Global Employee Privacy Notice

Date of Last Update/Review: April 2024

Introduction

This Global Employee Privacy Notice (“**the Notice”**) provides information about why Verisk Analytics Inc., its subsidiaries or affiliates (”**Verisk**”, “**the Company”, “We” or “Our”)** may process the Personal Information of job candidates, current or former employees, contractors or agency staff (collectively ”**employees**”, **“you”, “your”**).

This Notice replaces previous Employee Privacy Notices and any references to these in your employment contract or other documentation should be read to refer to this Notice. Verisk operates in many countries globally. Some of these countries have specific legal requirements governing the use of employee Personal Information. Verisk will comply with all such laws and regulations, by implementing additional procedures, standards, and policies to meet these requirements. Accordingly, the employee Personal Information collected in a particular jurisdiction may be unique to comply with local laws and this Notice also may be supplemented by jurisdiction-specific addenda or consent authorization documents, where applicable.

Definitions

- **Personal Information:** Any information relating to an identified or identifiable individual. In this Notice, references to Personal Information may be read to include its subset Sensitive Personal Information, where appropriate.
- **Sensitive Personal Information**: Any information revealing race, ethnicity, political views, religion, health, sexual orientation, trade union membership, genetic or biometric data, information about criminal convictions and offenses, and as otherwise defined by applicable laws.

Data Controller

The Verisk entity which employs you (“**Your Employer**”) is the data controller of any Personal or Sensitive Personal Information that the Company holds about you except for the instances where your Personal Information needs to be processed in respect of corporate functions for which Verisk Analytics, Inc., acts as the controller and coordinates these activities for itself and its subsidiaries.

Personal Information Collection

Your personal data is collected directly from you through your interactions with Verisk such as when you complete a job application form or enter information about yourself into our systems. Examples of personal data you may provide includes your name, address, telephone numbers, email addresses and your date of birth. Additionally, we may develop your personal data indirectly through your interactions with Verisk company equipment, systems and networks. Your personal data may also be collected indirectly from other sources, such as your manager, or in some cases, (with your prior written consent, where required by law) external sources, such as recruitment agencies, specialist search organizations. background checks, referees, vendors or publicly accessible sources, such as tax agencies and other public authorities. Your personal data is processed for various purposes including Human Resources (“HR”) requirements, business activities, safety and security.

Data Security

Verisk maintains appropriate technical and organizational measures designed to protect your personal data against loss or accidental, unlawful or unauthorized alteration, access, disclosure or use.

Personal Information Processing Purposes

We may process your personal data when we have an appropriate basis to do so or are permitted to do so in accordance with applicable laws (“lawful basis”). Verisk needs to process employee Personal Information in the context of the employment relationship for various business purposes, services and/or activities including but not limited to Human Resources (“**HR**”) requirements, business activities, safety and security matters as listed below in further detail.

The table below details employee Personal Information categories Verisk may need to process about you in connection with its business and related employment, administration, payroll or benefits processing as well as the applicable legal basis permitting us to collect and process this data. Examples of an acceptable legal basis include:

i) **processing necessary to fulfill contractual requirements** such as your employment contract;
ii) **processing based on a legitimate interest of the business** such as data security or employment administration, payroll or benefits processing; or
iii) **processing based on your consent.**

What Information We Process	Purposes for Using Your information	Legal Basis Examples
1. Personal Information: • Name • Contact information including home address, email address, telephone number, mobile numbers, instant messenger • Emergency contact details • Photographs or videos of you as well as voice recordings • Gender, including pronouns • Racial /ethnic origin • Date and place of birth • Marital status • Dependents, family/household composition	• Organizational charts and directories • HR recruiting, records and business processes • Compensation and payroll management • Benefits management • Occupational health and wellness Programs • Corporate travel logistics and security • Staffing and organizational planning Training • Site and electronic network access • Communications with you about your employment, including sending you work schedule information, compensation and other Company information • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management • Facilitating charitable contributions to corporate campaigns or local volunteer efforts • To manage and administer the employment relationship and to fulfil obligations set out in the employment agreement and related agreements (such as payroll and other benefits or expenses) • To conduct internal and external corporate or employee communications activities • To comply with our obligations according to applicable laws (such as employment, tax, and accounting laws) • To conduct diversity monitoring	• To fulfil the obligations set out in your employment contract and related agreements • Verisk's legitimate interests including prudent business management, operations and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent • For racial / ethnic origin, when explicitly permissible or required by law or collective agreements
2. Identification & Work Eligibility: • National ID (passport, visa, social security, driver's license, other government-issued identifications) • Citizenship • Residency • Nationality • Country of birth • Military and/or veteran status	• Verifying your identity and maintaining the integrity of our HR records • Complying with immigration and other work permit requirements • Security and risk management including collating driver's license data for employees who operate Company automobiles, professional license verification, fraud prevention and similar purposes • Appointing representatives in legal, government or regulatory proceedings • Selecting employees as representatives and/or authorized signatories for representing the Company (including managing banking and financial accounts) • Obtaining tax and other government incentives benefiting our employees and/or operations • Complying with the requirements of corporate governance and stewardship, security and contingency planning and required external reporting • Supporting investigations and incident management	• To fulfil the obligations set out in your employment contract and related agreements • As applicable, Verisk's Analytics Inc's legitimate interest as parent company or subsidiary's legitimate interests including prudent business management and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent
3. Health related information: • Information related to the physical or emotional health of an employee including any disabilities or limitations to perform work duties or functions • Drug testing and other types of health examinations • Information regarding rehabilitation, sick leave and in connection with safety related certification for certain work tasks	• Determining your fitness to work in a particular role, and reasonably accommodating any disabilities • Supporting your ability to participate in our leave of absence and/or disability insurance programs • Complying with occupational health and workplace safety and government reporting requirements • Managing employee safety and business risks associated with the COVID-19 pandemic or similar health emergencies • Facilitating your participation in health benefit programs, including our health plans and related programs • Managing health and safety related issues according to employment law (such as safety related certification for certain work tasks, administrating vaccinations and health checks, monitoring absences due to health-related reasons • Applying and following-up on internal policies • Complying with the requirements of corporate governance and stewardship, security and contingency planning and required external reporting • Supporting investigations and incident management	• To fulfil the obligations set out in your employment contract and related agreements • As applicable, Verisk's Analytics Inc's legitimate interest as parent company or subsidiary's legitimate interests including prudent business management and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent

