Global Privacy Notice

L1-007-PL5

1. Purpose and Scope

a. This Privacy Notice (the "Notice") describes how AECOM and its subsidiaries and affiliates (individually and collectively, "AECOM", "Company", "we", "us" and/or "our") may Process your Personal Data, including the reasons AECOM collects it, how and how long it is stored, who may access it and under what conditions, and what rights you have to control, delete, correct, and be informed about your Personal Data—including rights that may differ depending on your location. Please read this Notice carefully.

b. If you have questions, contact the AECOM Privacy Office at privacyquestions@aecom.com. Please note that this Notice does not apply to AECOM's recruitment activities. If you are applying for a job with us, please see the AECOM Recruitment Privacy Notice.

c. For purposes of this Notice:

   i. "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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

   ii. "Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, either by automated means, such as collection, recording, saving, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

d. If you do not provide the Personal Data requested, we may not be able to provide certain of our services to you. We will notify you where this applies to you.

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

   i. Section 13.1: EU / UK Residents

   ii. Section 13.2: Brazil Residents

   iii. Section 13.3: California Residents

   iv. Section 13.4: Thailand Residents

   v. Section 13.5: Kingdom of Saudi Arabia Residents

   vi. Section 13.6: Mainland China Residents

   vii. Section 13.7: The Republic of Singapore Residents

   viii. Section 13.8: Australia Residents

   ix. Section 13.9: Hong Kong SAR Residents

   x. Section 13.10: Canada Residents

Refer to aecom.com Privacy Policy to view 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**: AECOM may collect Personal Data that you provide when contacting us through phone, email, web forms, projects, bids, quality and compliance questionnaires, proposals, or other means.

b. **Third Parties or Publicly Available Sources**: Subject to applicable law, AECOM may obtain Personal Data from: a representative of your company (such as if we are performing work for your company, or your company is performing work for AECOM), publicly available online professional organizations, social media, and other networking platforms (e.g., LinkedIn, ZoomInfo).

c. **Combining "Personal Data" from Different Sources**: AECOM 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, such as for the marketing purposes described at Section 3.3.

3. What Personal Data we use and why

AECOM may collect the Personal Data listed in the below subsections, for the specified reasons and in the specified manner.

3.1 When you visit our Websites

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Contact details and contact preferences. • The products, or services we, or our customers/clients provide to you, and/or your use of them. • Personal Data related to your support request or any other type of inquiry you need our assistance with.	• To manage our interactions with you, communicate with one another, and respond to queries and complaints through available communication channels, including chat, email, social media platforms, webforms, telephone, surveys (telephonic/online and in-person). • To comply with client requirements.	• Our legitimate interest in delivering satisfactory customer service to you and ensure a good customer experience of our brand. • Your consent where required. • Performance of a public task in the public interest handed down by public official authority, such as conducting a census for a government function.
• Contact details (e.g., name, phone, email address). • Age and title. • Email open/click rates. • Other Personal Data you provide to us.	• To understand your experiences, interests and concerns about our products, services, and brand, by means of conducting insight related initiatives such as surveys and research studies. • To comply with client requirements.	• Our legitimate interest in improving our products, services, and customer experience; understanding overall performance and efficiency of our insight related initiatives. • Your consent for marketing purposes in those countries where required to track email open / click rates, or to conduct surveys and research studies.
• Information provided in connection with your event registration and participation such as your contact details, dietary requirements, or other needs when relevant.	• To plan, organize, and manage events you have agreed to and/or participated in.	• Our legitimate interest in advertising our business services and products. • Your consent, where required.

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Personal Data that we collect during the event (including, where applicable, photographs and videos depicting you).		
• Contact details. • Professional details.	• To Process your Personal Data for the purpose of lead management if you are not yet a customer.	• Our legitimate interest to handle prospective customers. • Your consent, where required.

AECOM Processes certain Personal Data when you use our websites. For further information about the Personal Data we Process and the technologies we use, please see our cookie policy.

3.2 When we Communicate and Connect with you

AECOM collects Personal Data when you contact us or when we contact you on behalf of our clients through project-related work.

3.3 For Marketing our Services and Products to you

AECOM collects Personal Data to personalize news, marketing content, and offers, which may be communicated to you via various channels such as postal mail, phone, email, and social media. Where we obtain information about you from third parties, we have implemented checks and reviews to confirm that the information was lawfully obtained by the relevant third party and that the third party has the right to provide us with this information. If you no longer wish to receive marketing offers from us, you can always let us know by selecting 'unsubscribe' at the bottom of each marketing email or similar in the other channels.

