AECOM Global

Global Privacy Notice

L1-007-PL5

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 Global Privacy Notice ("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, described, 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 "Revised" date above. If we make material changes to this Privacy Notice, we will notify you by email or by posting a notice on our website. We encourage you to periodically review this Privacy Notice to stay up to date on our privacy practices.

2. Data Collected and Purpose

The table below provides an overview of the Personal Information AECOM collects about you for purposes described herein.

Personal Information	Purpose
Full Name, Telephone Number, Address, Email Address	a. Communicate with alumni, talent networks job applicants, clients, vendors, contractors, sub-contractors and other third parties concerning AECOM employment opportunities, projects and business operations. b. Administer background/clearance checks, legal due diligence/anti-corruption screening, and quality, occupational health and safety standard checks on job applicants, vendors, contractors and sub-contractors. c. To verify individual's identity. d. Recording of working time and timesheet records for contractors and sub-contractors. e. Incident response communications with customers, vendors, contractors, sub-contractors and other third parties. f. Administration of safety and protection of AECOM employees, resources, and workplaces.
Business Relationship Status (e.g., visitor, vendor, contractor, sub-contractor)	a. Ensuring access to correct areas is granted for customer staff, vendors, contractors and sub-contractors. b. Identification purposes for physical site access and security. c. Recording of working time/timesheet records for contractors and sub-contractors.
Emergency Contact/Next of Kin Name and Telephone Number	a. Emergency contact use for contractors and sub-contractors.

Personal Information	Purpose
Date of Birth, Nationality, Citizenship, Country of Birth	a. To administer eligibility to work checks. b. Administer denied parties, legal due diligence/anti-corruption screening, and quality, occupational health and safety standard checks on vendors, contractors and sub-contractors.
Gender	a. Requirements for reporting on diversity and equality.
Government Issued Identification / Passport Number/ National ID	a. Accounting/government tax and auditing business purposes for vendors, contractors and sub-contractors. b. To run checks for suitability for work for vendors, contractors and sub-contractors c. To verify individual's identity.
Username/Unique Identifier and Password	a. System access and authentication. b. 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 information from AECOM network and computing resources.
Medical (e.g., Medical Certificate)	a. Required by Occupational Health surveillance laws related to individual's functional ability and fitness for specific work, with any advised restrictions. b. To make reasonable adjustments based on disability. c. Reporting of worksite safety incidents.
Insurance Policy Number	a. Administer quality standard checks on vendors, contractors and sub-contractors.
Bank Information, including Routing and Account Number	a. Remuneration for vendor, contractor or sub-contractor services. b. Administer denied parties, legal due diligence/anti-corruption screening for vendors, contractors, or sub-contractors.
Job Titles Skills/Work History Experience History Training and Certification Records Evaluations References /Background Check	a. To administer eligibility to work before employment starts. b. 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. c. Manage AECOM business and project-related operations.
Fingerprint scanning, photograph	a. Identification purposes for physical site access and security of certain site locations and project worksites.
Ethnic origin, sexual orientation, health and religion or belief	a. Administer equal opportunities monitoring.

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 information 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 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 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 Information.

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 Task**: the processing is necessary for AECOM to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

f. **Legitimate Interests**: the processing is necessary for the purposes of the legitimate interests pursued by AECOM or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data where the data subject is a child.

Unless otherwise required by applicable data protection law, AECOM relies on legitimate interests for processing Personal Information during the recruitment process, forming contractual business relationships, and complying with legal requirements. Where AECOM relies on legitimate interests as a reason for processing Personal Information, it has considered whether those interests are overridden by the rights and freedoms of individuals affected by that need.

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.

AECOM may need to collect Sensitive Personal Information. Where required under applicable local law, such 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.

Please note that at this time, we do not respond to or honor "do not track," also known as DNT, signals or similar mechanisms transmitted by web browsers

5. 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 candidate Personal Information may be processed and retained for immigration requirements as part of the rehire process, including the sharing of that data with legal advisers and government bodies. The length of time data may be stored will be based on laws relating to these requirements.

6. Data Privacy Rights

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

Note that we may be unable to provide you access to your Personal Information 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 Information 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.

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

- Enough information to identify you [(e.g., your full name, address, birthdate, or other identifier)]
- A description of what right you want to exercise and the information to which your request relates.

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

Any Personal Information we collect from you to verify your identity in connection with your request will be used solely for the purposes of verification.