What Information We Process	Purposes for Using Your information	Legal Basis Examples
4. Employment-related Information: • Job title/position and responsibilities • Skill or competency related information • Employment history, performance evaluations, employment contracts, appraisals, work absence and attendance records, travel & expense data, training records • Educational background, business reference information • Recruitment, promotions and disciplinary sanctions • Termination or resignation reasons and relevant dates	• Recruiting and monitoring the usage of resources, improving services, allocating and managing company assets and human resources, strategic planning, project management, and ensuring business continuity • Managing and administering the employment relationship and to fulfil obligations set out in the employment agreement and related agreements (such as payroll and other benefits) • Evaluating and following up on work tasks and performance (such as feedback and evaluation processes) • Managing work activities and personnel generally including employee training and development, succession planning	• To fulfil the obligations set out in your employment contract and related agreements • As applicable, Verisk's Analytics Inc's legitimate interest as parent company or subsidiary's legitimate interests including prudent business management and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent
5. Compensation, benefits and payroll information: • Bank account information • Current and historical compensation information • Bonus and financial benefit information • Insurance beneficiary information	• Managing and administering the employment relationship and to fulfil obligations set out in the employment agreement and related agreements (such as payroll and other benefits) • Complying with our obligations according to applicable laws (such as employment, tax, and accounting laws) • Planning, managing and administering our business and payroll	• To fulfil the obligations set out in your employment contract and related agreements • As applicable, for our legitimate interests as parent company or subsidiary including prudent business management and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent
6. Parent Company corporate activities: • Personal information • Information relating to your employment • Compensation benefits & payroll	• HR planning including recruitment, monitoring the usage of resources, improving HR services • Allocating and managing company assets and human resources, strategic planning, project management and ensuring business continuity • Compiling audit trails and other reporting tools, maintain records relating to business activities, budgeting, financial management and reporting, communications, managing corporate mergers, acquisitions, sales, reorganizations or disposals and integration with purchasers • Corporate reporting and audits • Maintaining and preserving business reporting tools and records relating to business activities, budgeting, financial management and communications • Managing mergers, acquisitions, sales, reorganizations, integration projects or disposals • Managing and administering operations and security • Managing and administering Verisk's incentive program	• To fulfil the obligations set out in your employment contract and related agreements • Verisk Analytics Inc's legitimate interest as parent company to protect the health and safety of employees and others, maintain prudent business management and business continuity, safeguarding and maintaining IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent
7. Technology; Communications: • Information about your use of Verisk technology resources (or devices enrolled in the Bring Your Own Device ("BYOD") Program, as further detailed in our Mobile Device Policy • Employee ID, electronic identifiers such username, online credentials, IP addresses and MAC addresses, internet usage, access logs, communication logs • Information collected through automated means and electronic content produced by you using company systems, including documents, instant messages, emails and telephone traffic and conversations)	• To investigate and gather evidence in respect of suspected criminal or disloyal activities, such as breaches of the employment contract, internal rules or policies; • To ensure the security and safety of our physical facilities and IT infrastructure.	• To fulfil the obligations set out in your employment contract and related agreements • As applicable, for our legitimate interests as parent company or subsidiary including prudent business management and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent