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Contact details (name, email address). • Contact preferences for marketing communications. • Record of your privacy choices, such as opt-out of marketing, cookie settings (date and time of your choice).	• To record and manage your choices. • To send marketing communications that you have requested or may be of interest to you, according to your preferences.	• Your consent to receive direct marketing communications (e.g., email marketing) from us. • Where you have bought a service from us, and where applicable, where we send marketing communications to you as representative for a business, our legitimate interest to send you marketing communications. • Our legal obligation to document and demonstrate whether you have consented to receiving marketing communications from us and record and respect your contact preferences and when and what you have opted out from.

3.4 For Employees of our Clients or Business Partners

AECOM collects Personal Data to: manage existing and prospective clients, customers, suppliers, or other third-party relationships (e.g. in relation to the initiation, conclusion, or fulfillment of a contract); Communicate about products or services we offer or intend to offer; improve our products or services; and review our business relationship; perform accounting, auditing, billing, and collection activities; meet legal obligations (e.g. financial and administrative obligations); and establish, enforce or defend against legal claims.

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Identification data, such as full name, preferred name, business/mailing address, email address, and telephone number. • Other business data, such as data on invoices, purchase orders, agreements, bids, proposals, and other related business records that may contain Personal Data. • Other information you make available to us throughout our business relationship.	• To maintain our business relationship with you, communicate with you and otherwise address matters concerning our business relationship.	• Our legitimate interest in maintaining our business operations.
• Electronic and voice communications data - a record of our contacts with you, including interviews, and disposition (which may include CCTV footage captured within our offices), visitor sign-in logs, and business communications content and data, including IP address and session identification through all applicable communication channels, including email, text, instant message or chat, transcriptions and/or telephone communications, voice recordings, and video recordings.	• To manage safety and security at our facilities.	• Our legitimate interest to maintain security and safety, prevent theft and fraud on our premises.

3.5 For Shareholders

As AECOM a publicly traded company, AECOM has certain obligations to you, as a shareholder, pursuant to Securities and Exchange Commission (SEC) regulations. To meet these obligations, AECOM collects and stores the following information about you in your role as a shareholder:

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Contact information. • Proof of identification. • Information regarding proxies representing shareholders, where applicable.	• To identify shareholders, manage the shareholder register, prepare for shareholder meeting, and conduct shareholder meetings.	• To comply with our legal obligation, including those required by the Security and Exchange Commission.

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Information about your shareholding. • Visual material and/or audio recordings (such as recordings during a general meeting). • Other information that you make available to us (such as via e-mail, notifications to a general meeting, request to address a specific matter at a general meeting and other communication).	• To fulfil our obligations towards you as a shareholder under applicable law. • To fulfil our obligations under applicable law. • To manage Company holdings, including any share distributions where applicable. • To communicate with you as a shareholder.	• Our legitimate interest in identifying you as a shareholder and to communicate with you. • Our legitimate interest in managing and, where applicable, distributing our holdings and share relevant information (including but not limited to Personal Data relating to you as a shareholder) with third parties such as central securities depositories and banks issuing depository receipts, as relevant.

3.6 Contractors and Subcontractors

a. AECOM collects the following Personal Data when onboarding contractors and subcontractors in order to satisfy AECOM's contractual obligations:

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Identification data, such as: full name, preferred name, business address, home address, email address telephone number, username/password, date of birth, nationality, citizenship status, country of birth, photo/image, and biometric data (i.e., fingerprint scan) where applicable. • Emergency contacts, such as full name, address, and telephone number. • Employment and professional information, such as: job title/position, prior work or project experience, reference contacts, CV/resume, academic/ professional qualifications, skills, work-related licenses, education, references, military status, work permits, and training reports. • Government-issued data, such as Social Security Number, federal tax identification number, national identification number, driver's license number, and passport number. • Financial/Insurance data, such as bank name and routing and account number, and insurance policy information.	• To maintain our business relationship with you, communicate with you and otherwise address matters concerning our business relationship. • Conduct legal due diligence/anti-corruption screening, denied or restricted party checks (Descartes MK Denial), recording of Administration of work time, business continuity and incident response communications. • To evaluate your skills and experience, verify your data, to contact you for project opportunities and general business operations. • Accounting/government tax and auditing business purposes. • 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. • Administration of safety and protection of AECOM employees, resources, and workplaces, physical site access	• Legitimate interest (to maintain our business operations and to secure our network). • Legal obligation (laws that require us to carry out requirements such background or denied party screening, tax reporting, and OSHA requirements). • Your express consent when required by law for background checks, including denied party screening.

