LSEG Global Employee Privacy Notice

LSEG (which includes London Stock Exchange Group plc, LCH Limited and other companies within the London Stock Exchange Group, collectively referred to as “Company”, “we”, “us”, or “our”) is a global business with networks, databases, servers, systems, support and help desks located around the world.

This Notice applies to current and former employees, workers, interns, agency workers, consultants, individual contractors, directors as well as any family members and beneficiaries, whose data (collectively, “Employee Personal Data”) you provide to us in connection with your engagement with LSEG (e.g., for the purposes of emergency contact information or in relation to entitlement to staff benefits).

As part of normal business, Employee Personal Data may be transferred to or accessed by LSEG and/or third parties around the world, as described in this Global Employee Privacy Notice (“Notice”).

Whilst your LSEG employing entity will be the primary controller of your personal data, other entities within the LSEG Group may also process your personal data from time to time, consistent with the purposes set out in this Notice.

Employee Personal Data is protected by an Intra-Group Agreement (IGA) between all LSEG operating entities. The IGA provides specific safeguards when Employee Personal Data is processed or transferred within LSEG worldwide.

This Notice does not form part of any contract (including any contract of employment or engagement) and does not confer any contractual right on you or place any contractual obligation on us.

If you have questions about this Notice, please contact your manager, your Human Resources contact (“HR Contact”), or the Privacy Office.

Table of Contents

PURPOSE AND SCOPE OF THIS NOTICE

This Notice outlines Company practices regarding the collection, processing, and use of Employee Personal Data

This Notice applies to Employee Personal Data processed and stored in global HR systems and Employee Personal Data that is collected and sent through LSEG's' network. In the event of a conflict between this Notice and local Human Resources policies or practices, this Notice will override. For more information about how Employee Personal Data is handled locally, please contact your HR Contact.

The Company collects and processes Employee Personal Data fairly, transparently, in good faith and in accordance with applicable laws.

SYSTEMS AND APPLICATIONS USED TO STORE EMPLOYEE PERSONAL DATA

Below is a representative list of the primary global databases and systems holding Employee Personal Data. This list, which is not all-inclusive, may change from time to time when the Company changes platforms, information systems and/or third-party service providers:

- Learning and development platforms
- Payroll provider systems and services support, including from TCS
- IT Support including from ServiceNow
- Travel support including from CWT and MyTravel
- Workday
- Approved 3rd party cloud services, e.g., Microsoft Office 365, SharePoint
- Company employee participation benefits and provider systems
- Other internal administrative systems and databases necessary to operate the business (e.g., internal directory, Condeco, Physical access control system (PACS), financial administration systems, compliance systems)

TYPES OF EMPLOYEE DATA THE COMPANY COLLECTS

The Company may collect, use, store, and otherwise process certain Employee Personal Data, as set out in this Notice, and including, for example:

- Name
- contact information (work and personal, including home and office postal and email address(es), home and office phone number(s) and mobile phone number(s))
- country of residence
- date of birth, country or place of birth, social security or other governmental identification number, national insurance number, gender, marital status
- education
- citizenship and passport information
- bank account information
- immigration and right to work data (including but not limited to visa, deputation letter, country resident permits, citizenship, evidence of address)
- work locations
- photographs, images, videos and/or voice recordings stored on corporate systems
- driver’s license details and driving records
- credit card information when sent via Company networks
- data related to an employee’s family members and dependents
- CV, application information, records of interview or interview notes, references and vetting and verification documentation, psychometric and competency-based test data as more fully detailed in the Privacy Policy for Job Applicants

TYPES OF EMPLOYEE DATA THE COMPANY COLLECTS DURING THE COURSE OF THE EMPLOYMENT

- position/ title, grade, job description and assigned business unit or group, location(s)
- employee identification number
- emergency contact / next of kin
- languages spoken
- start and end dates of employment
- supervisor/manager
- reporting lines / reporting structure
- employment status (full-time or part-time)
- salary and benefits package
- bonus information and tax information
- pension contributions and pension scheme certificate
- equity awards, where applicable
- share options and grants, as applicable
- employee discount programme
- company car and fuel allowance, mobile phone usage allowance
- benefits or support information, including third party benefit recipient information, which may include health or medical information
- incapacity data (and related health data) and/or pregnancy, maternity, paternity or adoption information, where permitted by applicable law, and as may be included in received medical forms, reports and certificates
- working hours, locations, attendance records, and terms and conditions of employment/engagement
- employee claims complaints and/or disclosures data, staff involvement in incident reporting and/or disciplinary and grievance information including, for example, warning letters, records, investigations, and outcomes information
- job performance and/or related evaluative information, including, for example, input information from colleagues and manager feedback, assessments, appraisals, and outputs, training and development information, competency and learning information, apprenticeship schemes
- certifications, practicing certificates, unique regulatory identifiers, course completion data and marks
- payroll information