What Information We Process	Purposes for Using Your information	Legal Basis Examples
8. Facilities and Security Data: • Where permitted by local law, identifiable images in CCTV footage, badge swipe information, system and building login access records including geolocation, time and duration, keystroke, download and print records, call recordings, information collected by IT security programs and filters • Fingerprint data, if required for facilities access system	• To investigate and gather evidence in respect of suspected criminal or disloyal activities such as breaches of the employment contract, internal rules or policies • To ensure the security and safety of individuals, our physical facilities and IT infrastructure • To monitor facilities occupancy and employee in-person attendance at company facilities in accordance with company requirements	• To fulfil the obligations set out in your employment contract and related agreements including overseeing employee attendance to ensure its aligned with the agreed obligations in the employment agreement and related agreements • As applicable, for our legitimate interests as parent company or subsidiary including prudent business management and continuity, safeguarding and maintaining its IT infrastructure, office equipment, facilities and other property • Where applicable, processing is based on your consent

Data Sharing

We may share your Personal Information with other entities within Verisk, and Service providers that provide/process: benefits; payroll; emergency communications; work-related travel arrangements; expense reimbursement; background checks; interoffice communication; training; incident intake; business cards; security; offsite information storage; customer and contract cycle management; ticketing management; and other organizations that Verisk may engage to provide general support for general human resource, business management, security functions and any other services reasonably required by the Verisk. In accordance with applicable law, we have entered into legally binding agreements requiring service providers and organizations to use or disclose personal information only as necessary to perform services on our behalf or comply with applicable legal requirements.

In addition, we may disclose personal information about you to:

(a) public authorities if we are required or permitted to do so by law or legal process, for example due to a court order or a request from a law enforcement agency,
(b) to relevant third parties when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss,
(c) to public authorities in connection with an investigation of suspected or actual fraudulent or other illegal activity, and (d) to prospective buyers in the event we sell or transfer all or a portion of our business or assets (including in the event of a reorganization, dissolution, or liquidation).

You may request a complete list of all recipients of your personal information by contacting us via the contact details below.

Cross-Border Transfers

Your personal information may be disclosed to Verisk's affiliates or third parties either within or outside of the country from which it was collected. Some of your personal information may be transferred to a country (including the U.S.) that may not afford statutory protections for personal information equivalent to those within the country in which it was collected. In all such cases Verisk will take steps designed to comply with applicable data protection law such as only permitting your personal information to be transferred when:

- The country to which the personal information will be transferred has been granted a European Commission adequacy decision;
- We have put in place appropriate safeguards in respect of the transfer, for example the EU Standard Contractual Clauses.

You may request more information and a copy of the safeguards that Verisk has put in place in respect of transfers of personal information by contacting us as described in the How to Contact Us section below.

Data Retention

Your personal Information is retained for the duration of your relationship with Verisk, plus a reasonable period thereafter as necessary, to fulfil the purposes described above. When processing elements of your personal information is no longer necessary in relation to the purposes for which it was collected, Verisk will erase that personal information if there are no special legal requirements that require it to be retained. Retention periods are generally summarized below, and may be extended if we are required to preserve your personal information in connection with a separate legal obligation, such as in connection with any claims, litigation, investigations or proceedings.

Employee Personal Information Types	Retention Period *(may vary depending on your location)*
1.Personal Information	**Up to 8 years** from the time you leave Verisk
2.Identification & Work Eligibility:	**Up to 3 years** from the time you leave Verisk (U.S., related to I-9 processing); otherwise follows Personal Information retention.
3.Health Related Information	**Up to 6 years** from the time you leave Verisk
4.Employment related Personal Information :	**Up to 8 years** from the time you leave Verisk
5.Compensation and Benefits related Personal Information	**Up to 10 years from the date you leave Verisk** (in accordance with the limits set by applicable accounting laws and regulations) In certain jurisdictions this data may be held up until your retirement to ensure your pensions are correctly registered; in the U.S. particularly this may be kept for a longer duration to facilitate pension disbursements and related auditing required thereafter.
7.Parent company corporate activity related Personal Information:	**Up to 10 years** (per the specific personal information type involved)
8.Technology; Communications	**Up to 2 years** (in certain jurisdictions this may be further limited, such as for Germany this is limited to 6 months from the date you leave Verisk)
9.Facilities & Security related Personal Information	**Up to 7 years** (more limited retention obligations apply for specific data types such as CCTV recordings as specified under applicable local laws and regulations)

Your Rights and Choices

You have the right to:

- request information about the processing and a copy of your personal data.
- get incorrect or outdated personal information corrected, updated, or completed.
- In the European Union or United Kingdom, object to the processing if it is based on our legitimate interest, unless we can demonstrate compelling legitimate grounds for the processing of your personal information which override your interests and rights. You always have the right to object to the processing of your personal information for direct marketing.
- In the European Union or United Kingdom, obtain a restriction of processing of your personal information provided we do not have a legal right to continue the processing.
- get your personal information deleted if it is no longer necessary to be retained for the purposes for which it was collected, if you have withdrawn the consent on which the processing was based, if you object to the processing and there are no overriding legitimate grounds for the processing, if the personal information has been processed unlawfully, or if the personal information must be deleted in order to fulfil a legal obligation.
- obtain the personal information that you provided to us in a structured, commonly used and machine-readable format and transfer it to another controller if the processing is based on your consent or an agreement between us ("**data portability**").
- withdraw your consent at any time by contacting us (contact details below).