Type of Personal Data Collected	Purpose for AECOM's Use	Lawful Basis for AECOM's Use
• Medical/Health data, such as medical certificates, work site incident and accident reports.	and security, including use of individuals who are required to maintain specific qualifications or certifications, and to manage AECOM business and client project-related operations.	
• 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 are set forth below. Where the Processing of demographic data is not required by law, we will ask for your express consent. • To carry out equal opportunities monitoring, analyze our procurement practices, support our efforts to create and maintain a diverse workforce and produce diversity statistics.	• AECOM only collects this Personal Data with your consent*. * If you choose to consent, you can withdraw this at any time, by contacting us.
• Electronic and voice communications data, such as record of our contacts with you, including interviews, and disposition (which may include CCTV footage captured within our offices), and business communications content and data, including IP address and session identification through all applicable communication channels, including email, text, instant message or chat, transcriptions and/or telephone communications, voice recordings, and video recordings.	• To manage AECOM business and project-related operations • To manage safety and security at our facilities. • 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 the AECOM network and computing resources.	• Our legitimate interest to maintain security and safety, prevent theft and fraud on our premises.

b. In addition to the Personal Data identified in the above table, AECOM may collect the following additional Personal Data about you:

i. CCTV monitoring and Fleet Vehicle Dash Cams

AECOM may use Closed Circuit Television ("CCTV") monitoring at its physical sites, and/or dash cams in fleet vehicles where permitted by law. CCTV monitoring is generally used to control and prevent unauthorized access to AECOM's premises and equipment, however in some countries it may also be used for the purpose to ensure compliance with health and safety guidelines and procedures and for overall production improvement purposes. Fleet vehicle CCTV is used for driver safety. CCTV and fleet vehicle dash cam images and recordings are securely stored and only accessible on a need-to-know basis (for example, to investigate an incident).

ii. Special categories (Sensitive Personal Data)

Certain Personal Data may be regarded as "Special Category" Personal Data under applicable data privacy laws, such as certain Personal Data about religion, ethnicity, genetics, biometrics, sex life, political opinions or health data. Any such Special Category Personal Data must be handled with extra care and requires additional protective measures. Where AECOM Processes Special Category Personal Data, we will only do so where there is a lawful basis and/or where you provide your explicit consent. In such cases, AECOM will inform you and (if required by law to do so) seek your explicit consent to Process such data.

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 we reasonably consider that we need it for another purpose compatible with the original purpose and there is a legal basis for such Processing.

b. 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, AECOM will provide you with an opportunity to choose whether to have your Personal Data so used or disclosed.

5. Retention of Your Personal Data

a. Your Personal Data will be retained only for as long as required to achieve the purposes for which it was collected, in line with this Notice, and will be securely destroyed when no longer required.

b. The following criteria are what determine the period for which the Company will keep your Personal Data:

   i. When it is no longer required to be retained to comply with regulatory requirements or financial obligations

   ii. Until we are no longer required to do so by any applicable law

   iii. Until all purposes for which the data was originally gathered have become irrelevant or obsolete; or

   iv. Until the goods and/or services we have provided are no longer in active use.

We may also use aggregated, anonymized, and/or pseudonymise datasets which are de-identified so that they no longer constitute Personal Data.

6. Your Data Privacy Rights

a. Where required by applicable law, AECOM extends certain data privacy rights to you, as listed below and subject to the conditions set out in applicable law:

   i. **The right to request access**. You may have the right to request copies of your Personal Data. Note that 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.

   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 have the right to request AECOM delete your Personal Data under certain conditions. Note that AECOM may not always be able to accomplish such deletion because of overriding legal requirements. In those cases, AECOM will provide an explanation of why we could not delete the data.

iv. **The right to withdraw consent.** Where you have provided written consent to the collection, Processing, or transfer of Personal Data, you have the legal right to withdraw consent. Where we have Processed your Personal Data based only on your written consent, you can withdraw that consent at any time, but this may mean that we cannot provide certain services to you. Note that withdrawing consent will not affect the lawfulness of any Processing the Company conducted prior to your withdrawal of consent, 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 have the right to request AECOM transfer your Personal Data that we have collected from you to another organization, or directly to you, in a structured, commonly used, and machine-readable format, when technically feasible.

vi. **The right to restrict Processing**. You 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 have the right to 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 to review 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 to the AECOM Privacy Office or to the supervisory authority in your country of residence.

x. **Object to Processing.** You may be able to object to our Processing where AECOM is using your Personal Data for marketing purposes. You may also be able to object to our Processing where AECOM is using your Personal Data for other purposes, such as legitimate interests, unless the company can demonstrate compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

b. 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.

