AECOM

AECOM Global

Recruitment Privacy Notice Policy

L1-007-PL7

1. Purpose

a. AECOM takes its recruitment candidate's privacy seriously. Please read this privacy notice ("Notice") carefully as it contains essential information on how and why AECOM and its subsidiaries and affiliates (collectively, "AECOM", "Company", "we", "us" and "our") Process your Personal Data.

b. The "data controller" is the AECOM company based in the country where the position you applied for is located. Company details, including postal addresses can be found: here.

c. *Additional information for residents of certain jurisdictions*: For persons in the EU / UK, and residents of Brazil, California, Thailand, Kingdom of Saudi Arabia, Mainland China, Singapore, Australia and Hong Kong SAR, we provide additional information as required by local law; please review the following sections of our Notice that apply to you:

i. Section 14.1: Persons in the EU / UK
ii. Section 14.2: Brazil Residents
iii. Section 14.3: California Residents
iv. Section 14.4: Thailand Residents
v. Section 14.5: Kingdom of Saudi Arabia Residents
vi. Section 14.6: Mainland China Residents
vii. Section 14.7: Singapore Residents
viii. Section 14.8: Australia Residents
ix. Section 14.9: Hong Kong SAR Residents

d. Within the context of this Notice, "Personal Data" means any information relating to an individual who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier. If you do not provide the Personal Data requested, you may not be able to continue going through our recruitment process. We will notify you where this applies to you.

e. As a global company, we may Process Personal Data from around the world and have included some extra country-specific information in Section 14 of this Notice.

f. Refer to AECOM.com for this Notice in other languages.

2. How might we collect your Personal Data?

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

a. **Direct Interactions**: You give us your "Personal Data" when contacting us through phone, email, web forms or other means.

b. **Third Parties or Publicly Available Sources**: Subject to applicable law, AECOM may also obtain information about you from publicly available online professional organizations, social media, other networking platforms (e.g., LinkedIn, ZoomInfo), recruiters, references from a previous employer, business partners, sub-contractors providing recruiting or technical services, analytics providers, and background check and search information providers. We may also retain that "Personal Data" after you have been employed (where this is relevant and to the extent permitted by applicable law) which is addressed in our Employee Privacy Notice – AECOM Global. We may also receive information (which may include your "Personal Data") from our hiring manager, from our human resources staff, and, from time to time, from our other employees (for instance, in the course of conducting an interview).

c. **Combining "Personal Data" from Different Sources**: We may combine the "Personal Data" we receive from various sources with "Personal Data" we collect from you and use it as described in this Notice.

3. What Personal Data We Use and Why

a. The "Personal Data" requested from you during the recruitment process is required by us in order to assess your application for employment with us. If you do not provide some or all of this "Personal Data" it may affect our ability to process your application and therefore to offer you employment. In some cases, it may mean that we are unable to continue with your application for employment as we will not have the "Personal Data" we believe to be necessary for the effective and efficient management of the recruitment process.

b. The tables throughout this Notice identify "Personal Data" AECOM may collect. AECOM will not necessarily process all the data listed below about you, and some of the purposes for processing will overlap and there may be several purposes which justify our use of your "Personal Data".

c. In addition to the "Personal Data" identified in the table in Section 3.1, please note the following additional information:

Special categories (Sensitive Personal Data)

Certain "Personal Data" may be regarded as "Special Category" Personal Data under applicable data privacy laws, e.g. certain "Personal Data" about religion or health. Any such "Personal Data" must be handled with extra care and requires additional protective measures. AECOM will only process Special Category Personal Data if AECOM has a lawful basis to process such "Personal Data", which may require us to obtain your explicit consent to process such data. In such cases, AECOM will inform you and (if required by law to do so) seek your explicit consent to process such data.

3.1 For Job Candidates that Apply for Jobs or Candidates We Source from Online Sources

a. Subject to applicable law, AECOM collects "Personal Data" from you in connection with your resume and the application you submit to us when applying for a job. We use your information to evaluate your skills and abilities for job opportunities, verify your information, carry out reference checks and/or background checks (where applicable), communicate with you about the recruitment process, recommend potential career opportunities at AECOM, creating and/or submitting reports as required under applicable laws/regulations, and making improvements to AECOM's application or recruitment process.

b. If your application is unsuccessful, we may ask you if you would like your "Personal Data" that we have collected during the recruitment process to be kept on file. If you say yes, we will proactively contact you should any further suitable vacancies arise. Our lawful basis for this processing will be that you have provided your consent to this. You can withdraw your consent at any time, by contacting us.