Exercising Your Rights; Complaints

If you wish to exercise any of your data protection rights or you consider that we have processed your personal information in violation of applicable law, please contact us as detailed in the "How to Contact Us" section below. If you consider that we have processed your personal data in violation of applicable law, you may also lodge a complaint with your local data protection supervisory authority.

How to Contact Us

If you have any questions or comments about this Notice or any issue relating to how we collect, use, or disclose personal data, you may contact us at privacy@verisk.com. If you would like us to update the Personal Information we have about you or your preferences, you may contact your local HR representative or our Chief Privacy Officer at privacy@verisk.com and please include your name and the name of your specific Verisk or third-party entity employer to which your request refers. You may also reach out to company's external Data Protection Officers for the entities below at the following contact details:

Actineo Group Proliance GmbH Leopoldstr. 21, 80802 Munich, Germany datenschutzbeauftragter@datenschutzexperte.de +49 2236 48003100	**AIR Germany** Joachim Maass Data Pro Security GmbH Kaiser-Wilhelm-Str. 2 82319 Starnberg, Germany jmaass@data-pro-security.com +49 8151 4468968	**S.V. Krug** Fred Birkelbach Axians IT Business Solution GmbH Werner von Siemens Str 15, 66793 Saarwellingen, Germany. fred.birkelbach@axians.de +49 6838 89930

JURISDICTION SPECIFIC GLOBAL EMPLOYEE PRIVACY NOTICE ADDENDA

California Addendum

This California Addendum to the Global Employee Privacy Notice ("**CA Addendum**") is provided on behalf of Verisk on behalf of itself, its subsidiaries, and affiliates (hereinafter, "**we**" "**our**" or "**us**") and applies solely to our California Employees, Applicants, and Independent Contractors (hereinafter, "**you**" or "**your**").

Personal Information Categories Collected

Category	Examples	Collected [Y/N]
Identifiers	Real name, alias, postal address, unique personal identifier, online identifier, device identifier, Internet Protocol address, e-mail address, account name, or other similar identifiers	**Y**
Personal information categories listed in CA Civil Code § 1798.80(e)	Name, signature, physical characteristics or description, address, telephone number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information	**Y**
Protected classification characteristics	Age (40 years of age or older), marital status, gender, veteran, or military status	**Y**
Commercial information	Records of personal property and products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies	**N**
Internet or other similar electronic network activity	IP address, device ID or other information you may disclose or provide to us online	**Y**
Geolocation data	Physical location, geocode, longitude/latitude	**Y**
Audio, electronic, visual, thermal, olfactory, or similar information	interview videos and/or audio recordings; images or videos captured as part of facilities security footage, company calls, meetings, presentations or other events where recording is permitted	**Y**
Professional or employment-related information	Current or past job history; skill or competency information, performance evaluations; professional references	**Y**
Education Information as defined in 20 U.S.C. §1232g, 34 C.F.R. Part 99	Transcripts and related educational data upon your consent/authorization	**Y**
Inferences drawn from any of the information identified above to create a consumer profile	Inference: A derivation of information, data, assumptions, or conclusions from facts, evidence. Profile: data reflecting a consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	**N**

Sensitive Personal Information	• Social security number, driver's license number, state identification card, passport number, visa information, precise geolocation
	• Racial or ethnic origin, citizenship or immigration status, credit history information
	• Medical history, including disability information, mental or physical health conditions, diagnosis or treatment
	• Images, audio and/or video recordings
	• Information concerning sex life or sexual orientation (to the extent you voluntarily provide such information to us)
	  • Biometric information (physiological, behavioral, and biological characteristics or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints and voiceprints, imagery of the iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data)
	  • Genetic data
	  • Contents of mail, email, and/or text messages where Verisk is not the intended recipient of such communication
		Y

Sensitive Personal Information

We use your sensitive personal information in order to:

- Perform services related to the recruitment, hiring, and employment process, such as performing background checks, administering benefits and payroll, and related purposes
- Perform other services on our behalf, including managing headcount, activities related to performance and compensation, managing travel and business-related expenses, and for diversity and inclusion initiatives
- Prevent, detect, and investigate security incidents
- Prevent or resist malicious, deceptive, fraudulent, or illegal actions
- Ensure your physical safety

Sources of Personal Information

We obtain personal information from the following sources: directly from the employee, candidate, or independent contractor, affiliates/subsidiaries, public sources, third parties that may include background check companies, prior employer, third party vendors (educational), and state and federal government agencies.

