# Privacy Notice for Staff and Job Applicants

## Issued: April 1, 2023

## Updated:

## 1. Introduction

American Equity Investment Life Holding Company together with all of its subsidiary companies ("AEL", "we" or "us") has issued this Privacy Notice (this "Notice") to describe how we handle Personal Data that we collect and process about our staff members and job applicants (collectively referred to as "you") applying for a job at or working for AEL in the United States. The term "staff member" includes those who work on a permanent and non-permanent basis, including contingent workers, temporary workers, and interns. This categorization is for convenience and does not demonstrate any particular employee, worker or other status.

We respect the privacy rights of individuals and are committed to handling Personal Data responsibly and in accordance with applicable law. This Notice sets out the Personal data that we collect and process about you, the purposes of the processing and the rights that you have in connection with it.

Please take the time to read and understand this Notice, which should be read in conjunction with our other corporate policies and procedures. When appropriate, we will provide a "just in time" notice to cover any additional processing activities not mentioned in this document. If you are a California resident, please see the CCPA/CPRA Addendum appended to this Notice for additional disclosures regarding the information we collect and any rights you may have under California law.

If you have any comments or questions about this Notice, please contact us at the contact details in Section 8 below.

## 2. Types of Personal Data we Collect

In the course of your employment at AEL, or when making an application for employment, we may process Personal Data about you and your dependents, beneficiaries and other individuals whose Personal Data has been provided to us.

We use the term "Personal Data" (also called "personal information" or "personally identifiable information" in the laws of some jurisdictions) to refer to information that reasonably identifies, relates to, describes, or can be associated with you. Data that has been de-identified, anonymized, or aggregated, or that otherwise cannot reasonably be related back to

a specific person is not considered Personal Data. The precise definition of Personal Data may vary depending on your state of residence, but we take the same approach to protecting your privacy.

The types of Personal Data we may process include, but are not limited to:

- Identification data – such as your name, gender, photograph, date of birth, staff member IDs.
- Contact details – such as home and business address, telephone/email addresses, emergency contact details.
- Employment details – such as job title/position, office location, employment contract, performance and disciplinary records, grievance procedures, sickness/time-off records.
- Background information – such as academic/professional qualifications, education, CV/resume, criminal records data (for vetting purposes, where permissible and in accordance with applicable law).
- Government identifiers – such as government issued ID/passport, immigration/visa status, social security or national insurance numbers.
- Information on your spouse/partner and/or dependents – such as your marital status, identification and contact data about them and information relevant to any AEL benefits extended to such people.
- Financial information – such as bank details, tax information, withholdings, salary, benefits, expenses, company allowances, stock and equity grants.
- IT information – information required to provide access to company IT systems and networks (and information collected by/through those systems) such as IP addresses, log files and login information.

We may also process sensitive Personal Data relating to you (and your spouse/partner and/or dependents). Sensitive Personal data includes any information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, sexual orientation, trade union membership, criminal convictions, genetic data, biometric data for the purposes of unique identification, information about your health ("Sensitive Personal Data"). In the United States, Sensitive Personal Data also includes government identifiers (including social security, driver's license, state identification card, or passport number), citizenship or immigration status, and precise geolocation data. As a general rule, we try not to collect or process any Sensitive Personal data about you, unless authorized by law or where necessary to comply with applicable laws or to provide benefits. We do not sell Sensitive Personal Data collected under this Notice.

However, in some circumstances, we may need to collect, or request on a voluntary disclosure basis, some Sensitive Personal Data for legitimate employment-related purposes: for example,

information about your racial/ethnic origin, gender and disabilities for the purposes of equal opportunities (on the basis that it is in the public interest and in accordance with applicable law), monitoring, to comply with anti-discrimination laws and for government reporting obligations; or information about your physical or mental condition to provide work-related accommodations, health and insurance benefits to you and your dependents, or to manage absences from work.

## 3. Sources of Personal Data

Usually you will have provided the information we hold about you, but there may be situations where we collect Personal Data or Sensitive Personal Data from other sources. For example, we may collect the following:

- Certain background and other information from recruitment agencies, academic institutions, referees, background checking agencies and other third parties during your recruitment.
- Certain information on your performance, conduct or other information relevant to formal internal procedures (e.g. disciplinary or whistleblowing procedures), from customers or other organizations you routinely work with.
- Information on your training and development from external training partners and information about your experience and impressions of AEL through external survey providers.
- Information about your health, including your fitness to carry out work and/or any accommodations or adjustments to be considered from your doctor, other specialist medical adviser or other medical expert.
- Information on accidents or incidents from AEL's insurance brokers, insurers and their appointed agents, where they are involved.
- Information on tax payable from local tax authorities and AEL's appointed payroll agents and tax/financial advisers.
- Information collected through AEL's IT systems and other devices as set out in Section 2 above.
- Information about your entitlement to participate in, or receive payments or benefits under, any insurance or pension scheme provided by AEL from the relevant benefit provider or its appointed agent.
- Information from publicly available sources (e.g. news sources and/or from social media platforms) in connection with any investigation or formal procedure concerning the same (for instance, for the investigation of an allegation that a staff member has breached our rules on social media use or conduct generally).