- vacation allotment, leave and absences
- restructuring, termination and/or exit data, including for example, information processed in connection with redundancy, layoff or termination arrangements and payments, exit interviews and references
- health and safety information, where permitted by applicable law, personal data in audits, health assessments, (where required, for example, as a result of exposure to hazardous substances), or other data collected or processed as part of our pandemic, major event, health and safety or other business continuity management planning
- use of the Company's facilities and equipment, including laptops, mobile devices, notably computer and telecommunications systems, to the extent permitted by applicable law
- building security, access control, and monitoring data including CCTV, system and building logs and access records, keystrokes, download and print records, call recordings, data captured by corporate IT security systems and filters, and were permitted by applicable law, body temperatures and other data (where required, for example as part of our pandemic management and planning)
- records (including logs) and contents of communications sent over Company networks, such as emails, instant messages, and visits to external websites. Such records are maintained in accordance with the Company Code of Conduct, other Company policies and applicable law

Any other personal data which you disclose during the course of your employment or engagement, whether verbally as recorded or in written form (including, for example, on work emails), opinions you have shared in the context of your professional communications or work conduct, and informal data including opinion data generated in the course of your employment or engagement, including where related to the administration or management of our relationship with you.

WHY THE COMPANY COLLECTS AND PROCESS EMPLOYEE DATA

The Company may process such data for various human resources, employment and/or data security/facilities-related purposes, and other similar purposes, including these below:

Purpose of personal data processing:	**Legal bases for processing:**
Processing in the context of recruiting or engaging with relevant personnel, including secondments, internal assignments, and other recruitment decisions. Processing activities may include: • Carrying out candidate evaluations. We may use techniques such as artificial intelligence and machine learning to process	• Processing as is necessary for contract performance, or taking steps prior to entering into a contract with you • Our legitimate interests as a business and as an employer for engaging personnel to roles and opportunities within the business

Purpose of personal data processing:	**Legal bases for processing:**
and analyse data for recruitment purposes. There will never be any automated decision-making; all decisions will involve a manual review. • Reviewing and acting in respect of provided information shared in the context of role application • Creating, maintaining, and updating staff records • Any background checks applicable to role and in accordance with applicable laws • Reviewing eligibility to work and immigration status	• Processing as is necessary for compliance with a legal obligation which LSEG is subject to • With your consent in appropriate circumstances (e.g. completion of voluntary information, which you can withdraw at any time with no effect on your employment or relationship with LSEG).
In context of offering/ providing support, and provision of work tools and equipment that allow performance of personnel duties and the carrying out of role commitments, including: • Processing in the context of performance of job role requirements • Creation of logs, records, work materials • Internal and external communications, • Applications, recordings, records and /or certifications completed or carried out in the course of personnel duties • Technical support • Employee surveys • Subject to applicable laws, monitoring and enforcing compliance with Company policies and procedures for example analysis of attendance records to establish compliance with the Hybrid policy, legal requirements /obligations or in connection with workplace or law enforcement investigations • Processing in support of any claim, defence or declaration in a case or before any jurisdictional and/or administrative authority, arbitration or mediation panel, including but not limited to creation of relevant materials, witness statements and complying with court process	• Processing as is necessary for contract performance • Our legitimate interests as a business and as an employer for providing a suitable environment for carrying out work duties • Processing as is necessary for compliance with a legal obligation which LSEG is subject to • With your consent in appropriate circumstances (e.g. completion of voluntary information, which you can withdraw at any time with no effect on your employment or relationship with LSEG)