Purposes for Collecting Personal Information

We may use personal information that we collect for one or more of the following purposes:

- To perform services related to the recruitment, hiring, and employment process, such as performing background checks, administering benefits and payroll, and related purposes
- Perform other services on our behalf, including managing headcount, activities related to performance and compensation, managing travel and business-related expenses, and for diversity and inclusion initiatives
- To operate, evaluate, and improve our business
- To develop, maintain the quality or safety of, improve, upgrade, or enhance our products and services
- To perform internal market research, or to advertise our products and services and determine the effectiveness of such advertising
- To administer our websites or identify and repair errors that impair existing intended website functionality
- As required or necessary in response to law enforcement requests or to comply with applicable law, court orders, or governmental regulations
- To perform auditing related to a current interaction with you and concurrent transactions, including, but not limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards
- To detect data security incidents and help ensure your physical safety
- To resist and protect against malicious, deceptive, fraudulent, or illegal activity
- To perform services on behalf of, or for, clients or service providers, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of clients or service providers
- To undertake internal research for technological research, development, analysis, or demonstration

Categories of Third Parties to whom we disclose Personal Information

- Affiliates and subsidiaries
- service providers, sub-processors, and other entities that perform services for us, our affiliates, and/or our subsidiaries, including but not limited to: benefits, payroll, workers compensation, unemployment, and related services, background checks, state and federal court entities, state and federal compliance reporting agencies, and other government entities
- Our customers, including insurance companies, who may contact you regarding products or services that may be of interest to you

Purposes for Disclosing Personal Information to Third Parties

We may disclose personal information to third parties for the following purposes:

- To fulfill the reason the information was provided: for example, to provide the requested product or service
- To develop, operate, evaluate, and improve our business or products and services
- To detect data security incidents or help ensure your physical safety
- To resist and protect against malicious, deceptive, fraudulent, or illegal activity

Personal Information Selling or Sharing

"**Selling**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to a third party for monetary or other valuable consideration.
"**Sharing**" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to a third party for cross-context behavioral advertising.

We do not Sell or Share your personal information.

Personal Information Retention

We will retain your Personal Information for the period necessary to meet the purposes for which it was collected as documented in our corporate retention schedule, unless a longer period is required or permitted by law or legal process, such as a pending claim, investigation or litigation requiring preservation of relevant records.

Your Personal Information Rights

- The right to know what Personal Information has been collected about you, including the categories of personal information, the categories of sources from which it is collected, the purpose(s) for collecting, selling, or sharing it (as applicable), and the categories of third parties to whom it has been disclosed
- The right to delete personal information collected about you, subject to certain exceptions
- The right to correct inaccurate information we maintain about you

Exercising Your Rights

To exercise your rights under applicable consumer data privacy laws, or to appeal a refusal to take action on a previously submitted request to us, you or your authorized agent may contact us at:

- https://secure.ethicspoint.com/domain/media/en/gui/69464/index.html
- Privacy@verisk.com
- 1(844) 845-6988

In order for us to process your request, we may ask that you provide information to verify or validate your identity and address in accordance with applicable law, such as a billing statement or utility bill. Any information collected will only be used for verification purposes. Information such as account numbers, balances, etc. should be removed from any such documents prior to submitting to us.

Non-discrimination / No retaliation

You will not receive discriminatory treatment or be retaliated against for exercising any of your rights as described above or otherwise in accordance with applicable law.

Contact Us

If you have questions or concerns about this notice, you may contact: Privacy@verisk.com

Canada Addendum

The following additional provisions apply to employees, candidates and external staff working in Canada.

Manner of Collection

We collect personal information that you provide directly to us (such as through the job application process or in connection with the management of your employment or working relationship) as well as information devices provide to us automatically, as described above. We may also collect personal information indirectly with consent. For example, we collect background verification information from third-party background screening providers and we may also obtain personal information from recruitment agencies or job references.

Personal Data Transfers

We and our service providers (including affiliates) may access, store and otherwise process personal information outside of your province (including, for Quebec residents, outside of Quebec), including in other parts of Canada, the United States, and other foreign jurisdictions where we or our service providers are located. We, our affiliates and our service providers may disclose your personal information if we are required or permitted by applicable law or legal process, which may include lawful access by foreign courts, law enforcement or other government authorities in the jurisdictions in which we or our service providers operate.

Retention

We will retain your Personal Information for the period necessary to meet the purposes for which it was collected, unless a longer period is required or permitted by law or legal process, such as a pending claim, investigation or litigation requiring preservation of relevant records.

Your Rights

Subject to limited exceptions under applicable law, you have the right to access, update, rectify and correct inaccuracies in your personal information in our custody and control and withdraw your consent to our collection, use and disclosure of your personal information (although an employee cannot withdraw consent to the collection of personal information necessary to administer their employment). You may request access, updates, rectification, and corrections of inaccuracies in your personal information in our custody or control or withdraw your consent by emailing Privacy@Verisk.com. We may require certain personal information to verify your identity or that of the individual making the request.

