Select Equity Group, L.P. Privacy Notice for Job Applicants and Employees

Last Updated and Effective November 5, 2024

Select Equity Group, L.P. (the "**Firm**") has issued this Privacy Notice (this "**Notice**") to describe how we handle Personal Data (as defined herein) 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 the Firm. The term "**staff member**" includes those who work on a 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. This Notice does not limit in any way the Firm's policy of at-will employment.

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.

If you are a California resident, please click here for additional disclosures regarding the information we collect and any rights you may have under California law.

If you are a resident of the United Kingdom, please see Additional Information for Residents of the United Kingdom below.

Data We Collect

In the course of your employment at the Firm, 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, province, or country of residence, but we take the same approach to protecting your privacy regardless of where you reside.

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, personal and business 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, credit searches, social media, CV/résumé, 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 Firm 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, and 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 do not collect or process any Sensitive Personal Data about you, unless permitted 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 business or 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 investor reporting; 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.

For the avoidance of doubt, the Firm's use of any Personal Data and/or Sensitive Personal Data will comply with applicable law.

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, references, background checking agencies, and other third parties.
- 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 the Firm 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 the Firm's appointed medical expert.
- Information on accidents or incidents from the Firm's insurance brokers, insurers and their appointed agents, where they are involved.
- Information on tax payable from local tax authorities and the Firm's appointed payroll agents and tax/financial advisers and, if relevant, information related to court-required payments such as garnishments.
- Information collected through the Firm's IT systems and other devices as set out above.
- Information about your entitlement to participate in, or receive payments or benefits under, any insurance or pension scheme provided by the Firm, 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).

Purposes for processing Personal Data

1. Recruitment purposes

If you are applying for a role at the Firm, 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 the Firm, 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 the Firm in the future.

2. Employment or work-related purposes

If you become a staff member at the Firm, we collect and use your Personal Data for the purpose of managing our employment or working relationship with you – for example, your employment records (so we can manage our employment relationship with you), your bank account and salary details (so we can pay you), your non-cash compensation (if any) (deferral or other plan administration), and details of your spouse and dependents (for emergency contact and benefits purposes).

We process our staff members' Personal Data through one or more human resources systems ("**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. The Firm may host these servers or utilize service providers to do so.

3. The Firm directory

We maintain a directory of staff members which contains your professional contact details (such as your name, location, photo, job title, and contact details, including personal cell phone number). This information will be available to everyone in the Firm to facilitate cooperation, communication, and teamwork.

4. 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;
- as required for business needs – for example, in responding to "Know Your Customer" or other similar requests;
- to investigate violations of law or breaches of our own internal policies and more generally to protect the rights and interests of the Firm, 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 the Firm (for more information on such monitoring, refer to the Employee 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 Firm-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, newsgroup post, e-mail message, and each file transfer into and out of our systems and networks. The Firm may monitor this activity at any time, and, to the extent permitted by applicable 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; and
- to foster diversity, equity, inclusion, and a welcoming work culture.

The Firm may monitor access to and use of Firm technology and access to such technology (including location information), and may also use video cameras and recording equipment for its premises, offices, and facilities, and store 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.

The Firm may also request or require you to enable your device used for work, whether personal or issued by the Firm, to recognize facial or fingerprint IDs. Your biometric information will be stored on the device itself, and the Firm will never transfer this data to its servers or to any third party, except as set forth below. With respect to your personal device, this means that the Firm will never collect or possess your biometric information. For Firm-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. The Firm will adhere to any obligation it has under law to notify and bargain with the applicable bargaining representative before imposing such a requirement on represented employees.

5. 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 Firm.

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.

1. Transfers to other members of the Firm and affiliates

As mentioned above, we will share your Personal Data with other members of the Firm and its affiliates 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.

2. 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, including to:

- service providers who provide us with payroll, vendors who assist with deferred or other non-cash compensation, tax, benefits or benefits administration, 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.

3. 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.

Data retention periods

Personal Data will be stored in accordance with applicable laws and kept as long as the Firm 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 or 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.

Updates to this Notice

This Notice may be updated periodically to reflect changes in our privacy practices. We encourage you to check back periodically to ensure you are aware of the most recent version of this Notice. Please note that the Firm does not discriminate against those who exercise their rights under applicable data protection laws.

Contact details

Please address any questions or requests relating to this Notice to the Head of Human Capital or, alternatively, you can raise any concerns with your manager or the Legal team. If you have a

disability, you may access this notice in an alternative format by contacting privacyinquiry@selectequity.com.

Additional Information for Residents of the United Kingdom

How we collect information about you

We may collect Personal Data about you through:

- information provided directly to us by you, or another person on your behalf, through this website, or by email or post, or in person; or
- information that we obtain in relation to any transactions between you and us.

If you are a candidate for employment with the Firm, we may receive information from you directly (through this website), from a recruitment agency, or from references. We may also, in some circumstances, receive personal information about you from third parties, such as service providers or trading counterparties, regulatory or law enforcement agencies, credit reference agencies, and agencies conducting background checks. Personal information about you may also be obtained from publicly accessible sources of information, such as public databases, industry associations, social media, and online professional networks.

Why we collect information about you

We may collect and use your personal information for the purposes of recruitment, administering the relationship between us, monitoring and analysing our activities, reporting, and complying with applicable legal or regulatory requirements.