## 4. Purposes for processing Personal Data

(i) Recruitment purposes

If you are applying for a role at AEL, then we collect and use your Personal Data primarily for recruitment purposes – in particular, to determine your qualifications for employment and to reach a hiring decision. This includes assessing your skills, qualifications and background for a particular role, verifying your information, carrying out reference checks or background checks (where applicable) and to generally manage the hiring process and communicate with you about it.

If you are accepted for a role at AEL, the information collected during the recruitment process will form part of your ongoing staff member record.

If you are not successful, we may still keep your application for internal reporting and to allow us to consider you for other suitable openings within AEL in the future.

(ii) Employment or work-related purposes

Once you become a staff member at AEL, we collect and use your Personal Data for the purpose of managing our employment or working relationship with you – for example, your employment records and contract information if you have a contract (so we can manage our employment relationship with you), your bank account and salary details (so we can pay you), your equity grants (for stock and benefits plans administration) and details of your spouse and dependents (for emergency contact and benefits purposes).

We process our staff members' Personal Data through a human resources system ("HR System"), which provides tools that help us to administer HR and staff member compensation and benefits and which allows staff members to manage their own Personal Data in some cases. This will involve transferring your Personal Data to our HR System provider's servers in the United States. AEL may host these servers or utilize third party servers, but in either case will be responsible for the security access of Personal Data on the HR System provider's servers in the United States.

(iii) Employee directory

We maintain a directory of all staff members which contain your professional contact details (such as your name, location, photo, job title and contact details). This information will be available to everyone in the AEL group of companies to facilitate coordination, communication and teamwork.

(iv) Other legitimate business purposes

We may also collect and use Personal Data when it is necessary for other legitimate purposes, such as:

- To help us conduct our business more effectively and efficiently – for example, for general HR resourcing, reporting or analytics, IT security/management, business continuity purposes, accounting purposes, or financial planning;
- To investigate violations of law or breaches of our own internal policies and more generally to protect the rights and interests of AEL, our employees, applicants and others. For instance, we may monitor your browsing or communications activity or location when using our devices or systems, if we suspect that you have been involved in phishing scams, fraudulent activity or activities in competition with or inconsistent with your work for AEL (for more information on such monitoring, refer to the Team Member Handbook).
- To help secure our networks and systems from unauthorized access, scams, and malicious code. For instance, we may monitor and review electronic mail communications sent or received using AEL issued devices or accounts, or stored on or using such a device or account. We may also monitor and record each website visit, each chat session, e-mail message, and each file transfer into and out of our systems and networks. AEL may monitor this activity at any time, and, to the extent permitted by laws, users of our networks and systems should not expect privacy when using these systems and devices.
- In accordance with any policies pertaining to the use of personal devices for work purposes. For instance, we may deploy security software on your personal device that monitors URLs for phishing risks and other security threats.
- To foster diversity, inclusion, and a welcoming work culture.

AEL also uses video cameras and recording equipment for its premises, offices, and facilities, and stores information captured by this equipment, in order to secure its networks, systems, and property, and may monitor access and use of its systems using this equipment.

AEL may also request or require you to enable your device used for work, whether personal or issued by AEL, to recognize facila or fingerprint IDs. Your biometric information will be stored on the device itself, and AEL will never transfer this data to its servers or to any third party. With respect to your personal device, this means that AEL will never collect or possess your biometric information. For company-issued devices, we will only store biometric information on the device itself and only on the basis of your explicit consent, and only for the period of time that such device is issued to you.

(v) Law-related and other purposes

We also may retain and use your Personal Data where we consider it necessary for complying with laws and regulations, including collecting and disclosing staff member Personal Data as required by law (e.g. for tax, health and safety, anti-discrimination and other employment laws), under judicial authorization, to protect your vital interests (or those of another person), or to exercise or defend the legal rights of the AEL group of companies.

## 5. Who we share your Personal Data with

We take care to allow access to Personal Data only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate business purpose or other lawful ground for accessing it. Whenever we permit a third party to access Personal Data, we will implement appropriate measures to ensure the information is used in a manner consistent with this Notice and that the security and confidentiality of the information is maintained.

(i) Transfers to other group companies

As mentioned above, we will share your Personal Data with other members of the AEL group in order to administer human resources, staff member compensation and benefits on the HR System, as well as for other legitimate business purposes such as IT services/security, tax and accounting, and general business management.

