

Privacy Policy for Job Applicants

FEBRUARY 2021



LSEG

ABOUT THIS NOTICE

Your privacy and trust are important to us. From 1 February 2021 this privacy policy (“**Notice**”) explains LSEG – London Stock Exchange Group (“**LSEG**,” “**we**,” “**us**,” “**our**” or the “**Company**”) will collect, handle, store and protect personal data (also referred to as personal information in some jurisdictions) about you when you are applying for a job at LSEG. It also provides information about your rights and how you can contact us if you have questions about how we handle your personal data.

WHO THIS NOTICE APPLIES TO AND WHAT IT COVERS

This Notice applies to individuals who use any website of ours that hyperlinks to this Notice (in each case the “**Website**”) or otherwise applies for or enquires about a job or similar employment related opportunities at LSEG.

For the purposes of this Notice, your job application or enquiry, your personal data and any other information we collect in connection with your application or enquiry is called “**Applicant Data**”.

This statement does not cover personal data which you may provide to LSEG when interacting with us otherwise than in relation to your job applications or related enquiries, for example when using one of our products or services. Our general Privacy Statement is available here: <https://www.lseg.com/privacy-and-cookie-policy>. If you are successful in your application to LSEG, once employed, your personal data will be processed in accordance with a separate employee privacy notice.

WHO WE ARE

LSEG is part of the LSEG group of companies, and is a global company that is made up of numerous legal entities. When you submit Applicant Data via the Website it becomes available to the LSEG group of companies. As set out below, your Applicant Data will then also be disclosed to the LSEG entity to whom you have applied or enquired. The LSEG entity responsible for the collection and processing of your Applicant Data in connection with your job application is the LSEG entity to which you apply for a job. Other LSEG group entities may also process your applicant Data in support of your job application on behalf of the entity to which you apply for a job.



LSEG

APPLICANT DATA WE COLLECT

We may obtain the following categories of Applicant Data from you, either directly as shared by you, or through other sources, such as our recruitment service providers or referees:

- **Identifiers:** such as real name, alias, signature, personal contact details, including home address, phone number, and email address, unique personal identifier (e.g., a device identifier, unique pseudonym, or user alias/ID), online identifier, internet protocol address, account name, Social Security number, driver's license number, national insurance number (or your local country equivalent) and other tax-related information, state identification card number, passport number, age/date of birth, and other similar identifiers
- **Demographic Information and Protected Classifications:** demographic information, which may include characteristics of protected classifications under U.S. federal or state law or other applicable national or local law, such as race or ethnic origin, national origin, religion, age, sex, gender, gender identity, sexual orientation, marital status, medical condition, disability, country of birth and residence, citizenship and immigration status (to determine if a work permit is required), and military and veteran status
- **Online Activity:** Internet and other electronic network activity information in connection with your use of the Company's facilities, equipment and websites, including, but not limited to, browsing history, search history, and information regarding your interaction with websites or applications
- **Sensory Information:** audio (e.g., interview recordings), electronic, visual (e.g., photographs, physical characteristics or description, CCTV footage), and similar information
- **Employment Information and provided Third Party Information:** talent management information, including occupation details, CV or resume information, education details, certifications and professional associations, language and other job-related skills, historical compensation details, previous employment details and references, financial information (where necessary for financial background checks), and pre-employment screening and background check information, including criminal records information, emergency contacts and details of any dependents, and any additional information that you choose to tell us or that your referees may provide about you
- **Inferences:** inferences drawn from any of the information outlined above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes

SOURCES OF APPLICANT DATA

We obtain Applicant Data from you:

- **through information you provide to us**, e.g. when you submit an application or enquiry for a job or you create a profile on our careers site. We may also ask you to provide original documents that verify your employment eligibility and identification
- **through your system/device.** We collect information that is automatically sent to us by your web browser when you visit or use the Website. This information typically includes the IP address of your Internet service provider and device type, the name of your operating system name and version of your browser
- **through cookies and similar technologies included on our Websites**, which is described in LSEG's [Cookie Policy](#)

We also collect Applicant Data from third parties where we ask individuals for whom you have provided us with contact details to provide employment references and where (if we are permitted to do so by law) we conduct pre-employment background checks which are carried out by professional third parties. In addition, we collect Applicant Data from recruitment agencies and, with your permission at the time of collection, we also collect personal data from employment-orientated social networking platforms and online job boards. Where Applicant Data is provided to us by our recruitment service providers or from another third-party source, and where such sources are the controllers of your data in their own right, this means they will make their own decisions about how your data is processed, and you should refer to their privacy notices and policies in respect of how they use your personal data.



