GLOBAL EMPLOYEE PRIVACY POLICY

Thomson Reuters ("Company" or "We") is a global business with networks, databases, servers, systems, support and help desks located around the world.

As part of normal business, individually identifiable information related to employees (collectively, "Employee Personal Data") may be transferred to or accessed by Thomson Reuters and/or third parties around the world, as described in this Global Employee Privacy Policy ("Policy"). Employee Personal Data of Company employees is protected by an Intra-Group Agreement (IGA) between all Thomson Reuters operating entities. The IGA provides specific safeguards when Employee Personal Data is processed or transferred within the Thomson Reuters group of companies.

If you have questions about this Policy, please contact your manager, your Human Resources contact ("HR Contact"), or the **Privacy Office**.

CONTENTS:

PURPOSE AND SCOPE OF POLICY

This Policy outlines Company practices regarding the collection, processing and use of Employee Personal Data in global employee databases and communications transmitted over Company networks and systems.

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:

- Success Factors Learning
- Payroll provider systems
- MyExpenses
- MyTravel
- Taleo
- Workday
- Approved 3rd party cloud services, e.g., Microsoft Office 365
- Company employee participation benefits and provider systems
- Other internal administrative systems and databases necessary to operate the business (e.g., internal directory, financial administration systems)

This Policy applies to Employee Personal Data processed and stored in global HR systems and Employee Personal Data that is collected and sent through Thomson Reuters' network. **It does not apply to any data held solely by local Human Resources departments in various countries where Company employees reside**. In the event of a conflict between this Policy and local Human Resources policies or practices, this Policy will control. **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.

TYPES OF EMPLOYEE DATA THE COMPANY COLLECTS

The Company may collect, use, store, and otherwise process certain Employee Personal Data, including, for example:

- name
- contact information (including home address, home phone number and mobile phone number)
- country of residence
- date of birth
- country of birth
- social security or other governmental identification number
- national insurance number
- gender
- education
- citizenship and passport data
- bank account information
- visa/country residence permits/citizenship
- photographs
- driver's license details and driving records
- credit card information when sent via Company networks
- information related to an employee's family members and dependents

Employee Personal and Family Information

Information Related to an Employee's:

- position/title
- location
- employee identification number
- work address and telephone number
- start and end dates of employment
- supervisor/manager
- reporting structure
- employment status (full-time or part-time)
- salary
- bonus
- equity awards, where applicable
- benefits information, which may include health or medical information
- job performance and related evaluative information
- payroll information
- vacation allotment and absences
- use of the Company's facilities and equipment, including laptops, mobile devices, notably computer and telecommunications systems, to the extent permitted by applicable law
- 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

The Company may use such information for various human resources, employment and/or data security-related purposes, such as:

- workflow management, such as assigning, managing, and administering projects
- project costing and estimates
- compensation, including stock plan administration
- payroll processing
- performance management
- succession planning
- benefits administration, including health and medical benefits, leave entitlements, bonuses, and pensions
- personnel administration
- employee candidate evaluations
- travel reservations and planning
- employee directories
- technical support
- employee surveys
- subject to local law requirements, monitoring and enforcing compliance with Company policies and procedures, legal requirements or in connection with workplace or law enforcement investigations
- protection of the Company's networks, systems, databases, hardware and intellectual property assets, including through its **data leakage protection** program
- protection of employee, customer, prospective customer and other personal data, including through its **data leakage protection** program
- compliance with applicable legal obligations
- to support any claim, defense or declaration in a case or before any jurisdictional and/or administrative authority, arbitration or mediation panel
- to monitor and prevent sexual harassment, bullying, discrimination and/or criminal offenses

Sensitive Personal Data

The Company may also collect, process and use Employee Personal Data that may be considered "sensitive," which may include (depending on applicable law) information about an employee's racial or ethnic origin, nationality or citizenship, marital status, veteran status, health-related data or disabilities requiring work accommodations.

The Company may need to collect this information to comply with applicable law; to administer or facilitate health, medical or other employee benefits; 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.

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.

HOW IS EMPLOYEE PERSONAL DATA COLLECTED?

The Company typically collects Employee Personal Data directly from job candidates and employees through the application and background check process, or from an employment agency or background check provider in connection with an individual's employment. The Company sometimes collects information from others when permitted by law; including references, former employers, and other third parties such as credit reference agencies or background check agencies. In addition, the Company collects information 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).

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

If you provide the Company with information about members of your family and/or dependents (e.g., for emergency contact or benefits administration purposes), it is your responsibility to 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 Policy.

WHO HAS ACCESS TO EMPLOYEE PERSONAL DATA?

Within the Company, the Human Resources Department, relevant business managers, and members of the IT, Finance, Payroll, Legal and Benefits departments may have access to some Employee Personal Data. As a matter of policy, 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.

For information about who outside of Thomson Reuters has access, please see the section below "**CAN ANYONE OUTSIDE OF THE COMPANY ACCESS OR USE EMPLOYEE PERSONAL DATA, AND IF SO, WHY?**"

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

Thomson Reuters Subsidiaries and Affiliated Entities ("Thomson Reuters Group")

The Company may disclose Employee Personal Data to Thomson Reuters Group entities, including but not limited to affiliates in the United States, Canada, the European Economic Area, Switzerland, Latin America, India, Australia and Asia for various purposes, including the following:

- benefits and personnel administration, including health and medical benefits, leave entitlements, bonuses and pensions
- compensation-related activities and compensation analysis
- workflow management, such as assigning, managing and administering projects
- performance management and technology support
- physical and information security
- data leakage protection
- facilities management

Auditors/Professional Advisors and Other Third Parties

If necessary, and in accordance with applicable law, the Company may disclose Employee Personal Data to its auditors and other outside professional advisors, and to other parties that provide products or services to the Company, such as IT systems providers and consulting firms. 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 Thomson Reuters Group entities may also disclose Employee Personal Data to third party service providers to help them perform various functions for the Company, such as:

- benefits and leave administration
- compensation administration
- human resources administration and assistance
- employee relocation services
- administration of the Company's Global Expatriate Policy
- providing human resources information 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
- information security
- data leakage protection (for more information about Thomson Reuters data leakage protection program, please click **here**).

When the processing of Employee Personal Data is delegated to a third party service provider, 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.

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 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. 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.

You can find out more about how Thomson Reuters addresses record retention **here** and records management team can be contacted **here**.

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. If you wish to access such data, you may view your information via the available Human Resources self-service portal submit a written request to your HR Contact.

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 **Code of Business Conduct and Ethics**, 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 **Information Security Handbook**, 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 Policy and applicable law. Specifically, the Company may monitor activities in order to:

- to investigate potential violations of the Company Code of Conduct, Company acceptable use policies and/or other Company policies
- to investigate potential crimes or otherwise unlawful conduct
- to manage, protect or maintain the Systems and data held on such Systems
- to address potential or actual emergencies or disruptions to the Systems such as a virus infestation or system crash
- to protect employee, customer, prospective customer and other personal data (including in connection with the data leakage protection program)
- to 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 information 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). For more information about Thomson Reuters' data leakage protection program, please click **here**.

Finally, 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.

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.

CHANGES TO THIS POLICY

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 Policy, the Company will notify affected employees as soon as possible by reissuing a revised Policy or taking other steps in accordance with applicable laws, such as obtaining consent where required, prior to making such modifications.