(ii) Transfers to third party service providers

In addition, we make certain Personal Data available to third parties who provide services to us. We do so on a "need to know basis" and in accordance with applicable data privacy laws.

For example, some of this information will be made available to:

- Our benefit/reward plans service providers (including retirement plan and medical insurance providers);
- Service providers who provide us with payroll, tax and expense administration support services;
- Providers of our HR Platform, including our recruitment platform;
- Service providers who provide, support and maintain our IT, security, and communications infrastructure (including for data storage purposes) and/or provide business continuity services;
- Service providers who assist in the coordination and provision of relocation, travel and/or travel permit services (in connection with work-related travel);

- Service providers who provide services in relation to staff training and/or qualifications and staff surveys; and
- Auditors, advisors, legal representatives and similar agents in connection with the advisory services they provide to us for legitimate business purposes and under a contractual prohibition of using the Personal Data for any other purpose.

(iii) Transfers to other third parties

We may also disclose Personal Data to third parties on other lawful grounds, including:

- Where you have provided your consent;
- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant;
- In response to lawful requests by public authorities (including for tax, immigration, health and safety, national security or law enforcement purposes);
- As necessary to establish, exercise or defend against potential, threatened or actual legal claims;
- Where necessary to protect your vital interests or those of another person; and/or
- In connection with the sale, assignment or other transfer of all or part of our business.

We do not sell the Personal Data we collect from and about you as described in Sections 2-4.

## 6. Data retention periods

Personal Data will be stored in accordance with applicable laws and kept as long as AEL has an ongoing legitimate business need to carry out the purposes described in this Notice or as otherwise required by applicable law. Generally this means your Personal Data will be retained until the end of your employment, employment application, or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries, comply with regulatory obligations, or to deal with any legal matters (e.g. judicial or disciplinary actions), document the proper deductions during and on termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits.

## 7. Updates to this Notice

This Notice may be updated periodically to reflect changes in our privacy practices. In such cases, we will indicate at the top of the Notice when it was most recently updated, and if we make a material change, we will inform you, for example, on our intranet or by company-wide email. We encourage you to check back periodically in order to ensure you are aware of the most recent version of this Notice. Please note that AEL does not discriminate against those who exercise their rights under applicable data protection laws.

## 8. Contact details

Please address any questions or requests relating to this Notice to Compliance@american-equity.com or alternatively, you can raise any concerns with your manager or HR Business partner. If you have disabilities, you may access this notice in an alternative format by contactingCompliance@american-equity.com.

# California Consumer Privacy Act Addendum

These provisions apply only to California consumers and supplement the Privacy Notice for Staff and Job Applicants. The California Consumer Privacy Act of 2018 ("CCPA"), including the California Privacy Rights Act of 2020 ("CPRA") and any regulations promulgated thereunder, provides California consumers with specific rights regarding their Information. This CCPA Addendum describes your rights under the CCPA and CPRA, explains how you may exercise your rights, and provides an overview on the types of Personal Information we collect.

General information regarding our collection, use, and disclosure of your data is detailed in the Notice that precedes this CCPA Addendum.

## Our Personal Information Collection Practices

The CCPA defines "Personal Information" as information that identifies, relates to, describes, references, or is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. To help consumers make informed privacy decisions, the CCPA classifies Personal Information into defined categories, and our practices regarding Personal Information are organized below into the aforementioned categories. Please note that some types of Personal Information may apply to multiple categories.

In the past 12 months, we have collected some or all of the categories of Personal Information described in the table below. The table below further describes the business or commercial purpose(s) for which the Personal Information was collected and the entities to whom such information has been disclosed within the last 12 months.

| Category | Examples | Purposes | Disclosed to |
|---|---|---|---|
| Identifiers | Name, alias, postal address, unique personal identifier, online identifier, internet protocol (IP) address, device, browser, email address, account name, or other similar identifiers | Recruitment; employment or work-related purposes; inclusion in the AEL Employee Directory; other business purposes set forth in Section 4 of the Notice | AEL group companies; service providers; public or governmental authorities |
| Customer records information | Name, signature, physical characteristics or description, address, telephone number, insurance policy number, education, employment, | Recruitment; employment or work-related purposes; inclusion in the AEL Employee Directory; | AEL group companies; service providers; public or governmental authorities |