Stage 1: Up to and including Shortlisting

How will we use and may share your "Personal Data" ('purpose')?	The information we use ("Personal Data")	How we get your information?	Why we collect the information
• Enabling registration of candidates in AECOM's recruitment systems. • To enable recruitment personnel or the hiring manager to contact candidates to progress applications, arrange interviews and inform outcomes. • General administration of job applications.	• Your name and contact details (i.e., address, home and mobile phone numbers, email address).	• Directly from you	• Legitimate interest: to carry out recruitment. • Legitimate interest: to progress candidate applications, arrange interviews and inform outcomes.

How will we use and may share your "Personal Data" ('purpose')?	The information we use ("Personal Data")	How we get your information?	Why we collect the information
• Enable recruitment team and hiring manager to assess and verify skills and qualifications to make an informed short list or recruitment decision. (Note: individual making shortlisting decision receives pseudonymized or anonymized details only.)	• *Employment, education history and background information* – resume, Curriculum Vitae, educational history, academic degrees and qualifications, certifications, skills, work history, professional background, • Performance, behavioural, skills, analytical and evaluation assessments, and tests in connection with recruitment screening and processes. • *Electronic and voice communications data such as a r*ecord of our contact with you, including interviews, assessment results, and disposition through all applicable communication channels, including email, text, instant message or chat, transcriptions and/or telephone communications, voice recordings, and video recordings.	• Directly from you	• Legitimate interest: to carry out recruitment process. • Legitimate interest to make an informed decision to shortlist for an interview or to recruit.
• To find qualified potential candidates to invite them to apply to AECOM job opportunities. • General recruitment and candidate administration.	• Publicly available information on job portals, professional websites, or social media (e.g., contact information, work and education history, professional affiliations, and certifications).	• Publicly available sources, such as LinkedIn public profiles. • Job Placement Agencies • Job Boards	• Legitimate interest (to communicate with prospective candidates and increase candidate pool). • Candidate consent
• To check whether criminal convictions or driving history would prevent us from offering you employment. • To enable recruitment team members and management to make informed recruitment decisions. • To carry out statutory background checks. • Information shared with regulatory authorities.	• Criminal record, driving history.	• Background check screening services • Denied party screeners, such as MK Denial	• Legitimate interest (to assess candidates) • Legitimate interest (recruitment screening) • Legitimate interest (fleet safety and safe driving requirements) • Legal obligations • Candidate consent
• Enabling the use of and communication through AECOM's recruitment system.	• IT-related data, such as e-mail and password for the recruitment system including automatic messages and other communication.	• Direct from you.	• Legitimate interest (to manage applications)

How will we use and may share your "Personal Data" ('purpose')?	The information we use ("Personal Data")	How we get your information?	Why we collect the information
• To carry out equal opportunities monitoring, analyze our recruitment practices, support our efforts to create and maintain a diverse workforce and produce diversity statistics. • To provide work-related accommodations or adjustments; and	• *Demographic Data** – such as gender, ethnicity, race, disability status, gender identity, transgender status, sexual orientation, and religion. * AECOM processes demographic data for a variety of reasons, and this will vary in our different jurisdictions. Our reasons for collecting this data will be disclosed at the time of request. Where the processing of demographic data is not required by law, we will ask for your express consent.	• Direct from you.	• Legal obligation (laws that require us to carry out and report on equal opportunities monitoring and/or consider reasonable adjustments in the workplace.) Otherwise, we only process this "Personal Data" with your consent*. * If you choose to consent, you can withdraw this at any time, by contacting us.
• Dealing with queries or complaints relating to the recruitment process. • Asserting or managing any kind of claims that we may bring or that may be raised against us.	• Employment, education history and background information – resume, Curriculum Vitae, educational history, academic degrees and qualifications, certifications, skills, work history, professional background, credit history, driving history, criminal records, and other information revealed during background screenings (where allowed by law). • Performance, behavioural, skills, analytical and evaluation assessments, and tests in connection with recruitment screening and processes. • Electronic and voice communications data such as a record of our contact with you, including interviews, assessment results, and disposition through all applicable communication channels, including email, text, instant message or chat, transcriptions and/or telephone communications, voice recordings, and video recordings.	• Direct from you • From recruitment or management team	• Legitimate Interest