Note: AECOM will not disclose data 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.

c. 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.

d. 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 of Personal Data

AECOM shares Personal Data in the following ways and circumstances:

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

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

c. **Vendors**: AECOM shares Personal Data to selected vendors to perform services on behalf of the organization. These vendors may include, for example:

   i. Cloud providers / Data hosting / storage providers: for example, in connection with our customer relationship management or subcontractor onboarding systems.

   ii. Denied and Restricted Party Screening Providers: for example, to help us to comply with sanctions rules.

d. **Clients**: AECOM shares certain Personal Data as part of our solicitation of and provision of professional services to our clients for bids and proposals, project-related work, security clearances or as required by security protocols.

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

   i. where required by law or legal process (e.g., to tax and social security authorities, or in response to judicial subpoenas)

   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.

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

8. International Transfers

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, Central and South America, the Middle East, or the United States for the purposes identified. Any such transfer of Personal Data will take place in compliance with applicable law through legally appropriate methods, including adequacy decisions, international data transfer agreements, Standard Contractual Clauses, or other similar methods that have been recognized by Data Protection Authorities as providing a legally adequate level of protection to Personal Data. AECOM will further ensure all such transfers of Personal Data are subject to legally appropriate safeguards. You may request a copy of these safeguards using the contact details provided at Section 12 of this Notice.

9. 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, because no method of transmission over the Internet or electronic storage is entirely secure, AECOM does not warrant the security of any Personal Data that you may provide.

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.

10. External Links and Features

Communications from AECOM 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. Your use of those third party provided websites, features and services is done at your sole discretion and AECOM is not responsible for the information practices of such third parties, including their collection, use, and disclosure of your Personal Data. 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.

11. 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 at https://aecom.com/content/privacy-policy/recruitment-privacy/ and the date of this notice will indicate its last update.

12. 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.

13. Jurisdictional Specific Provisions

13.1 EU / UK Residents

AECOM cooperates with European Union data protection authorities and complies with the advice given by such authorities regarding human resources data transferred from the European Union in the context of the employment relationship. If you consider that your rights as described in Section 6 of this Notice 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.

13.2 Brazil Residents

a. The Brazilian General Data Protection Law and this subsection applies to Personal Data collected and Processed about Brazil citizens and/or individuals located inside of Brazil.

b. In addition to those rights stated above, you have the following additional rights pursuant to the law:

   i. Confirmation of the existence of the Processing.

   ii. Access to the Personal Data.

   iii. Correction of incomplete, inaccurate, or out-of-date Personal Data.

   iv. Anonymization, blocking or deletion of unnecessary or excessive Personal Data or Personal Data Processed in noncompliance with the provisions of the Brazil Data Protection Law.

   v. Portability of the Personal Data to another service provider or product provider, by the means of an express request, pursuant with the regulations of the Autoridade Nacional de Proteção de Dados (ANPD), and subject to commercial and industrial secrets; deletion of Personal Data Processed with your consent, except in the situations provided in Article 16 of the Brazil General Data Protection Law.

   vi. Information about public and private entities with which AECOM has shared Personal Data.

   vii. Information about the possibility of denying consent and the consequences of such denial.

   viii. Revocation of consent as provided in Section 5 of Article 8 of the Brazil General Data Protection Law.

13.3 California Residents

a. This section of the Notice ("**California Notice**") describes how we Process the personal information of California residents, pursuant to applicable California privacy laws, including the California Consumer Privacy Act (the "**CCPA**"). This California Notice also explains your rights concerning your personal information. This California Notice describes our information practices under the CCPA, specifically our offline and online collection and Processing of "Personal Information". Under the CCPA, "Personal Information" is any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident, household, or device. This California Notice does not address or apply to our handling of publicly available information or Personal Information that relates to Company employees or job applicants with whom the Company engages; different notices apply. This California Notice also does not apply to our information practices or that are otherwise exempt under the CCPA. Depending on how you interact or engage with us, we may provide you with other privacy notices with additional details about our information practices.

b. **Categories of Personal Information AECOM May Collect or Disclose**. The table below sets out generally the categories of Personal Information AECOM may collect about you (and may have collected in the prior 12 months), as defined by the CCPA, as well as the categories of other entities to whom we may disclose this information for a business or commercial purpose. Our collection and disclosure of Personal Information will vary depending upon the circumstances and nature of our interactions or relationships with You.