| | | | |
|---|---|---|---|
| | employment history, or other similar information. Some personal information included in this category may overlap with other categories | other business purposes set forth in Section 4 of the Notice | |
| Characteristics of protected classifications under California or federal law | Age, race, color, ancestry, national origin, citizenship, religion or creed, marital or familial status, medical condition, physical or mental disability, sex, veteran or military status, genetic information, and other similar information | Recruitment; employment or work-related purposes | AEL group companies; service providers; public or governmental authorities |
| Biometric information | Fingerprints, facial or hand imagery, or voice recordings | Employment or work-related purposes (only for regulated personnel) | Service providers processing regulated personnel registrations; public or governmental authorities |
| Internet or other similar network activity information | Browsing history, search history, information regarding consumer's interaction with a website, application, or advertisement | Security and fraud prevention | AEL group companies; service providers |
| Sensory data | Audio, electronic, visual, or similar information | Security and fraud prevention; inclusion in the AEL Employee Directory | AEL group companies; service providers |
| Professional or employment-related information | Employer, employment history, resumes and CVs, background checks, and other employment-related information | Recruitment; employment or work-related purposes; inclusion in the AEL Employee Directory; other business purposes set forth in Section 4 of the Notice | AEL group companies; service providers; public or governmental authorities |

| | | | |
|---|---|---|---|
| Education information | Records maintained by an educational agency or institution that pertain to a student, such as grades and transcripts | Recruitment | AEL group companies; service providers |
| Sensitive personal information | Social security, driver's license, state ID, or passport number; racial or ethnic origin; union membership; biometric information; personal information concerning health, sex life, or sexual orientation. | Recruitment; employment or work-related purposes | AEL group companies; service providers; public or governmental authorities |

The Personal Information described in the table above is collected directly from you, or from the sources set forth in the Notice at Section 3, "Sources of Personal Data." In addition to the parties described above, we may disclose your Personal Information to other third parties for legal, security, or safety purposes; to regulatory authorities, courts, and government agencies if required by applicable law; or with a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, brands, affiliates, subsidiaries, or other assets.

We never sell your Personal Information, nor do we share it with third parties for the purposes of cross-context behavioral advertising. However, we may use de-identified, anonymized, or aggregated versions of your Personal Information for any purpose.

## Rights to your information

Right to Know

As a California consumer, you have the right to request that we disclose certain information to you about our collection, use, disclosure, or sale of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, and subject to certain limitations that we describe below, we will disclose such information. You have the right to request any or all of the following:

- The categories of Personal Information that we have collected about you.
- The categories of sources from which the Personal Information is collected.
- Our business or commercial purpose for collection, use, or disclosure of that Personal Information.
- The categories of third parties with whom we sell or share that personal information.

Right to Data Portability

You have the right to request a copy of Personal Information collected and maintained about you in the past 12 months. The CCPA allows you to request this information from us up to twice during a 12-month period. We will provide our response in a readily usable (in most cases, electronic) format.

Right to Delete

You have the right to request that we delete any of your Personal Information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your Personal Information from our records unless an exception applies. For example, we may deny your deletion request if retention of the Personal Information is:

- Necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Reasonably anticipated within the context of your employment or application for employment with us;
- For solely internal uses that are reasonably aligned with your expectations based on your relationship with us;
- Necessary to comply with a legal obligation; or
- Otherwise necessary for internal use in a lawful manner that is compatible with the context in which you provided the Personal Information.

Right to Correct

You have the right to request the correction of any Personal Information we maintain about you.

Right to Limit the Use or Disclosure of Sensitive Personal Information

You have the right to limit the use or disclosure of your Sensitive Personal Information ("SPI") if we are using your SPI beyond what is reasonable and proportionate within the context of your relationship with us as an employee or job applicant. You can make a request for us to limit the use or disclosure of your SPI by emailing us at Compliance@american-equity.com.

Right to Nondiscrimination

You have the right not to receive discriminatory treatment by us for the exercise of your CCPA privacy rights.

## Exercising your rights

To exercise the rights described above, please submit a request to us by emailing Compliance@american-equity.com.

After submitting a request, we will take steps to verify your identity in order for us to properly respond and/or confirm that it is not a fraudulent request. In order to verify your identity, we will request, at a minimum, that you provide your name, email address, address, and relationship to us, so that we can seek to match this information with the information existing in our systems. When providing us this information, you represent and affirm that all information provided is true and accurate. If we are unable to verify that the consumer submitting the request is the same individual about whom we have collected personal information, we may contact you for more information, or we may not be able to meet your request.

Only you, or an agent legally authorized to act on your behalf, may make a verifiable request related to your Personal Information. If you are making a request as the authorized agent of a California consumer, we will ask you also submit reliable proof that you have been authorized in writing by the consumer to act on such consumer's behalf.

We will make every effort to respond to your request within 45 days from when you contacted us. If you have a complex request, the CCPA allows us up to 90 days to respond. We may contact you within 45 days from the date you contacted us to inform you if we need more time to respond.

## Contact

If you have any questions, comments, or any complaints about how we use your information, or would like to exercise any rights that you may have under the CCPA, please reach out to us by using the contact information provided in Section 8 ("Contact Details") in the above Notice.