. Data Privacy means the legal rights and expectations of individuals to control how their Personal Information is collected and used.
- b. Personal Information means any information relating to describing, reasonably capable of being associated with, or capable of reasonably being linked, directly or indirectly, to an identified or identifiable natural person.
- c. Processing any operation or set of operations that are performed upon Personal Information, whether by automatic means or otherwise. This includes the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, disclosure

by transmission, dissemination or making available in any other form, linking, alignment or combination, blocking, erasure or destruction of Personal Information.

- d. Sensitive Personal Data sensitive information includes Personal Information that, if leaked or if used illegally, is likely to cause harm to a natural person’s personal dignity or endanger his/her personal safety or the safety of his/her property, including information such as biometric identifiers, religious faith, particular identities, medical care and health, financial status, and location tracking, as well as Personal Information of minors under the age of 14.

13. Change Log

Rev #	Change Date	Description of Change	Location of Change
0	30-Nov-2021	Initial release as L3AS(CN)-007-PL2	