How to Contact Us

If you have any questions or comments about this privacy notice or the manner in which we or our service providers (including our service providers outside Canada) treat your personal data, or to request access to or correction of your personal data, or to withdraw your consent, please contact our Chief Privacy Officer, Samantha Vaughan by emailing Privacy@Verisk.com or by writing to her at Verisk Analytics, 545 Washington Blvd, Jersey City, NJ 07310.

Verisk China Employee Privacy Notice (“Privacy Notice”)

This Privacy Notice applies to employees of Verisk Analytics Inc. ("**Verisk**") entities located in the People's Republic of China ("**China**") and sets forth how Verisk will process and protect personally identifiable information ("**Personal Information**") in connection with the human resources function. Verisk is the data controller of the Employee's personal information.

Legal basis

Verisk processes your personal information in full compliance with one or more of the legal bases under Article 13 of the Personal Information Protection Law of the People's Republic of China (the "**PIPL**").

Personal Information and Purpose of Processing

We may collect and process the following personal information for the following purposes. The PIPL classifies data in bold as sensitive personal information, which means that if such data is leaked or illegally used, it is likely to damage an individual's personal dignity or endanger personal safety or property.

Categories of Personal Information	**Scope of Personal Information**	**Purposes of Processing**
Personally Identifiable Information	Name, contact details, title, date of birth, **government-issued ID number, passport or other citizenship information, bank account details**, tax identification number, gender, race, ethnicity, disability, veteran status, **sexual orientation**. Insurance beneficiary information, emergency contact details, hobbies/ interests, travel and expense data, references	• Decisions related to your employment relationship with us • Manage HR functions, including payroll and benefits • To comply with a legal obligation
Healthcare data	Medical and health data	• Comply with health and safety obligations • To comply with a legal obligation • Manage benefits
Biometrics	Fingerprint, other biometric features	• Perform safety and security functions and obligations, including workplace access or facilities attendance • Time logging
Internet or other electronic network activity and use	Use of the Internet, e-mail for communication	• Decisions related to your employment relationship with us • Business Purposes • To comply with a legal obligation • Perform safety and security functions and obligations
Geolocation data	Employee-related geolocation data	• Decisions related to your employment relationship with us • Perform safety and security functions and obligations
Audio, electronic, and visual information	Photographs, audio or video recordings, records of the use of company systems and equipment	• Decisions related to your employment relationship with us • Implement security measures to comply with health and safety obligations
Occupation or employment-related information	Labor rights documents, professional and work history, compensation and benefits records, performance evaluations, disciplinary actions, grievances, training records, professional memberships and licenses, educational history.	• Decisions related to your employment relationship with us

Data Sharing

Verisk may share your personal information with:

- Other Verisk entities.
- Service providers who perform services (including payroll and benefits) on our behalf, emergency communications, work-related travel arrangements, expense reimbursement, background checks, internal office communications, training, incident escalation, security, off-site data storage, and other human resources, business management, security functions and support. We have entered into legally binding

agreements in accordance with applicable law that require these service providers to use or disclose personal information only as necessary to perform services on our behalf or to comply with applicable legal requirements.

- Share data with Verisk's customers in response to their requests for audits or security assessments, or other requests from customers as part of their engagements.

- In addition, data sharing may include (1) where the sharing is required or permitted by law or legal process, (2) we believe disclosure is necessary or possible to prevent physical harm or financial loss, (3) in connection with an investigation of suspected, actual fraud or other illegal activity, or (4) our sale or transfer of all or a portion of our business or assets (including in the event of a reorganization, dissolution, or liquidation).

Transfer of personal information overseas

As noted above, Verisk may share your personal information with affiliates, service providers, or third parties outside of China, including in countries that may not have the same level of legal protection for personal information as in China. However, we have put in place security measures and processes to provide the same level of protection for your personal information as in China. In addition, we will only transfer personal information on the basis of an appropriate legal basis and if the appropriate transfer agreement is in place.

You acknowledge and consent to the transfer of your personal information to the following entities for the following purposes:

Supplier Code	Vendor Type
SHANGHAI DELOITTE TAX LTD.BEIJING BRANCH	Tax firm
CIIC FINANCIAL CONSULTING LIMITED	Payroll
CHINA INTERNATIONAL INTELLECTECH CORP	Payroll
PWC CONSULTANTS SHENZHEN LTD BEIJING BRA	Tax firm
CITS American Express Global Business Travel	Travel agent
GUOFUHAOHUA TAX AGENCY	Audit firm
MING GUANG ACCOUNTING FIRM	Audit firm
BEIJING MINGPU CPA GENERAL PARTNERSHIP	Audit firm
MORGAN LEWIS AND BOCKIUS LLP	Legal firm
FESCO BEIJING LIMITED	Payroll & HR Services
TRICOR CONSULTANCY BEIJING LTD	Finance service
TRICOR CONSULTANCY BEIJING LTD SHANGHAI BRANCH	Finance service
CITIC International Bidding Co. Ltd	Bidding agent
TEC	Landlord

The content of personal information transferred and the purpose of the transfer: see the section "Personal Information and Purpose of Processing" above.