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 Information, 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 Information, 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.

i. California residents have certain other privacy rights, as described below:

Disclosure of Personal Information We Collect About You	You have the right to know: • The categories of Personal Information we have collected about you; • The categories of sources from which the Personal Information is collected; • Our business or commercial purpose for collecting Personal Information; • The categories of third parties with whom we share Personal Information, if any; • The categories of Personal Information that we disclosed about you for a business purpose; and • The specific pieces of Personal Information we have collected about you. • Please note that we are not required to: – Retain any Personal Information about you that was collected for a single one-time transaction if, in the ordinary course of business, that information about you is not retained; – Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered Personal Information; or – Provide the Personal Information to you more than twice in a 12-month period.
Opt-Out of the Sale of Personal Information to Third Parties	In connection with any personal information we may disclose to a third party for a business purpose, you have the right to know: • The categories of Personal Information that we disclosed about you for a business purpose. Please see Section 8 below for this information. Please note that under the California Consumer Privacy Act of 2018 (CCPA), we do not sell Personal Information to Third Parties. We do not sell Personal Information of minors under 16 years of age and we will not do so without affirmative authorization. Cal. Civ. Code § 1798.83 allows you to request opt-out of the disclosure of your personal information to third parties for their direct marketing purposes. We do not disclose personal information to third parties for their direct marketing purposes.
Right to Deletion	Subject to certain exceptions set out below, on receipt of a verifiable request from you, we will: • Delete your personal information from our records; and • Direct any service providers to delete your personal information from their records. Please note that we may not delete your personal information if it is necessary to: • Complete the transaction for which the personal information was collected, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between you and us; • Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity; • Debug to identify and repair errors that impair existing intended functionality; • Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law; • Comply with the California Electronic Communications Privacy Act; • Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when our deletion of the information is likely to render impossible or seriously

	impair the achievement of such research, provided we have obtained your informed consent; • Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us; • Comply with an existing legal obligation; or • Otherwise use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

You can submit a request to exercise these data privacy rights to the AECOM Privacy Office at privacyquestions@aecom.com. California residents may also call 888.299.9602. AECOM will request specific 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.

7. 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 Information 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.

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 the use of European Union Standard Contract Clauses and data protection agreements.

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

AECOM may also protect data through other legally valid methods, including 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 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.

Pursuant to the CCPA, in the preceding 12 months, we have not sold, but may have disclosed for a business purpose to one or more third parties the following categories of Personal Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular data subject:

- Identifiers (e.g., a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers);
- Information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number/tax identification, driver's license or state identification card number, insurance policy number for verification purposes, education, employment, employment history, bank account number, credit card number, or any other financial information for payment, medical certificates, or health insurance information;
- Characteristics of protected classifications under California or federal law;
- Internet or other electronic network activity information (e.g., browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement);
- Geolocation data;
- Audio, electronic, or similar information;
- Professional, education, certifications or employment-related information;
- Inferences drawn from any of the information identified above to create a profile about a data subject reflecting the preferences, characteristics, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

8. Data Security

AECOM has adopted and maintains reasonable and appropriate information 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 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 Information is commensurate with the level of risk involved.

9. 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 information 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.

10. Complaints and Questions

If the 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 in your country of residence.

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

11. 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	means any operation or set of operations that is performed upon Personal Information.
d.	Sensitive Personal Information	has definitions that vary from country to country. For example, European data protection laws treat certain categories of Personal Information as especially sensitive, e.g., biometric, information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information specifying medical or health conditions, or sex life. In the United States, sensitive information includes, but is not limited to, Social Security numbers, bank account numbers, passport information, healthcare related information, medical insurance information, credit and debit card numbers, drivers' license and state ID information, information from children under the age of 13, biometric information.

12. Change Log

Rev #	Change Date	Description of Change	Location of Change
0	12-Feb-2020	Initial release as L1-007-PL5	
1	14-Aug-2020	• Section 6, subsection i – the inclusion of a chart that outlines specific rights for California residents. • Section 6, subsection i – the inclusion of the Ethics hotline as a secondary method for California residents to submit privacy rights requests. • Section1, updated to include applicability to job applicants and sub-consultants. • Section 2, inclusion of a table representing examples of personal data collected to comply with transparency requirements under GDPR, CCPA and other data protection laws. • Section 12 - updated definitions for Personal Information and Sensitive Personal Information to comply with CCPA • Section 7 - removed reference to Privacy Shield principles as a mechanism to transfer personal data from the European Union. • Section 7 – inclusion of the use of European Union Standard Contract Clauses and data protection agreements as a mechanism for transfer of personal data from the European Union. • Removed section 8 – reference EU-US Privacy Shield.	
2	26-Aug-2020	• Removed references to Privacy Shield in sections 4, 6, and 9	