LSEG

HOW APPLICANT DATA IS USED

In accordance with applicable law, Applicant Data will be used by LSEG for job application evaluation and processing purposes, more specifically, for:

Purposes	Categories of Personal Data
<p>Recruiting; processing job applications; assessing and verifying that the Applicant Data provided is true and accurate; performing background checks; determining suitability for employment; determining physical and/or mental fitness for work; reviewing and evaluating applications; managing and responding to any request or information you submit through our Website; determining salary and other forms of compensation; providing references; securing immigration statuses; reviewing hiring decisions; providing access to facilities; and retaining your record for future hiring needs, including for the purpose of communicating with you, building a relationship with you and learning more about your career interests, creating a candidate profile for you in our Recruitment system, processing for diversity and inclusion purposes where you have consented to providing data for this purpose, requesting additional information, if required, assessing your suitability for other current and future roles at the LSEG Group and providing you with information regarding potential career opportunities that may suit you.</p>	<ul style="list-style-type: none"> - Identifiers - Demographic Information and Protected Classifications - Online Activity - Sensory Information - Employment Information and provided Third Party Information - Inferences
<p>Ensuring business continuity; protecting the health and safety of our staff and others; safeguarding, monitoring, and maintaining our IT infrastructure, Company equipment, facilities, and other property; detecting security incidents; detecting, preventing or protecting against malicious, deceptive, fraudulent, or illegal activity and prosecuting those responsible for that activity.</p>	<ul style="list-style-type: none"> - Identifiers - Demographic Information and Protected Classifications - Online Activity - Sensory Information - Employment Information and provided Third Party Information - Inferences
<p>Operating and managing our IT, communications systems and facilities, and monitoring the use of these resources; performing data analytics; reporting activities, including visitor activity and demographics reports, performing and improving our services, such as our Website and recruitment methodologies, as well as personalizing the content which is presented to you on the Website; debugging to identify and repair errors that impair existing intended functionality; auditing related to a current interaction with you and concurrent transactions; undertaking internal research for technological development and demonstration; undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance our services; allocating and managing company assets and human resources; managing our HR records and updates to our employee database; strategic planning; project management; assisting us in managing external providers (e.g., recruitment agencies); compiling audit trails and other reporting tools; maintaining records relating to business activities, budgeting, and financial management; managing mergers, acquisitions, sales, reorganizations or disposals and integration with business partners.</p>	<ul style="list-style-type: none"> - Identifiers - Demographic Information and Protected Classifications - Online Activity - Sensory Information - Employment Information and provided Third Party Information - Inferences



Purposes	Categories of Personal Data
Complying with legal requirements, such as record-keeping and reporting obligations, including equal employment opportunities monitoring; ensuring that applicants meet applicable regulatory standards for their prospective role; conducting audits; management and resolution of health and safety matters; complying with requests from government or other public authorities; responding to legal process such as subpoenas and court orders; pursuing legal rights and remedies; defending litigation and managing complaints or claims; conducting investigations; and complying with internal policies and procedures.	<ul style="list-style-type: none"> - Identifiers - Demographic Information and Protected Classifications - Online Activity - Sensory Information - Employment Information and provided Third Party Information - Inferences

Where appropriate and in accordance with local law, we collect sensitive personal data about your racial or ethnic origin, gender identity, disability, age and/or sexual orientation to ensure our practices align to our equal opportunities policy, where you have chosen to “self-identify” to us, (for more information here, please see the Sensitive Applicant Data section below), and to fulfil applicable legal and/or regulatory reporting requirements.

WHAT LAWFUL BASIS WE RELY ON TO PROCESS APPLICANT DATA

Some laws require us to explain our lawful reason for processing your personal data. Subject to applicable law, we process personal data about you on the basis that it is:

- in our legitimate interests and does not unduly affect your interests or fundamental rights and freedoms, for example to:
 - o assess your application and evaluate your suitability for the role applied for;
 - o collect statistical information about your use of our Websites and to better understand Website visitors' interests and to improve the content and functionality of our Websites;
 - o inform you about new job opportunities which you may be interested in;
 - o assess and verify that the information you have provided is true and accurate (e.g., by means of reference checks);
 - o protect the health and safety of visitors to our premises;
 - o ensure the security of LSEG premises and safeguard Company equipment, facilities and other property; and
 - o benefit from cost-effective services (e.g. we may opt to use certain IT platforms offered by suppliers).
- for compliance with a legal obligation (e.g., to respond to a court order or a regulator); and
- necessary to perform our contractual obligations towards you or to take pre-contractual steps at your request, such as preparing a contract of employment for you following a decision to make you an offer of employment.