Data Protection

Verisk takes appropriate technical and organizational measures to strive to protect your personal information from loss or accidental, unlawful or unauthorized alteration, access, disclosure or use.

Data Retention

Verisk will retain your personal information for the duration of your relationship with Verisk and, as appropriate, for a reasonable period thereafter in order to fulfill the purposes set forth above. The retention period may be longer if we need to retain your personal information in connection with litigation or investigation, or if a longer retention period is required or permitted by applicable law.

Your Rights and Choices

In accordance with applicable laws (including the PIPL), you have certain rights in relation to your personal information:

- The right to access and copy personal information about you.
- The right to request that we correct inaccurate or incomplete personal information.
- The right to request that we delete your personal information, provided that the deletion does not affect our management of human resources matters related to your employment relationship. This right does not affect

the lawfulness of our processing of personal information prior to the receipt of a deletion request, nor does it affect the lawfulness of processing based on applicable legal grounds.

- The right to request further explanations from us on our rules for the processing of personal information, provided that these rules are not clear or not mentioned in this Privacy Notice.
- We have the right to request us to transfer your personal information held by us to other personal information processors subject to the conditions stipulated in the PIPL.
- The right to withdraw your consent to certain types of processing activities. However, such withdrawal will not affect the lawfulness of the processing of personal information prior to the withdrawal of consent, nor will it affect the lawfulness of processing based on applicable legal grounds.
- Other rights permitted by applicable law.

If you wish to exercise any of the above rights, or if you believe that we have processed your personal information in a way that violates applicable law, please contact us using the contact details in the "How to Contact Us" section below. If you believe that we have failed to rectify an unlawful act, you may also lodge a complaint with the appropriate data protection supervisory authority.

How to contact us

If you are interested in learning more about how we process personal information, have any questions regarding this Employee Privacy Notice, or if you have a complaint or request in this regard, please contact Bhanu Gudipati in your local Human Resources Department at Bgudipati@verisk.com.

Costa Rica Addendum

If you are a resident of Costa Rica, the following specific provision applies to the processing of your personal information in addition to the Global Employee Privacy Notice:

You will be duly informed whether the personal information requested during the application process must be provided on a mandatory or optional basis. In case of refusal to provide the mandatory information, Verisk will not be able to process your Personal Information for the purposes described in Global Employee Privacy Notice.

India Employee Privacy Notice for Verisk Affiliates (“Privacy Notice”)

The Verisk Analytics Inc. (“**Verisk**”) entity by which you are employed is responsible for the processing of your personal information or personal data (collectively, “**personal data**") in connection with various human resources functions. This Privacy Notice covers personal data of employees of Verisk’s India business units only. Verisk is the data controller in respect of employee personal data.

What Information We Process

Verisk collects and uses personal data such as:

• Personal details and characteristics including your name, home address, personal and business email addresses, home telephone number, date of birth/age, racial/or ethnic origins, gender, marital status and dependents, hobbies/interests, emergency contact details, insurance beneficiary information, photographs, audio or video recordings, citizen and immigration information, government-issued identification number, Tax ID number.

• Compensation, benefits and payroll information including bank account information, current and historical compensation information, bonus and financial benefit information.

• Information relating to your position including job title/position, job responsibilities, employment history, performance evaluations, employment contracts, work absence and attendance records, security badge swipe data, travel & expense data, and date and reason for resignation or termination.

• Talent management information including training records, educational background, business reference information, disciplinary sanctions.

• Information about your use of Verisk technology resources (or devices enrolled in the Bring Your Own Device (BYOD) Program) such as use of media and communications means, use of mobile devices.

• Geolocation data

We do not collect your sensitive or special category personal data unless we are required or permitted to do so by applicable law, or you have otherwise provided your explicit consent to the collection and processing of your sensitive or special category personal data. Sensitive or special category personal data may include, but is not limited to, information relating to sexual orientation, criminal convictions and offences, political contributions and affiliation, and fingerprints.

How We Use Your Information and Legal Basis(es)

Verisk uses your personal data, subject to applicable law, for the following purposes:

• **Managing our workforce:** managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, payroll administration, expense reimbursement, benefits administration, work planning and allocation, employee training and development, monitoring information related to raises, salaries, performance reviews/ratings, and promotions, developing and undertaking diversity and inclusion initiatives, absence and sickness monitoring, background checking, making travel arrangements, creating employee directories, managing disciplinary matters, grievances and terminations, reviewing employment decisions, providing access to facilities, facilities security and managing facilities occupancy rates and verifying attendance at physical facilities. We process personal data for these purposes on the basis that it is necessary for our legitimate interests in managing and administering out business, ensuring our business is adequately resourced, and implementing and enforcing compliance with our internal policies. We process your personal data for payroll purposes, expense reimbursement and benefits administration because these activities are necessary for Verisk to perform under its contract of employment with you.