Stage 2: Pre-final Decision to Recruit

How will we use and may share your "Personal Data" ('purpose')	The information we use ("Personal Data")	How we get your information	Why we collect the information
• To collect reference about you. • To comply with legal or regulatory requirements. • Shared with management and HR personnel to make hiring decisions.	• Information about previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time, and attendance, from references obtained about you from previous employers and/or education providers.	• References provided by you.	• Legitimate Interest: to make an informed decisions to recruit. • Legal obligations. • Legitimate Interest: to maintain employment records.
• To make recruitment decisions and carry out statutory checks. Information may be shared with regulatory authorities to carry out such checks.	• Information regarding criminal records, criminal records certificates, and enhanced criminal records certificates.	• Background screening services.	• To perform the employment contract. • Legal obligations. • Legitimate interest: verification of information.
• To carry out right to work checks. • Shared with HR personnel and other authorized personnel.	• Nationality, immigration status, passport information, immigration information, and other government identification.	• Directly from you.	• To perform the employment contract. • Legal obligations. • Legitimate interest: to maintain employment records.
• To ensure candidates applying for roles that require driving for the company have a valid driver's license and have a clean driving record. May be shared with the Company's insurer.	• A copy of your driver license.	• Directly from you.	• To perform the employment contract. • Legal obligations. • Legitimate interest: to ensure driver safety and reduce accidents.
• Enabling assessment of the candidate's health status (if needed for specific positions or other reasons)	• Health data, such as health examinations, drug & alcohol tests, and medical certificates	• Health clinic • Drug/Alcohol screeners.	• Candidate consent
• To carry out right to work checks. • To check and confirm citizenship status.	• Information about your work authorization status, including your nationality and immigration status and data from related documents, such as your passport or other identification and immigration information.	• Government verification services	• Legal obligation (laws that require us to carry out requirements such as right to work checks and citizenship status)

4. Change of Purpose for Processing Your "Personal Data"

a. AECOM will only use your "Personal Data" for the purposes for which it was originally collected unless the Company reasonably considers the Company needs it for another purpose compatible with the original purpose and there is a legal basis for further "Processing".

b. However, if "Personal Data" covered by this Notice is to be used for a new purpose that is materially different from that for which the "Personal Data" was originally collected or subsequently authorized or is to be disclosed to a third party for their own purposes, we will provide you with notice of this new use or disclosure. We will obtain your explicit consent before proceeding, unless such use or disclosure is otherwise permitted or required by law.

5. Automated Decision Making

The AECOM online recruitment system or process may include screening questions to identify whether candidates have certain predefined minimum competences for applied positions. Please note if you provide a negative answer to any of the screening questions you may be automatically removed from the recruitment process through automatic decision mechanisms in the recruitment system. In such case you will receive an automated message that your application has been declined. You can contact your recruiter for further information.

6. Retention of Your "Personal Data"

We will retain candidate "Personal Data" for a period of up to 12 months following the closure of the recruitment process relating to the role for which you applied in the event other job opportunities arise within AECOM. In all cases, we will retain your "Personal Data" for a period of time corresponding to the applicable statute of limitations for any kind of claims that we may bring or that may be raised against us, or legal or regulatory obligations.

7. Your Data Privacy Rights

a. Where required by applicable law, AECOM extends certain data privacy rights to you.

b. Note we may be unable to provide you access to your "Personal Data" in instances where we have destroyed, erased, or anonymized the data, if we are unable to verify your identity using information we have on file for you, or if it would reveal "Personal Data" about another person. We may also refuse any request if applicable law allows or requires us to do so. We will inform you of the reasons for refusal.

c. If you choose to contact us to submit a request, you will need to provide us with:

   i. Enough information to identify you (e.g., your full name, address, birth date, or other identifier).

   ii. A description of what right you want to exercise and the information to which your request relates.