Categories of Personal Information	To Whom AECOM May Disclose for a Business or Commercial Purpose
i. **Identifiers, generally**. Includes direct identifiers such as name, alias, account name/user ID/username, email address, phone number, postal address, unique personal identifier, online identifier, IP address, or other similar identifiers.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Data analytics providers • Advertising networks • Social networks • Other clients, customers, or website users • Others as required by law
ii. **Identifiers, government identification**. Includes identifiers provided by a government institution, such as social security number, driver's license number, state identification card number, passport number, or other similar identifiers.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Others as required by law
iii. **Customer Records**. As defined by Cal. Civil Code § 1798.80, this category includes information such as signature and physical characteristics or description.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Others as required by law
iv. **Commercial Information**. Includes records of our products and services that you have purchased, obtained, or considered, or other purchasing or use histories or tendencies.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Data analytics providers • Advertising networks • Social networks • Others as required by law
v. **Internet or Other Electronic Network Activity Information**. Includes, but is not limited to, browsing history, clickstream data, search history, and information regarding interactions with our website, advertisements, or emails, including other usage data related to your use of any of our products or services.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Data analytics providers • Advertising networks • Social networks • Others as required by law

Categories of Personal Information	To Whom AECOM May Disclose for a Business or Commercial Purpose
vi. **Location Data**. Includes, but is not limited to, general location information about a particular individual or device.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Others as required by law
vii. **Audio, Electronic, Visual, or Similar Information**. Includes, but is not limited to, information collected via call recordings (or transcripts) if You are interacting with us in a customer service capacity or if You call us on a recorded line, CCTV monitoring, recorded meetings and webinars, videos, photographs, and user profile images.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Other clients, customers, or website users • Others as required by law
viii. **Professional Information**. Includes, but is not limited to, job title, company name, business email, business phone number, and other similar professional-related information.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Other clients, customers, or website users • Others as required by law
ix. Protected Classifications. We may collect some information that is considered a protected classification under California or United States federal law, such as Your gender or sex, age, date of birth, religion or creed, or medical condition or disability information.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Others as required by law
x. Sensitive Personal Information. In some circumstances, we may collect: (1) government identification information, (2) account log-in information, (3) religious or philosophical beliefs, and (4) health or medical information.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Others as required by law
xi. **Inferences**. Includes, but is not limited to, inferences drawn from any of the information described in this section about a California resident including inferences reflecting an individual's preferences, characteristics, behaviors, attitudes, abilities, and aptitudes.	• Affiliates and subsidiaries • Service providers and vendors • Advisors and agents • Others as required by law

c. **Sources of Personal Information**. AECOM generally collects Personal Information from the following sources:

i. Directly from individuals

ii. Other AECOM clients, customers, and users

iii. Government agencies and public records

iv. Vendors and service providers

v. Data brokers and business partners

vi. Data analytics providers and advertising networks

vii. Social media platforms

viii. Internet service providers and operating systems and platforms; and

ix. Business customers and clients.

d. **Purposes of Collection, Use, and Disclosure**. In general, we collect and Process Personal Information for the following business or commercial purposes, or as otherwise directed or consented to by you:

i. When you visit our websites

1. To establish a connection to our website

2. To detect fraud and misuse when you interact with our web functions, e.g., misuse of forms and detection of bots
3. To remember the choices you have made on our websites (such as privacy settings and language)
4. To measure how our websites are being used and to gain insight into how the services are used; and
5. To better understand user behavior and improve the usability, reliability, and user experience of our websites.

ii. When we communicate and connect with you (through any channel such as chat, email, social media platforms, webforms, telephone or when you respond to surveys, or when we visit you in person)

1. To manage our interactions with you and respond to queries and complaints
2. To comply with client requirements, such as conducting landowner surveys, emergency response outreach
3. To obtain a better understanding of your experiences, interests, and concerns about our products, services, and brand by means of conducting insight-related initiatives such as surveys and research studies
4. To plan, organize, and manage in-person and virtual events to which you have agreed to and/or in which you have participated; and
5. For lead management purposes, if you are not yet a client.

e. For marketing our products and services to you

i. To record and manage your marketing choices, e.g., for email newsletters and website marketing and analytics preferences; and

ii. To send marketing communications that you have requested or that may be of interest to you, according to your preferences.

f. For our clients, employees of our clients, or business partners

i. To maintain our business relationship with you, communicate with you, and otherwise address matters concerning the business relationship; and

ii. To manage safety and security at our facilities.

g. For shareholders

i. To identify shareholders, manage the shareholder list, and prepare for and conduct the general meeting and related meetings

ii. To fulfill our obligations under applicable laws, e.g., disclosure of shareholder lists as legally required

iii. To manage Company holdings, including any share distributions where applicable; and

iv. To communicate with you as a shareholder.