We will use one of the permitted grounds under applicable law to process your information. Such grounds include instances where you have given your consent and cases where your consent is not required under applicable law, such as where we are required to comply with a legal obligation, or where we, or a third party, determine that it is necessary for our legitimate interests to collect and use your personal information.

The legitimate interests to collect your personal information may include any of the purposes identified above and any other purpose where we or a third party have determined that you have a reasonable expectation for us or a third party to collect or use your personal information for such purpose. You have the right to object to the use of your Personal Data for direct marketing purposes.

The types of Personal Data we may collect and use

The categories of Personal Data we may collect will depend on the nature of our relationship with you and the purpose for which information is being collected. Such Personal Data may include names, titles or positions with your organisation, residential addresses, telephone numbers, email addresses or other contact details. If you are a candidate for employment, we may also collect your signature, nationality, date and place of birth, national insurance or other tax identification number, photographs, copies of identification documents, bank account details, information on your education, background and past employment, including any past employment disciplinary action taken against you. We may carry out background checks in the context of pre-employment screening and obtain information on your credit history, criminal and administrative offences, or other special categories of Personal Data (including health and disability) that may be contained in relevant documents or materials.

Do we use automated decision-making processes?

No.

Do we share your personal information with third parties?

We may (to the extent relevant to the purpose for which we collect your information), share your Personal Data with third parties, such as:

- our affiliates or other entities that are part of our group or with our clients;
- any person to whom we have a right or obligation to disclose Personal Data, or where we determine that disclosure is necessary to protect or defend our rights or property, including with regulators, courts of law, governmental, regulatory or law enforcement agencies;
- our Internet, IT, telecommunications, and other service providers, including legal advisers, accountants, payroll administrators, insurance and employee benefits providers, and administrators;
- service providers and trading counterparties to our clients, including placement agents or distributors, brokers, banks, trading venues, clearing houses, custodians, corporate services providers, administrators of our funds, and providers of customer relationship management tools;
- credit reference agencies and other third parties conducting background checks in the context of employment or client, counterparty, or investment due diligence;
- any person, as directed by you; or
- any person to whom we transfer any of our rights or obligations under any agreement, or in connection with a sale, merger, or consolidation of our business or other transfer of our assets, whether voluntarily or by operation of law, or who is otherwise deemed to be our successor or transferee.

Transfers of personal information to countries outside of the United Kingdom (UK)

Due to the international nature of our business, your Personal Data may be transferred to countries outside of the UK, such as to jurisdictions where we or our clients conduct business or have a service provider, including countries, such as the United States, that may not have the same level of data protection as that afforded by the UK General Data Protection Regulation or other data protection legislation applicable to us in the United Kingdom (collectively, "**Data Protection Law**"). In these circumstances, we take steps to ensure that the recipient agrees to keep your information confidential and that it is held securely in accordance with the requirements of Data Protection Law, such as by entering into legal agreements with service providers and between Firm group entities containing contractual requirements to comply with the Data Protection Law.

For how long do we keep your personal information?

We will generally keep personal information about you for as long as necessary in relation to the purpose for which it was collected, or for such longer period if required under applicable law or necessary for the purposes of our other legitimate interests.

The applicable retention period will depend on various factors, such as any legal obligation to which we or our service providers are subject as well as on whether you decide to exercise your right to request the deletion of your information from our systems. At a minimum, information about you will be retained for the entire duration of any business relationship we may have with you.

We will, from time to time, review the purpose for which we have collected information about you and decide whether to retain it, update it, or securely delete it, if the information is no longer required.

What are your rights?

You have certain rights under Data Protection Law with respect to the Personal Data we hold about you and which you may exercise. These rights are:

- to request access to your personal information;
- to request rectification of inaccurate or incomplete personal information;
- to request erasure of your personal information (a "right to be forgotten");
- to restrict the processing of your personal information in certain circumstances;
- to object to our use of your personal information, such as where we have considered such use to be necessary for our legitimate interests (e.g., in the case of direct marketing activities);
- where relevant, to request the portability of your personal information;
- where you have given consent to the processing of your data, to withdraw your consent; and
- to lodge a complaint with the competent supervisory authority.

Additional disclosures for residents of other countries

Individuals in Andorra, Argentina, Australia, Canada, Cayman, Faroe Islands, Guernsey, Hong Kong, Israel, Isle of Man, Japan, Jersey, Mexico, New Zealand, Singapore, South Korea, Switzerland, Uruguay, and certain other jurisdictions may have certain data subject rights. These rights vary, but they may include the right to: (i) request access to and rectification or erasure of their Personal Data; (ii) restrict or object to the processing of their Personal Data; and (iii) obtain a copy of their Personal Data in a portable format. Individuals may also have the right to lodge a complaint about the processing of Personal Data with a data protection authority.

If you make a request related to Personal Data about you, you may be required to supply a valid means of identification as a security precaution. We will process your request within the time provided by applicable law.

How to contact us

If you have any questions about this Notice or requests with regards to the Personal Data we hold about you, please send them to privacyinquiry@selectequity.com.

Complaining to ICO

You have the right to complain to the Information Commissioner's Office ("**ICO**"). Further information is available from the ICO's website.