d. We are not obligated to make a data access or data portability disclosure if we cannot verify the person making the request is the person about whom we collected information, or if someone authorized to act on such person's behalf.

e. Subject to conditions set out in applicable law, you may have the following rights:

   i. **The right to request access**. You may have the right to request AECOM for copies of your "Personal Data".

   ii. **The right to request rectification**. If any "Personal Data" is inaccurate or incomplete, you may request that your "Personal Data" be corrected or completed.

   iii. **The right to request erasure**. You may have the right to request AECOM delete your "Personal Data" under certain conditions. We may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

   iv. **The right to withdraw consent.** Where you have provided written consent to the collection, processing, or transfer of "Personal Data", you may have the legal right to withdraw consent. Where we have processed your "Personal Data" with written consent, you can withdraw that consent at any time, but this may mean that you cannot continue in our recruitment process.

      Note: Withdrawing consent will not affect the lawfulness of any processing the Company conducted prior to withdrawal, nor will it affect the processing of the "Personal Data" conducted in reliance on a lawful basis other than consent.

   v. **The right to request portability**. You may have the right to request AECOM transfer your "Personal Data" that we have collected from you to another organization, or directly to you, under certain conditions.

   vi. **The right to restrict processing**. You may have the right to request that AECOM restrict the processing of your "Personal Data", under certain conditions, such as to opt-out of "sale" and "sharing" of your "Personal Data".

vii. **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 in each email subscription communication.

viii. **Results of automated decision making**. You have the right to request AECOM to conduct a review of automated decision-making that impacts you.

ix. **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 with the supervisory authority in your country of residence. You can also make a complaint to the AECOM Privacy Office.

x. **OBJECT TO PROCESSING.** You may be able to object to our processing.

f. You can submit a request to exercise these data privacy rights to the AECOM Privacy Office via the Data Subject Access Request (DSAR) - AECOM Global or email privacyquestions@aecom.com. You may also call 888.299.9602. AECOM will request specific information to help confirm identity and rights.

8. Sharing of "Personal Data"

a. AECOM shares "Personal Data" in the following ways:

i. **AECOM Staff**: AECOM shares "Personal Data" among staff having a legitimate business need to know based on their respective role with the Company.

ii. **Subsidiaries and Affiliates**: AECOM shares information among AECOM subsidiaries and affiliates for the purposes described in this Privacy Notice, where consistent with applicable legal requirements.

iii. **Service Providers**: AECOM shares "Personal Data" to selected affiliated or trusted service providers to perform services on behalf of the organization. These trusted service providers include, but are not limited to Technology Providers, Cloud Providers, Data Hosting Services, Denied and Restricted Party Screening Providers, Background Check Providers, and Data Storage Providers.

iv. **Clients**: AECOM shares certain "Personal Data" 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.

v. **Other Third Parties**: AECOM discloses certain "Personal Data" to other third parties:

1. where required by law or legal process (e.g., to tax and social security authorities)
2. where AECOM determines it is lawful and appropriate
3. 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
4. in an emergency where health or security is at stake.

vi. **Public Security/Law Enforcement**: AECOM may be required to disclose "Personal Data" in response to lawful requests by public authorities, including meeting national security or law enforcement requirements.

b. If your application for employment with us is successful and you accept a job offer from us, your "Personal Data" may also be shared as described in the Employee Privacy Notice – AECOM Global.

9. International Transfers

a. AECOM is a global company, with offices, Clients, and Suppliers located throughout the world. As a result, "Personal Data" may be transferred to (including through remote access by) 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 Data" shall take place only in compliance with applicable law through legally valid methods, including adequacy decisions for transfers, international data transfer agreements or Standard Contractual Clauses that have been recognized by Data Protection Authorities as providing an adequate level of protection to the "Personal Data" we process globally.

b. 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”.

c. AECOM will ensure all transfers of “Personal Data” are subject to appropriate safeguards as defined by data protection laws and regulations. You may request a copy of these safeguards using the contact details provided at Section 13.

10. Data Security

a. AECOM has adopted and maintains reasonable and appropriate information security policies, processes, and/or procedures to safeguard “Personal Data” 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 Data” that you may provide to us.

b. AECOM’s information security processes provide for the classification of information and the assignment of protection requirements and information security controls based on the classification of information. The safeguards used to protect “Personal Data” is commensurate with the level of risk involved.