h. For legal and compliance purposes

i. To protect our websites, services, and business operations, as well as our rights and those of our stakeholders and investors

ii. To prevent and detect fraud, unauthorized activities and access, and other misuse of our websites and services, including where we believe necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party, or violations of the AECOM Terms of Use;

iii. To comply with applicable legal or regulatory obligations, including as part of a judicial proceeding, responding to a subpoena, warrant, court order, or other legal Process, or as part of an investigation or request, whether formal or informal, from law enforcement or a governmental authority

iv. To conduct financial, tax and accounting audits, operational audits and assessments (including privacy, security and financial controls), as well as for risk and compliance purposes

v. to maintain appropriate business records and enforce our policies and procedures

vi. To assess and implement mergers, acquisitions, reorganizations, bankruptcies, and other business transactions such as financings; and

vii. to administer our business, accounting, auditing, compliance, recordkeeping, and legal functions.

i. **Sales and Sharing of Personal Information**. For purposes of this California Notice, a "sale" means disclosing or making available personal information to a third party in exchange for monetary or other valuable consideration; and "sharing" includes disclosing or making available personal information to a third party for purposes of cross-context behavioral advertising. While we do not disclose Personal Information to third parties in exchange for monetary compensation, we may "sell" or "share" the following categories of personal information: identifiers, Internet and network activity information, and commercial information. We may disclose these categories to third-party advertising networks, analytics providers, and social networks for purposes of marketing and advertising and to improve and measure our ad campaigns. We do not sell or share sensitive personal information, nor do we sell or share personal information about individuals we know are under the age of sixteen.

j. **Sensitive Personal Information**. Notwithstanding the purposes described above, we do not collect, use, or disclose "sensitive personal information" beyond the purposes authorized by applicable privacy law. Accordingly, we only use and disclose sensitive personal information as reasonably necessary and proportionate: (i) to perform our services requested by you; (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents; (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct; (iv) to verify or maintain the quality and safety of our services; (v) for compliance with our legal obligations; (vi) to our service providers who perform services on our behalf; and (vii) for purposes other than inferring characteristics about you.

k. **Personal Information of Children.** Our services are not designed for children, and we do not knowingly collect Personal Information from children under the age of thirteen (13). If you are a parent or legal guardian and you believe we have collected your child's Personal Information in violation of applicable law, please contact us at privacyquestions@aecom.com.

l. **Retention**. Your Personal Information will be retained only for as long as required to achieve the purposes for which it was collected, in line with this California Notice, and will be securely destroyed when no longer required. The Company uses the following criteria to determine how long we will retain your personal information:

i. When it is no longer required to be retained to comply with regulatory requirements or financial obligations.

ii. Until we are no longer required to do so by any law to which we are subject.

iii. Until all purposes for which the Personal Information was originally collected have become irrelevant or obsolete.

iv. Until the products and/or services we have provided are no longer in active use.

m. **Deidentified Data**. Regardless of any other section of this California Notice, the Company may collect, use, disclose, or otherwise Process data that has been deidentified to the extent that it no longer constitutes "Personal Information". As required by applicable law, we will not attempt to reidentify such deidentified data except as permitted to test our deidentification systems.

n. **California Privacy Rights**. Subject to certain conditions and exceptions (including but not limited to: completing transactions; detecting security incidents; exercising free speech; complying with legal obligations; performing necessary functions for research in the public interest; debugging to fix errors; defending legal claims; and situations where retaining data is necessary for legitimate business operations or legal compliance), California residents have the following rights with respect to their personal information:

   i. **Right to Know**. You have the right to request: (1) the categories or Personal Information we collected about you; (2) the categories of sources from which the Personal Information is collected; (3) our business or commercial purpose(s) for collecting, selling, or sharing Personal Information; (4) the categories of third parties to whom we have disclosed Personal Information; and (5) a copy of the specific pieces of Personal Information we have collected about you.

   ii. **Right to Delete**. You have the right to request we delete Personal Information we have collected from you.

   iii. **Right to Correct**. You have the right to request that we correct inaccuracies in your Personal Information.

   iv. **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.

   v. **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 beyond what is authorized by the CCPA. The Company only uses or discloses your sensitive personal information for the purposes stated in this California Notice or time of collection, and only as authorized by the CCPA. Should the Company otherwise use or disclose your sensitive personal information, this right is available to California residents.

   vi. **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.

o. **Exercising Your Privacy Rights**. California residents may exercise their privacy rights as set forth below:

   i. **Right to Know, Delete, and Correct**. California residents may submit CCPA requests to access/know, delete, and correct their Personal Information by:

      1. Using the Data Subject Access Request (DSAR) - AECOM Global webform
      2. Emailing us at privacyquestions@aecom.com; or
      3. 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. When necessary, we may request additional information to verify your identity or process your request. If we are unable to verify your identity after a good faith attempt, we may deny the request. In such cases, we 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. We may also require that the relevant individual directly verify their identity and the authority of the person seeking to act as an authorized agent.

   ii. **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 by clicking on Cookie settings. We will apply your opt-out based on the personal information in our records that is linked or reasonably linkable to the information provided in your request.