To the extent that we process any sensitive personal information relating to you for any of the purposes outlined below, we will do so because either: (a) you have given us your explicit consent to process the information; (b) the processing is necessary to carry out our obligations under employment, social security or other applicable law; or (c) the processing is necessary for the establishment, exercise or defence of legal claims.

In some cases, the personal data we collect from you is needed to meet our legal or regulatory obligations and, if your application is successful, to enter into an employment contract with you. If you fail to provide any personal data that we request, we may be unable to continue evaluating your application, comply with our legal and regulatory obligations, or offer you employment.

SENSITIVE APPLICANT DATA

Depending on applicable law, sensitive personal data may include information about your racial or ethnic origin, caste and tribe, political opinions, religious or philosophical beliefs, party or trade-union membership, health, sexual orientation, genetic and biometric information, addictions or sex life, or criminal records/history. Please do not submit sensitive personal data in connection with a job application or personal profile unless it is clearly and specifically requested. If you are asked to provide any of these types of information, it will be processed for the purposes described in this Notice and in accordance with applicable laws.

In accordance with applicable law, you may be asked to provide certain sensitive personal data:

- in connection with equal opportunities and/or human resource initiatives (e.g., gender, race or ethnicity information);
- for accessibility and ‘fit for work’ purposes (e.g., health or medical information); and
- if required to do so under applicable local law, governmental requirements or regulations.

You may also be given the choice to offer additional “self-identification” information, containing sensitive personal data, if you wish to do so. As appropriate and in accordance with local law, where you choose to self-disclose information in this way, it will be used for diversity and inclusion purposes, including reporting on an anonymised, aggregated basis to monitor and manage our compliance with our equal opportunities policy and to fulfil applicable legal and/or regulatory reporting requirements.



LSEG

In accordance with applicable law, LSEG may disclose this “self-identification” data externally, but only on an anonymised, aggregated basis, and only for limited purposes, such as to report on diversity and inclusion statistics to our customers or in connection with industry surveys. Self-identification data will not be used to make decisions regarding recruitment and hiring. If you are hired, the processing of such self-identification data will be subject to the employee privacy notice that will be provided to you upon joining LSEG.

Where permitted by law and/or required locally, a medical questionnaire and/or standard medical exam (or medical exam determined by LSEG) and/or a drug test may be requested by LSEG as part of the application process. Also, where permitted by local laws, we may undertake background checks, including conviction searches and verification of the information you have provided.

We do not collect your sensitive personal data unless we need to obtain this information to comply with applicable law or to perform our obligations in connection with your potential employment, or, to the extent required by applicable law, you have provided your explicit consent to the collection and processing of your sensitive personal data.

HOW WE SHARE APPLICANT DATA

Where permitted by applicable law, we may share Applicant Data for the purposes set out in this Notice, with the following categories of recipients:

- LSEG personnel, agents and contractors involved in the job application and recruitment processes;
- LSEG group companies;
- third parties that provide services to us such as analytics providers, IT and technical support, hosting providers, payment service providers, human resource services providers and companies who provide employment verification, reference and/or background check services and/or criminal checks (where such checks are appropriate and in accordance with applicable law), and if a job offer is extended, service providers assisting in the hiring process;
- third parties with information related to your reference or application (for example, current or past employers and educational institutions);
- professional advisors (such as lawyers, accountants and consultants);
- third parties in order to participate in, or be the subject of, any sale, merger, acquisition, restructure, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings), in which case we may disclose your personal data to prospective buyers, sellers, advisers or partners and your data may be a transferred asset in a business sale;
- third parties (i) where reasonably required to protect or defend our rights, (ii) when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss, or (iii) in connection with an investigation of suspected or actual fraudulent or other illegal activity; these third parties may include, legal counsel and information security professionals; and
- competent authorities (including any national and/or international regulatory or enforcement body, courts or other tribunal) where we, or any member of the LSEG group are required to do so by applicable law or regulation. We act responsibly and take account of your interests when responding to any such requests.

Where appropriate, and in accordance with applicable law, we will have entered into legally binding agreements requiring the above-mentioned recipients to use or disclose Applicant Data only as necessary to perform services on our behalf for the purposes described in this Notice, or to comply with applicable legal or regulatory requirements.

INTERNATIONAL TRANSFERS

Your Applicant Data will be added to our international resume database, which is currently located in the European Union. Your Applicant Data will also be processed by the LSEG entity with whom you are seeking employment in whichever country it is located. Additionally, LSEG has networks, databases, servers, systems, support and helpdesks around the world. We collaborate with third parties like cloud hosting services, suppliers and technology support located around the world to serve the needs of our business, workforce and customers.