11. External Links and Features

Our services may contain links to third-party websites or features or provide certain third-party connections or integrated services. Any access to and use of such linked websites, features, or third-party services is not governed by this Notice, but instead is governed by the privacy policies of those third parties. We are not responsible for the information practices of such third parties, including their collection, use, and disclosure of your personal information. You should review the privacy policies and terms for any third parties before proceeding to those websites or using those third-party features or services.

12. Other Important Information

Privacy laws and guidelines are part of a constantly changing environment. AECOM reserves the right, at its discretion, to modify, add, or remove portions of this Privacy Notice or any supplemental privacy notice at any time. Any material change to this Privacy Notice will be available on the website, and the date of this notice will indicate its last update.

13. Contacting AECOM Privacy Office

a. Any questions regarding this Notice or general privacy-related questions or concerns related to your “Personal Data” should be addressed to the AECOM Privacy Office at: privacyquestions@aecom.com.

b. For Germany inquiries, you may use the following email address: datenschutz@aecom.com.

14. Jurisdictional Specific Provisions

14.1 EU / UK Residents

If you consider that your rights as described in Section 7 have not been adequately addressed, you have the right to submit a complaint with the supervisory authority in your country of residence, place of work, or the country in which the alleged infringement of data protection law has occurred.

14.2 Brazil Residents

a. The LGPD (Brazilian General Data Protection Law) and consequently this annex applies to personal data collected and Processed about Brazil citizens and/or individuals located inside of Brazil.

b. Your rights as defined by the LGPD are the following:

   i. confirmation of the existence of the processing.

   ii. access to the data.

   iii. correction of incomplete, inaccurate, or out-of-date data.

iv. anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law.

v. portability of the data to another service provider or product provider, by the means of an express request, pursuant with the regulations of the national authority, and subject to commercial and industrial secrets; (New Wording Given by Law No. 13,853/2019)

vi. deletion of personal data processed with the consent of the data subject, except in the situations provided in Art. 16 of this Law.

vii. information about public and private entities with which the controller has shared data.

viii. information about the possibility of denying consent and the consequences of such denial.

ix. revocation of consent as provided in §5 of Art. 8 of this Law.

14.3 California Residents

14.3.1 California Privacy Rights

The CCPA provides California residents with specific rights regarding personal information. Subject to certain conditions and exceptions, California residents have the following rights with respect to their personal information:

a. **Right to Know**. You have the right to request: (i) the categories or personal information we collected about you; (ii) the categories of sources from which the personal information is collected; (iii) our business or commercial purposes for collecting, selling, or sharing personal information; (iv) the categories of third parties to whom we have disclosed personal information; and (v) a copy of the specific pieces of personal information we have collected about you.

b. **Right to Delete**. You have the right to request we delete personal information we have collected from you.

c. **Right to Correct**. You have the right to request that we correct inaccuracies in your personal information.

d. **Right to Opt Out of Sales and Sharing**. You have the right to opt out of “sales” and “sharing” of your personal information, as those terms are defined under the CCPA.

e. **Right to Limit Use and Disclosure of Sensitive Personal Information**. You have the right to limit the use and disclosure of your sensitive personal information. We do not use or disclose sensitive personal information beyond the purposes authorized by the CCPA; thus, this right is not available to California residents.

f. **Right to Non-Discrimination**. You have the right not to be subjected to discriminatory treatment for exercising any of the rights described in this section.

14.3.2 Exercising Your Privacy Rights

California residents may exercise their privacy rights as set forth below:

a. **Right to Know, Delete, and Correct**. California residents may submit CCPA requests to access/know, delete, and correct their personal information by:

i. Using our webform available - Data Subject Access Request (DSAR) - AECOM Global

ii. Emailing us at privacyquestions@aecom.com; or

iii. Calling us at 888.299.9602.

When you submit a request, we will take steps to verify your identity and request by matching the information provided by you with the information we have in our records. In some cases, we may request additional information in order to verify your identity, or where necessary to process your request. If we are unable to verify your identity after a good faith attempt, we may deny the request and, if so, will explain the basis for the denial.