   In addition, if we detect that your browser or device is signaling an opt-out preference, such as a "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 visit our website or access 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. More information about GPC is available at https://globalprivacycontrol.org/.

p. **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.

13.4 Thailand Residents

a. This section supplements and prevails over this Notice in the event of a conflict regarding our Processing of your Personal Data.

b. If you fail to provide your Personal Data, we may be unable to provide you with our services (or any part thereof), including onboarding you as a subcontractor, or comply with any applicable laws or regulations or guidelines and codes issued by regulatory or other authorities.

c. 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.

d. During the background check review process, we may collect sensitive Personal Data, in that case we will seek your explicit consent to the extent required by applicable law.

e. 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.

13.5 Kingdom of Saudi Arabia Residents

a. This section supplements and prevails over the Global Privacy Notice in the event of a conflict regarding our Processing of your Personal Data.

b. 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.

13.6 Mainland China Residents

This section supplements and prevails over the Global Privacy Notice in the event of a conflict regarding our Processing of your Personal Data if you are a resident in the People's Republic of China (for the purpose of this portion of the Notice only, excluding Hong Kong SAR, Macau SAR and Taiwan) ("**Mainland China**"). Our Processing is subject to the People's Republic of China's 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 section includes, where relevant, reference to sensitive Personal Data under the PIPL. For the purposes of this Notice subsection, we do not expect to Process sensitive Personal Data, but if we do, we will request your separate consent and will take enhanced protection measures to protect the sensitive Personal Data. 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). To Process your Personal Data for the purposes described in Section 3 of this Notice, we may rely on the following 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 7 of this Notice, 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 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 privacyquestions@aecom.com.

d. We may transfer your Personal Data outside of Mainland China as described in Section 8 of this Notice. If you would like to know further details about any overseas recipient, please contact us at privacyquestions@aecom.com.

13.7 The Republic of Singapore Residents

If you are a resident in the Republic of Singapore ("**Singapore**") or if a Singapore entity is Processing your Personal Data, this section supplements and prevails over any conflicting portion of this Notice in the event of a conflict with regard to our Processing of your Personal Data. Our Processing is subject to Singapore Personal Data Protection Act (2012) ("**PDPA**").

a. You may receive marketing communications as described in Section 3.3 of this Notice. 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, if your Singapore telephone number is not listed in the Do Not Call Registry, or if 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 business-to-business messages.

b. You may receive unsolicited commercial electronic messages (e.g., email, electronic message sent to instant messaging account) from us. If you do not wish to continue to receive any such message, you may utilise the unsubscribe facility provided in such message.

c. We may transfer your Personal Data outside of Singapore as described in Section 8 of this Notice. 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.

d. 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.

13.8 Australia Residents

This section supplements and prevails over this Notice in the event of a conflict with regard to our Processing of your Personal Data. 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 12 of this Notice. If you remain unsatisfied about any privacy matters, you may contact the Office of the Australian Information Commissioner for guidance at www.oaic.gov.au.

b. **International data transfers**. We may transfer your data outside of Australia as described in Section 8 of this Notice to recipients located in other countries for storage, Processing and use.

13.9 Hong Kong SAR Residents

This section supplements and prevails over the Global Privacy Notice 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 of Hong Kong.

a. 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.

b. Regarding direct marketing, the provisions of Section 3.3 of this Notice shall be replaced to the extent of any conflict with the following:

   i. We want to keep you updated and to be able to provide you with relevant news, marketing content and offers about us and our products and services, via email, SMS, post or other similar channels using your contact information you provide us, but we cannot do so without your consent.

   ii. If you do not wish to receive direct marketing communications from us, you can always let us know by selecting 'unsubscribe' at the bottom of each marketing communication.

13.10 Canada Residents

This Canada Privacy Addendum supplements the information contained in this Notice and applies solely to clients and others who reside in Canada. Any terms defined in the Personal Information Protection and Electronic Documents Act or a Personal Information Protection Act have the same meaning when used in this Canada Privacy Addendum. In the event of a conflict between the provisions of the Global Privacy Notice and the provisions of this Canada Privacy Addendum, the provisions of this Canada Privacy Addendum shall govern and control.

a. We collect, retain, Process, and disclose personal information generally for business and commercial purposes as described in Section 3 of this Notice.

b. Please be aware that information we collect, including personal information involving Canadian residents, may be transferred to, Processed, stored and used by AECOM, its clients or service providers in various provinces within Canada, the United States, and other countries.

c. We use physical, technical, and administrative security measures designed to reduce the risk of unauthorized access, use, disclosure, or alteration of your personal information. However, no system of security safeguards can guarantee the security of the Personal Data we collect. In addition, you share the responsibility for keeping your Personal Data secure while browsing our websites.