In some cases, we may need to disclose or transfer your personal data within LSEG or to third parties in areas outside of your country. These countries may not have the same data protection laws or provide an equivalent level of protection to the laws in the country in which you initially provided your personal data. In instances where LSEG discloses Applicant Data to such recipients, it will establish or confirm that appropriate protections are in place for such data transfers that meet the requirements of applicable data protection laws.

Consistent with this goal, we have put in place safeguards in accordance with applicable law (including the EU Standard Contractual Clauses, as approved by the European Commission). If you would like to know more about our data transfer practices and obtain copies of any relevant safeguarding measures, please contact us using the details below.

RETENTION OF APPLICANT DATA

We retain your information in accordance with our records retention schedule. Retention periods are calculated based on a number of factors such as the length of time necessary to fulfil the purposes for which we collected your Applicant Data, to be able to

appropriately response to queries, complaints or challenges, and to comply with any local laws which require Applicant Data to be retained for a specific period of time, including but not limited to compliance with legal, tax and accounting obligations.

Information relating to successful candidates is dealt with by the employee privacy notice that will be provided to you upon joining LSEG.

PROTECTION OF YOUR APPLICANT DATA

We will hold your Applicant Data securely whilst it is under our control, including where it is processed by third-party service providers on our behalf. We train our employees in respect of their obligations under data protection laws, and we ensure that only relevant LSEG employees, contractors and agents have access to your Applicant Data.

We take the security of our physical premises, our servers and our Websites seriously and we will take all appropriate technical measures using recognised security procedures and tools in accordance with good industry practice to protect your Applicant Data across all of these platforms.

Whilst we use all reasonable endeavours to protect your security in the manner described above, we consider that it is only appropriate to advise you that data transmission over the Internet and the World Wide Web cannot always be guaranteed as 100% secure, and therefore that you use our Websites and send us communications over the Internet at your own risk.

YOUR RIGHTS

We will honour your rights under applicable data protection laws. You may have the following rights under European laws and may have similar rights under the laws of other countries.

- **Right of subject access:** The right to make a written request for details of your personal data and a copy of that personal data.
- **Right to rectification:** The right to have inaccurate information about you corrected or removed.
- **Right to erasure ('right to be forgotten'):** The right to have certain personal data about you erased.
- **Right to restriction of processing:** The right to request that your personal data is only used for restricted purposes, where:
 - o the accuracy of the personal data is contested;
 - o the processing is unlawful but you object to the erasure of the personal data;
 - o we no longer require the personal data, but it is still required for the establishment, exercise or defense of a legal claim.
- **Right to object:** The right to object to processing of your personal data in cases where our processing is based on the performance of a task carried out in the public interest or we have let you know the processing is necessary for our or a third party's legitimate interests, or to object to direct marketing, or to object to decisions based solely on automated processing or profiling which produce legal effects concerning you or similarly significantly affect you.
- **Right to data portability:** The right to ask for the personal data you have made available to us to be transferred to you or a third party in machine-readable format.
- **Right to withdraw consent:** The right to withdraw any consent you have previously given us to handle your personal data. If you withdraw your consent, this will not affect the lawfulness of our use of your personal data prior to the withdrawal of your consent.

These rights are not absolute, and they do not always apply in all cases.

If you request the deletion of your personal data and you are a U.S.-based candidate, it will be retained in accordance with applicable laws regarding record retention, but you may withdraw your employment application at any time and LSEG will make your record inactive.

In response to a request, we will ask you to verify your identity if we need to (and to the extent permitted by applicable law), and to provide information that helps us to understand your request better. If we do not comply with your request, whether in whole or in part, we will explain why.

In order to exercise your rights please contact the Data Protection Team at DataProtection@lseg.com.

QUESTIONS

Any questions you have about this Notice should be sent to DataProtection@lseg.com.

If you are not satisfied with the response, we encourage you notify the Data Protection Team of your dissatisfaction via the same contact address and the matter will be escalated internally.

If you are not content with how LSEG manages your personal data, you can lodge a complaint with a privacy supervisory authority. In the European Economic Area, the relevant supervisory authority is the one in the country or territory where:

- you reside,
- you work, or
- the alleged infringement took place.

A list of National Data Protection Authorities in the European Economic Area can be found here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

For the Information Commissioner's Office in the United Kingdom, please visit <https://ico.org.uk/>.

CHANGES TO THIS PRIVACY NOTICE

This Notice may be subject to updates. Any material future changes or additions to the processing of personal data as described in this Notice affecting you will be communicated to you through an appropriate channel. For example, we may place a prominent notice on a product site, on our careers site or email you to let you know of an updated Notice.



LSEG