Purpose of personal data processing:	**Legal bases for processing:**
• Processing in taking reasonable steps to safeguard against or report sexual harassment, bullying, discrimination and/or criminal offenses • Processing in the context of arranging/participating in/following up in respect of Corporate Social Responsibility (CSR) events and volunteer days • To safeguard against discrimination and take appropriate and reasonable steps for equality of opportunity and access • In considering requests for, and processing in the context of the flexible working scheme or workstyle • Training records, courses, and programmes • To the extent permitted by applicable law, addressing occupational health issues, incapacity at work and making reasonable adjustments • Dealing with complaints, grievances and processing in the context of disciplinary processes and investigations • Managing professional certifications, annual certifications, practicing certificates, liaising with regulatory bodies on your behalf • Maintaining and use of emergency contact details • To confirm, maintain or monitor work-related licenses and credentials • Business administration, group-wide and senior management reporting and assessments • Making travel arrangements for work purposes • Processing in connection with corporate transactions, mergers or acquisitions	

Purpose of personal data processing:	**Legal bases for processing:**
For the purpose of carrying our employer commitments, processing the context of the managing and supporting personnel relationships, and wellbeing, including: • Workflow management, such as assigning, managing, and administering projects • Project costing and estimates • Compensation, including stock plan administration • Payroll, tax, expenses, and bonuses processing • Pensions processing (including but not limited to trustee disclosures) • Performance management • Succession planning • Benefits/welfare administration, including health and medical benefits, employee assistance (including where entitled, for relatives, spouses, next of kin etc.) • Processing for insurance, and for leave entitlements, • Personnel administration • Travel reservations and planning, including support to staff with relocations • Training records, courses, and programmes • Employee directories • Technical support • Employee surveys • Subject to applicable laws, monitoring and enforcing compliance with Company policies and procedures, for example analysis of attendance records to establish compliance with the Hybrid policy, legal requirements/obligations or in connection with workplace or law enforcement investigations • To support any claim, defense or declaration in a case or before any jurisdictional and/or administrative authority, arbitration or mediation panel	• Processing as is necessary for contract performance • Our legitimate interests as a business and as an employer for providing a suitable environment for carrying out work duties • Processing as is necessary for compliance with a legal obligation which LSEG is subject to • With your consent in appropriate circumstances (e.g. completion of voluntary information, which you can withdraw at any time with no effect on your employment or relationship with LSEG)

Purpose of personal data processing:	**Legal bases for processing:**
• To monitor detect, investigate, respond to and prevent sexual harassment, bullying, discrimination and/or criminal offenses • Processing in the context of arranging/participating in/following up in respect of Corporate Social Responsibility (CSR) events and volunteer days • To safeguard against discrimination and take appropriate and reasonable steps for equality of opportunity and access • In considering requests for, and processing in the context of the flexible working scheme or workstyle • To the extent permitted by applicable law, addressing occupational health issues, incapacity at work and making reasonable adjustments • Dealing with complaints, grievances, and processing in the context of disciplinary processes and investigations • Use of emergency contact details • Business administration, group-wide and senior management reporting and assessments • To administer employment restructuring or termination and providing references • To investigate or respond to complaints from customers or members of the public Processing in connection with corporate transactions, mergers. or acquisitions	
For meeting legal and regulatory requirements, including: • To safeguard against discrimination and ensure equality of opportunity and access • In responding to requests or orders from courts; law enforcement, regulators, government agencies, parties to a legal proceeding or public authorities, to comply with regulatory requirements or part of dialogue with a regulator	• Processing as is necessary for compliance with a legal obligation which LSEG is subject to • Our legitimate interests as a business in responding to regulators and Government information requests

Purpose of personal data processing:	**Legal bases for processing:**
• To exercise our rights to defend, respond to or conduct prospective or actual legal claims or proceedings	
In support of our diversity and inclusion initiatives and in accordance with our equal opportunities monitoring programme, including: • Making available Workday options to complete on personnel own Workday records • Responding to employee surveys • To the extent permitted by applicable law, in conducting an equal opportunity monitoring programme	• Processing as is necessary for compliance with a legal obligation which LSEG is subject to • Our legitimate interests as a business in taking steps to create a diverse and inclusive working environment, and working to support equal opportunities in line with policy
Wellbeing, Health, and Safety, including: • To the extent permitted by law, to manage wellbeing, health and safety at work, and to facilitate public health and safety, including but not limited to assessments and reporting, sending and responding to personnel communications, creating appropriate training and performing checks to confirm completion of required training • Incident investigations and reports • Managing and planning, including for business continuity purposes, pandemic, and other major event as well as monitoring for return to office policy and practice	• Processing as is necessary for contract performance • Our legitimate interests as a business and as an employer for providing a suitable environment for carrying out work duties • Processing as is necessary for compliance with legal or regulatory obligations which LSEG is subject to, and company policies, as appropriate • With your consent in appropriate circumstances (e.g. completion of voluntary information, which you can withdraw at any time with no effect on your employment or relationship with LSEG)
Audit, forensic investigations and responding to whistle-blowing allegations, including: • Conducting audits • Carrying out and reporting on forensic investigations • Reviewing, assessing, investigating, and responding to whistle-blowing allegations	• Processing as is necessary for contract performance • Our legitimate interests as a business and as an employer for providing a suitable environment for carrying out work duties, and acting appropriately to support our staff, and to protect and defend our business interests • Processing as is necessary for compliance with legal obligations to which LSEG is subject