d. Quebec Privacy Laws provide Quebec residents with the following rights. Please see Section 6 of this Notice for instructions on how to exercise these rights:

   i. **The right to be informed**. You have the right to know what personal information is collected from you, the means of collection of the personal information, the purposes of use of the collected information, the categories of persons who have access to collected data, and the duration of time that the personal information will be kept.

   ii. **The right of access**. You have the right to access to the personal information we hold about you (subject to certain restrictions). We may charge a reasonable fee, taking into account the administrative costs of providing the information. Unfounded, excessive or repetitive requests may be ignored.

   iii. **The right to rectification**. You have the right to have your personal information rectified if it is incorrect or outdated and/or completed if it is incomplete.

   iv. **The right to erasure/right to be forgotten**. In some cases, you have the right to have your personal information erased or deleted, de-indexed from association with your name, or to otherwise have us cease disseminating your personal information. Note this is not an absolute right, as we may have legal or legitimate grounds for retaining your personal information.

   v. **The right to withdraw consent**. You can withdraw your consent to our Processing of your data when such Processing is based on consent. The withdrawal of consent will not affect the lawfulness of Processing based on consent before its withdrawal.

   vi. **The right to restrict Processing**. You have a right not to have your personal information subject to automated Processing (e.g. profiling).

   vii. **The right to data portability**. You can request that computerized personal information held by AECOM be provided to you in a structured and commonly used technological format.

   viii. **Right to Challenge Compliance**. You have the right to challenge AECOM's compliance with Quebec's Law 25. If you believe your privacy rights have been violated, you can file a complaint with the Commission d'accès à l'information du Québec.

e. Non-Quebec residents have with the following rights:

   i. **The right to be informed**. You have the right to know what personal information is collected from you, the means of collection of the personal information, the purposes of use of the collected information, the categories of persons who have access to collected data, and the duration of time that the personal information will be kept.

   ii. **The right to access**. You have the right to access to the personal information we hold about you (subject to certain restrictions). We may charge a reasonable fee taking into account the administrative costs of providing the information. Unfounded, excessive or repetitive requests may be ignored

   iii. **The right to rectification**. You have the right to have your personal information rectified if it is incorrect or outdated and/or completed if it is incomplete.

   iv. **The right to withdraw consent**. You can withdraw your consent to our Processing of your data when such Processing is based on consent. The withdrawal of consent shall not affect the lawfulness of Processing based on consent before its withdrawal.

   v. **Right to Challenge Compliance**. You have the right to challenge AECOM's compliance. If you believe your privacy rights have been violated, you can file a complaint with the following:

      1. Office of the Privacy Commissioner of Canada
      2. Commission D'accès à L'information du Quebec
      3. Office of the Information and Privacy Commissioner for British Columbia
      4. Office of the Information and Privacy Commissioner of Alberta

14. Terms and Definitions

a.	Data Privacy	means the legal rights and expectations of individuals to control how their "Personal Data" is collected and used.
b.	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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
c.	Process	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, either by automated means, such as collection, recording, saving, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
d.	Sensitive Personal Data	has definitions that vary from country to country. For example, European data protection laws treat certain categories of "Personal Data" 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 may include, 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, genetic data, precise geo-location, and information about racial or ethnic origin, religious or philosophical beliefs, sex life, sexual orientation or union membership.

15. Records

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

16. 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 Data" and Sensitive "Personal Data" to comply with CCPA. • Section 7 - removed reference to Privacy Shield principles as a mechanism to transfer "Personal Data" from the European Union.	

Rev #	Change Date	Description of Change	Location of Change
		• 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	
3	20-Jan-2023	• Section 1 –updated entire section to clarify terms and requirements. • Section 2.1 – added new section 2.1 for public website data collection. • Section 2.2 – added new section 2.2 for collection and processing of candidate data. • Section 2.3 – added new section 2.3 for collection and processing of contractor and subcontractor data. • Section 2.4 – added new section 2.4 for collection and processing of client and vendor data. • Section 3 – added new section 3 for change of purpose of processing data. • Section 5 – Updated section 5 for lawful basis of processing data. • Section 6 – made updates to use and retention of data. • Section 7 – added right of human intervention for automated decision-making results. • Section 8 – made updates for sharing and onward transfer of data. • Section 10 – added new section 10 for California residents. • Section 13 – updated section to reflect email contact for Germany operations.	
4	22- Sept-2023	• Section 1 to Section 8 – made minor updates throughout	
5	29-Jan-2025	• Added country addendums • Removed applicability to job candidates and replaced with hyperlink to new Recruitment Privacy Notice.	ALL