You may also designate someone as an authorized agent to submit requests and act on your behalf. Authorized agents will be required to provide proof of their authorization in their first communication with us, and we may also require that the relevant individual directly verify their identity and the authority of the authorized agent.

b. **Right to Opt-Out of Sales and Sharing**. To exercise your right to opt out of the "sale" or "sharing" of your personal information, you may do so via our Cookie Preference Manager.

In addition, if we detect that your browser or device is transmitting an opt-out preference signal, such as the "global privacy control" or "GPC" signal, we will opt that browser or device out of cookies that result in a "sale" or "sharing" of your personal information. If you come to our website or use our products or services from a different device or from a different browser on the same device, you will need to opt out or use an opt-out preference signal for that browser and/or device as well. More information about GPC is available at https://globalprivacycontrol.org/.

We endeavour to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Contact Us: Any questions regarding this California Notice or general privacy-related questions or concerns related to your personal information should be addressed to the AECOM Privacy Office at privacyquestions@aecom.com.

14.4 Thailand Residents

If you are residing in Thailand, the following country-specific provisions will be applicable to you.

a. If you are a Thai national holding a Thai national identification card, we may collect your sensitive "Personal Data", i.e. religion and/or blood type, when collecting a copy of said identification document from you for management of our contractual relationship. If required by applicable data protection laws, we will collect this sensitive "Personal Data" with your explicit consent.

b. During the due diligence process, we may collect sensitive "Personal Data", in that case we will seek your explicit consent to the extent required by applicable law.

c. You have the following additional privacy rights:

   i. Right to Data Portability. You have the right to request a copy of your "Personal Data", in a machine-readable format, for the purpose of transferring it to another data controller.

   ii. Right to Withdraw Consent. If you have given your consent to anything we do with your "Personal Data", you have the right to withdraw your consent at any time (although if you do so, it does not mean that anything we have done with your "Personal Data" with your consent up to that point is unlawful). Please note that where your "Personal Data" is required for the purpose of contractual necessity, we may not be able to perform our contractual obligation or proceed with your request to enter into a contract with us if you withdraw your consent laws which are as strict as the ones required by your local "Personal Data" protection law.

d. International Data Transfers

Your "Personal Data" may be transferred to our group companies, affiliates, and service providers which are located outside of Thailand. While we try our best to ensure that the person who receives your "Personal Data" is in a country that has data protection laws, there could be an instance where your "Personal Data" will be transferred to other countries which do not implement adequate "Personal Data" protection standards. AECOM ensure that all such international data transfers are made in compliance with the applicable data protection laws in Thailand.

14.5 Kingdom of Saudi Arabia Residents

a. Consent or other lawful basis for processing “Personal Data”

We will only collect and process your “Personal Data” where we have a lawful basis to do so. We will usually ask for your consent before processing your “Personal Data” (and in particular any sensitive “Personal Data”), however we may also rely on the following bases, where applicable:

i. Where the processing is pursuant to another law.

ii. Where the processing is in implementation of a previous agreement to which the Data Subject is a party.

iii. If the Controller is a Public Entity and Processing is required for security purposes or to satisfy judicial requirements; or

iv. If the Processing is necessary for the purpose of our legitimate interest, without prejudice to your rights and interests, provided that no sensitive data is processed.

14.6 Mainland China Residents

This section supplements and prevails over this “Recruitment Privacy Notice Policy” in the event of a conflict with regard to our processing of your “Personal Data” if you are a resident in the People’s Republic of China (for the purpose of this Notice only, excluding Hong Kong SAR, Macau SAR and Taiwan) (“**Mainland China**”). Our processing is subject to the PRC Personal Information Protection Law (the “**PIPL**”).

a. The data controller of your “Personal Data” is the AECOM entity that operates the website you are visiting or the entity with which you communicate or conduct business.