Purpose of personal data processing:	**Legal bases for processing:**
Security/Facilities, including: • Facilities management and reporting • Subject to applicable laws, monitoring and enforcing compliance with Company policies and procedures, legal requirements /obligations or in connection with workplace or law enforcement investigations • Hosting and maintenance of corporate systems, sites, and infrastructure • To maintain appropriate security (technical, physical, and cyber) to protect work assets, people, premises, systems and sites • Management of company assets and infrastructure • Protection of employee, customer, prospective customer, and other Personal Data, including through its data leakage protection programme • Protection of the Company's networks, systems, databases, hardware and intellectual property assets, including through its data leakage protection programme • Tools designed to support compliance with company security policies and processes, to prevent, detect and investigate security issues, to provide spam protection, and to prevent malicious communications. Artificial intelligence and machine learning may be used to support with this. • Business continuity measures and planning • Virus protection and pandemic management • System testing • To monitor staff use of systems, records, IT and communications consistent with the law and LSEG internal policies • Processing to assess data breach reports or system breach reports	• Processing as is necessary for contract performance • Our legitimate interests as a business and as an employer for providing a suitable environment for carrying out work duties, and acting appropriately to support our staff and protect and defend our business interests, including, without limitation, monitoring compliance with Company policies • Processing as is necessary for compliance with legal obligations to which LSEG is subject

Purpose of personal data processing:	Legal bases for processing:
• To use CCTV and physical access control systems to protect the security of our offices and other buildings	

We only process your Personal Data where applicable law permits or requires it, including where the processing is necessary for the performance of our employment arrangement with you, where the processing is necessary to comply with a legal obligation that applies to us as your employer, for our legitimate interests or the legitimate interests of third parties, to protect your vital interests, where there is a valid public interest, or with your consent if applicable law requires consent. Where consent is offered, it shall be possible to withdraw your consent at any time without affecting the lawfulness of the processing based on the consent before its withdrawal. Where personal data is required from you for contractual or statutory purposes (i.e. where statutory, to comply with a legal requirement), it shall be made clear to you with the contract or request which data is mandatory to provide, and the possible consequences of not providing such data. For those employees in the European Economic Area, to the extent that the Company has in the past obtained your consent to process your Personal Data as may be outlined in an offer letter, employment contract or other similar employment arrangement, that consent is hereby waived or extinguished, and the Company will instead rely on the lawful grounds for processing as specified in this Notice.

Sensitive (special categories) Personal Data

The Company may also collect, process and use Employee Personal Data or protected characteristics (equality and diversity data) that are considered “sensitive”, which may include (depending on applicable law) data about an employee’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, nationality or citizenship, veteran status, genetic data, biometric data for the purpose of uniquely identifying a natural person, health-related data or disabilities requiring work accommodations, data regarding sex life or sexual orientation[1].

The Company may need to collect this data to comply with applicable laws; to administer or facilitate health, medical or other employee benefits/welfare; to administer sick leaves or other absences; to protect its networks, systems, equipment, and data; to protect employee, customer, prospective customer, and other Personal Data; in connection with the Company’s diversity and inclusion initiatives; and/or to protect health and safety in the workplace.

[1] The list of examples will vary in different jurisdictions.

In accordance with applicable law, the Company may also conduct background checks which may include data about an employee's criminal history, drug testing, credit and/or public records. Such data may be collected to comply with customer obligations, recruitment and/or for legal compliance purposes.

To the extent that we process any **sensitive (special categories) personal data** relating to you for any of the purposes outlined here, we will do so because:

a) you have given us your explicit consent to process the data (for example, voluntary programmes within LSEG which you are free to choose to participate in, and from which you can withdraw at any time, with no effect on your employment or relationship with LSEG);

b) the processing is necessary to carry out our obligations under employment, social security or other applicable law (for example, making reasonable work-place adjustments for disabilities, or sensitive personal data processing as part of our pandemic management and planning);

c) the processing is necessary for reasons of substantial public interest, including applicable processing pursuant to our equal opportunities policy;

d) where circumstances apply, where it is necessary to protect your or another person's vital interests, (e.g. in providing assistance in medical emergency situations) or where the processing is of personal data which you have manifestly made public;

e) where processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

f) where processing is necessary for reasons of substantial public interest, including in the area of public health/ safety, such as protecting against serious cross-border threats to health and/ or and on the basis of applicable law, where it is proportionate to the aim pursued and specific measures are in place to protect your data subject rights;

g) where the pressing is necessary for the working capacity of the employee including preventive or occupation medicine, medical diagnosis, provision of health/welfare or social care or treatment;

h) where it is necessary for an assessment of your working capacity (e.g. in carrying out occupational health assessments);

i) where it is necessary for archiving purposes in the public interest, or for scientific, historical research or statistical purposes;

j) or is in accordance with the data protection laws applicable to the processing activities, in processing of racial and ethnic diversity data of the organisation.

HOW IS EMPLOYEE PERSONAL DATA COLLECTED?

Directly from the employee: The Company typically collects Employee Personal Data directly from job candidates and employees through the application and background check process, or in respect of disclosures we ask you to make during your engagement as more fully detailed in the Group Vetting Policy, or from an employment agency or background check provider in connection with an individual's employment. (For job candidate, the Privacy Policy for Job Applicants apply).

From third parties: The Company sometimes collects data indirectly or from others when permitted by law; including references, former managers, and other references or data from third parties e.g. mortgage references, social media and sanctions screens, and others such as from credit reference agencies or background check agencies. We also receive data which may include your personal data from your managers (for example, in respect of performance reviews) or from time to time, from other colleagues, (for instance when they provide feedback about you or in the course of reporting or investigating a complaint/disciplinary issue).

From time to time, we may receive data including personal data about you from other third parties, for example, customers, members of the public, regulatory bodies, and LSEG business partners or vendors.

If you work for a business acquired by LSEG, we may receive data about you in the context of acquiring and integrating that business.

In the course of job-related activities: In addition, the Company collects data about employees in the course of their job-related activities, including related to the use of Company equipment and systems (see the section "Monitoring" below) as well as data collected within physical access control system (PACS).

WHAT TYPES OF DATA ABOUT AN EMPLOYEE'S FAMILY MEMBERS DOES THE COMPANY COLLECT?

If you provide the Company with data about members of your family and/or dependents (e.g., for emergency contact or benefits administration purposes), it is your responsibility to tell them, and inform them of their rights, and to obtain their explicit consent (where legally required and if they are legally competent to give such consent) to the processing of, transferring of and access to such Personal Data as set out in this Notice.

WHO HAS ACCESS TO EMPLOYEE PERSONAL DATA?

Data access will be to those who have a need to access the data in order to do their job, and in line with company policies, including the Human Resources Department, relevant business managers, and members of the IT, Finance, Payroll, Legal, Facilities, and Benefits departments. Employee Personal data may be shared by the Employee directly in the course of business. Where Employee Personal

Data is accessed within the Company, as a matter of Notice, access to such data is only given to those who need access for the reasons listed above or when required by law.

Access to the global internal employee directory is provided to all employees.

CAN ANYONE OUTSIDE OF THE COMPANY ACCESS OR USE EMPLOYEE PERSONAL DATA, AND IF SO, WHY?

LSEG Subsidiaries and Affiliated Entities (“LSEG Group”)

The Company may disclose Employee Personal Data to LSEG Group entities, including but not limited to affiliates in the United States, Canada, the European Economic Area, Switzerland, Africa, Latin America, India, Australia and Asia (including but not limited to service support functions in LSEG Sri Lanka), in order to achieve the purposes set out above.

Auditors/Professional Advisors and Other Third Parties

If necessary, and in accordance with applicable laws, the Company may disclose Employee Personal Data to its auditors and other outside professional advisors, insurers, and to other parties that provide products or services to the Company, such as IT systems providers and consulting firms. These firms may be located anywhere in the world. Before allowing such disclosures, the Company vets these third parties and requires them to comply with applicable laws and standards, including data security standards.