b. Reference to “Personal Data” in this Notice includes where relevant reference to sensitive “Personal Data” under the PIPL. For the purposes of this Notice, we do not expect to process sensitive “Personal Data”, but if we do, we will request your separate consent to our processing of such sensitive “Personal Data” and will take enhanced protection measures to protect it. The following categories of “Personal Data” constitutes your sensitive “Personal Data” under the PIPL: criminal records, proof of identification (if government issued ID), biometric data (i.e., fingerprint scan), social security number, national identification number, driver’s license number, passport number, bank account number, medical / health data (e.g. medical certificates, work site incident and accident reports), demographic data (i.e. disability status, gender identity, transgender status, and sexual orientation) and other types of sensitive “Personal Data” that you provided to us (e.g. in response to surveys, interaction with the website and your communication with us). Legitimate interest” is not a legal basis available under the PIPL. To process your “Personal Data” for the purposes described in Section 3, we may rely on the following legal bases: (i) where the processing is necessary to conclude or perform a contract to which you are a party; (ii) where the processing is necessary for us to comply with legal obligations; (iii) where the processing is necessary to protect the life, health or property of natural persons under emergency; or (iv) your consent.

c. Among the third parties with which we share your “Personal Data” as described in Section 8: (i) some are entrusted data processors that process your “Personal Data” on our behalf in accordance with our instructions. We are responsible for their processing activities; while (ii) the others are separate data controllers having their independent purposes and means of processing your “Personal Data”. They are responsible for their own processing activities. If you would like to know further details about any overseas recipient, please contact us at privacyquestions@aecom.com. We request your separate consent to sharing your “Personal Data” with such separate data controllers.

d. We may transfer your “Personal Data” outside of Mainland China as described in Section 9 above. If you would like to know further details about any overseas recipient, please contact us at privacyquestions@aecom.com. We request your separate consent to transfer your “Personal Data” with such overseas recipients.

14.7 The Republic of Singapore Residents

This section supplements and prevails over this "Recruitment Privacy Notice Policy" in the event of a conflict with regard to our processing of your "Personal Data" if you are a resident in the Republic of Singapore ("**Singapore**") or if a Singapore entity is processing your "Personal Data". Our processing is subject to Singapore laws such as Personal Data Protection Act (2012) ("**PDPA**").

a. You will only receive marketing messages (e.g., voice calls, text or fax messages) to your Singapore telephone number, if we have an ongoing relationship with you or your Singapore telephone number is not listed in the Do Not Call Registry or we have obtained your clear and unambiguous written consent. You may at any time opt out of such messages by using the same medium by which the message is sent. Exceptions to the foregoing include our communications regarding services purchased by you, market survey or research and B2B messages.

b. We may transfer your "Personal Data" outside of Singapore as described in Section 9 above. We will put in place contractual measures to ensure the overseas recipients process your "Personal Data" in accordance with our instructions and have in place technical and organizational measures to protect your "Personal Data" with a level of protection comparable to the protection under PDPA.

c. At your request, we will transmit your "Personal Data" that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format.

14.8 Australia Residents

If you are residing in Australia, the following country-specific provisions will be applicable to you.

a. Complaints

You may contact us on the details provided in Section 13 of this Privacy Policy. If you remain unsatisfied about any privacy matters, you may contact the Office of the Australian Information Commissioner (www.oaic.gov.au) for guidance.

b. International Data Transfers

We may transfer your data outside of Australia as described in Section 9 of this Privacy Policy to recipients located in the United States, United Kingdom, countries in the European Economic Area, countries in Asia and/or other countries for storage, processing and use.

14.9 Hong Kong SAR Residents

a. This section supplements and prevails over this "Recruitment Privacy Notice Policy" in the event of a conflict with regard to our processing of your "Personal Data" if your "Personal Data" is processed by a Hong Kong entity or if you are a resident in Hong Kong.

b. We will notify you if our processing of your "Personal Data" is mandatory or voluntary (for example, by using asterisks on application forms). If the processing of your "Personal Data" is mandatory and you do not provide such mandatory "Personal Data" to us, we may not be able to engage or respond to you or fulfil your request.

15. References

a. Employee Privacy Notice Policy – AECOM Global L1-007-PL6

b. AECOM Privacy Office Email - privacyquestions@aecom.com

c. German Privacy Office Email - datenschutz@aecom.com

d. Global Privacy Control

16. Records

a. Data Subject Access Request (DSAR) – AECOM Global L1-007-FM8

17. Change Log

Rev #	Change Date	Description of Change	Location of Change
0	28-Aug-2024	Initial Release as L1-007-PL7	ALL
1	15-Nov-2024	Added missing wording around obtaining consent when using personal data for a new purpose.	Section 4 (b)