The Company and LSEG Group entities may also disclose Employee Personal Data to third party service providers to help them perform various functions for the Company, including the systems and services referenced above, and such as to support:

- cloud services
- benefits and leave administration
- compensation administration
- human resources administration and assistance
- employee relocation services
- administration of the Company's Global Expatriate Notice
- providing human resources data services, learning and development services, payroll services, and recruiting services;
- administering employee surveys
- providing technology-related support, such as software development, system upgrades and IT Help Desk functions
- retirement plan administration
- data security
- data leakage protection

When the processing of Employee Personal Data is delegated to a third-party service provider, and they act as a *processor*, we ask such providers to act on our behalf and under our instructions and to provide sufficient technical, physical and organizational security guarantees to protect such data. Further, when required by applicable laws, the Company will execute relevant data protection agreements with such third parties, and/or will ensure that such third parties otherwise have appropriate and lawful data transfer and processing mechanisms in place.

Some third parties to whom we may disclose personal data, for instance, insurance providers, corporate credit card providers, travel providers, pension scheme trustees, legal advisors, and accountants, are *controllers* in their own right. This means they make their own decisions about how your data is processed, and you should refer to their own privacy notices and policies in respect of how they use your personal data.

Corporate Restructuring/ Sale/ Mergers/ Acquisitions

Employee Personal Data also may be disclosed, when permitted by applicable law, in connection with a corporate restructuring, sale, or assignment of assets, merger, divestiture, or other changes of control of the Company or any of its subsidiary or affiliated companies. The persons or entities who receive Employee Personal Data, who may be advisors, potential transaction partners, or interested third parties, may be located in countries where data protection laws do not provide an equivalent level of protection to the laws in your jurisdiction. In instances where the Company discloses Employee Personal Data to such recipients, it will establish and/or confirm that appropriate protections are in place for such data transfers.

Law Enforcement and Government Requests/Court Orders

The Company may also need to disclose Employee Personal Data to respond to law enforcement or government requests or when required by applicable laws, court orders, and/or government regulations (including disclosures to tax and employment authorities).

RETENTION AND ACCURACY OF EMPLOYEE PERSONAL DATA

The Company strives to keep Employee Personal Data accurate and up-to-date and to retain such data no longer than necessary for the purpose(s) for which it was obtained. In certain cases, legal or regulatory obligations require us to retain specific records for a set period, including following the end of your employment of engagement. In other cases, we may retain records for legitimate purposes in order to resolve queries or disputes which we reasonably think may arise from time to time. If you need to make any changes to your Personal Data, please use the available Human Resources self-service portal or discuss with your HR Contact. In some cases, you may also contact the third-party service provider which holds your Personal Data – for example, a health insurance plan provider. Should you inform your HR Contact, or the Company otherwise becomes aware of any factual inaccuracies in your Personal Data, it will seek to rectify such inaccuracies promptly.

In addition to Employee Personal Data processing informed above, LSEG will retain anonymised, aggregated data in certain circumstances, including diversity data collected for the purpose of equality, diversity and inclusivity initiatives and pursuant to conducting an equal opportunities monitoring programme, but such data will not be linked to, or capable of, identifying any individual.

You can find out more about how LSEG addresses record retention and records management by referring to the Personal Data Retention Procedure and consulting the Records Management resources on the intranet.

PROFILING AND AUTOMATED DECISION MAKING

Applicable data protection laws may include obligations regarding profiling and automated decision-making. LSEG may sometimes use profiling techniques in accordance with applicable law, to assess the performance of staff for performance management, or in restructuring exercises. For example, by analysing attendance, targets met and any other performance indicators. The results of any such profiling will always be reviewed by LSEG before any decisions are made. For more information about profiling techniques used by LSEG, please contact your HR Business Partner. LSEG will only operate processes which result in automated decisions being taken for its staff after communicated to staff and to the extent as permitted in accordance with applicable data protection laws, and standards.

DATA PROTECTION RIGHTS, INCLUDING ACCESS TO PERSONAL DATA

As explained above, and subject to applicable law, employees may—at no cost to employee—be entitled to access their Employee Personal Data and to have inaccurate data corrected or removed, and they may have the right to object to the processing of such data. Thus, subject to applicable laws, as an employee you may learn more about the Employee Personal Data that the Company holds about you.

We will honour your rights under applicable data protection laws. Where permitted by applicable laws, and to the extent as permissible, you have data protection rights to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning you or to object to the processing as well the right to data portability. These rights are not absolute, and they do not always apply in all cases.

In order to exercise your rights you can do so via the available Human Resources self-service portal, visit the following site, which can also be found here: or submit a written request to your HR Contact.

QUESTIONS

Any data protection questions you have about this Notice should be sent to:

CONTACT THE PRIVACY OFFICE

CONTACT THE DATA PROTECTION OFFICER

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/.

MONITORING

The Company maintains various communications systems and networks, including telephones, voicemail, email, mobile devices, fax machines, computers and related software, devices, printers and equipment, computer networks, instant messaging, and networks that allow access to the Internet and the Company Intranet (collectively, the "Systems"). As stated in the LSEG Code of Conduct, communications sent and received through the Company's Systems - including, but not limited to email, Internet and other forms of electronic communications and paper communications - may be the property of the Company.

In accordance with applicable laws and Company policies, including the Cyber Security policies and standards, the Company or a Company-authorized third-party service provider may monitor or review email communications, messaging, use of external storage devices, file transfers and Internet usage on Company Systems. Thus, you should not assume or expect privacy in your communications or Internet activities while at work or while using the Company's Systems, regardless of whether you use the Systems through a Company or personal device, and you agree that the Company may monitor your use of the Company's Systems, including any communications transmitted through the Systems, in accordance with this Notice and applicable laws. Specifically, the Company may monitor activities in order to:

- investigate potential violations of the Company Code of Conduct, Company acceptable use policies and/or other Company policies
- investigate potential crimes or otherwise unlawful conduct
- manage, protect, or maintain the Systems and data held on such Systems

- address potential or actual emergencies or disruptions to the Systems such as a virus infestation or system crash
- protect employee, customer, prospective customer, and other Personal Data (including in connection with the data leakage protection programme)
- meet a legal obligation of the Company

While monitoring the Systems, the Company may collect data about the length of time employees spend on Internet sites or otherwise use the Systems, the specific Internet sites visited, the email addresses of originators and recipients of email communications, and, in certain situations related to the purposes listed above, the content of communications and activities on the Systems. The Company may share this data with third parties, including technical consultants, service providers who perform specified functions for the Company and law enforcement authorities, as necessary and in accordance with applicable law(s).

While certain Systems, such as voicemail, email, and Internet access, may accommodate the use of passwords, they are intended to protect against unauthorized access to the Systems, not to keep employees' activities and communications private from authorized Company personnel and third parties with a legitimate business need.

Apart from the above, the Company may be required to carry out monitoring activities that vary by physical location, country, or region where you work, and the specific LSEG entity where you are employed. Monitoring practices may include, but are not limited to, any of the following:

- Video camera surveillance and monitoring as explained in the Physical Security and Privacy Statement
- Physical Access Control System (PACS) or similar controls for specific locations/ premises as explained in the Physical Security and Data Privacy Statement
- Remote Access monitoring of employee access to Company Systems

In this regard, the Company will comply with all applicable laws, communicate, and take such steps as required, where appropriate.

DATA SECURITY

In compliance with applicable laws and data security standards, the Company maintains appropriate technical and organizational security measures to protect Employee Personal Data against accidental or unlawful destruction, or accidental loss, alteration, unauthorized disclosure or access. These measures include data leakage protection, as referenced above.

You also have an important role to play in protecting the security of your personal data, and you should take care about whom you disclose personal data to, and how you protect your communications and devices. Please refer to the Group Cyber Security Policy and relevant Security Standards for more information about your responsibilities.

CHANGES TO THIS NOTICE

We reserve the right to update or otherwise amend this Notice at any time. Should the Company decide to materially modify the manner in which it collects or uses Employee Personal Data, the type(s) of Employee Personal Data it collects or any other aspect of this Notice, the Company will notify affected employees as soon as possible by reissuing or publishing a revised Notice or taking other steps in accordance with applicable laws, such as obtaining consent where required, prior to making such modifications.

Date of last update: 15-04-2025

Changes made during the last update include references to artificial intelligence tools used as part of processing employee personal data:

- Carrying out candidate evaluations. We may use techniques such as artificial intelligence and machine learning to process and analyse data for recruitment purposes. There will never be any automated decision-making; all decisions will involve a manual review.
- Tools designed to support compliance with company security policies and processes, to prevent, detect and investigate security issues, to provide spam protection, and to prevent malicious communications. Artificial intelligence and machine learning may be used to support with this.