• **Communications, facilities and emergencies:** facilitating communication with you, ensuring business continuity, providing references, protecting and promoting the health and safety of employees and others in the workplace, safeguarding and maintaining IT infrastructure, office equipment, facilities and other property, and facilitating communication with you and your nominated contacts in an emergency. We process personal

data for these purposes on the basis that it is necessary for our legitimate interests in managing and administering our business, and administering, maintaining and ensuring the security of our IT systems and premises.

• **Business operations**: operating and managing IT, communications systems and facilities, and monitoring the usage of these resources, improving our services, allocating and managing company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, reorganizations or disposals and integration with purchasers. We process personal data for these purposes on the basis that it is necessary for our legitimate interests in managing and administering our business or because we are required to do so by law.

• **Legal and compliance**: Compliance with legal and other requirements, such as tax, recordkeeping and reporting obligations, physical access policies, conducting audits, management and resolution of health and safety matters, compliance 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 any internal complaints or claims, conducting investigations and complying with internal policies and procedures. We process personal data for these purposes on the basis that we are required to do so by law or it is necessary for the establishment, exercise or defense of legal claims.

• **Sensitive information:** We may also collect certain types of sensitive or special categories of personal data for specific purposes, including: the collection of health/medical information in order to accommodate a disability or illness, to establish employee fitness to work, and to provide benefits; health and safety and accident information, in order to comply with health and safety law obligations and in order to make insurance claims; diversity-related personal data (such as gender, race or ethnicity), and information relating to criminal background checks. We do not collect your sensitive or special category personal data unless we are required or permitted to do so by applicable law, or you have otherwise provided your explicit consent.

Where consent is the legal basis for processing your personal data, you can withdraw your consent to at any time by contacting us. See more information in the How to Contact Us section below. Please note that if you withdraw your consent, for the processing of special categories of personal data, this does not affect the lawfulness of the data processing, which is legally based on the execution of the employment relationship.

Data Sharing

Verisk may share your personal data with:

- Other Verisk entities; and
- Entities that provide/process: benefits; payroll; emergency communications; work-related travel arrangements; expense reimbursement; background checks; interoffice communication; training; incident intake; business cards; security; offsite data storage; customer and contract cycle management; ticketing management; facilities management services and other organizations that Verisk may engage to provide general support for general human resource, business management and security functions.

We may share personal data with service providers that perform services on our behalf such as payment service providers and hosting providers. In accordance with applicable law, we have entered into legally binding agreements requiring them to use or disclose personal data only as necessary to perform services on our behalf or comply with applicable legal requirements.

Verisk may also share your personal data with Verisk clients as required in connection with such clients' audits or security assessments of Verisk, or as otherwise required with regard to employees who perform functions or services on behalf of Verisk clients.

In addition, we may disclose personal data about you (a) if we are required or permitted to do so by law or legal process, for example due to a court order or a request from a law enforcement agency, (b) when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss, (c) in connection with an investigation of suspected or actual fraudulent or other illegal activity, and (d) in the event we sell or transfer all or a portion of our business or assets (including in the event of a reorganization, dissolution, or liquidation).

Cross-Border Transfers of Your Information

Your personal data may be disclosed to Verisk's affiliates or third parties either within or outside of the country from which it was collected. Some of your personal data may be transferred to a country (including the U.S.)that does not afford statutory protections for personal data equivalent to those within the country in which it was collected.

Protection of your data

Verisk maintains appropriate technical and organizational measures designed to protect your personal data against loss or accidental, unlawful or unauthorized, alteration, access, disclosure or use.

Data retention

Your personal data is retained for the duration of your relationship with Verisk, plus a reasonable period thereafter as necessary to fulfil the purposes described above. Retention periods may be extended if we are required to preserve your personal data in connection with litigation, investigations and proceedings, or if a longer retention period is required or permitted by applicable law.

Your Rights and Choices

Subject to applicable law, you may have the right to request:

- confirmation of whether we process personal data relating to you and, if so, to request a copy of that personal data;
- that we rectify or update your personal data that is inaccurate, incomplete or outdated;
- that we erase your personal data in certain circumstances, such as where we collected personal data on the basis of your consent and you withdraw that consent;
- that we restrict the use of your personal data in certain circumstances, such as while we consider another request that you have submitted, for example a request that we update your personal data;
- withdrawal of your consent where you have given us consent to process your personal data; and
- that we provide a copy of your personal data to you in a structured, commonly used and machine- readable format in certain circumstances.

If you wish to exercise any of your data protection rights or if you consider that we have processed your personal data in violation of applicable law, please contact us as detailed in the How to Contact Us section below.

If you consider that we have processed your personal data in violation of applicable law and failed to remedy such violation to your reasonable satisfaction, you may also lodge a complaint with the data protection supervisory authority in your country.

How to Contact Us

If you have any inquiries, complaints or requests in relation to the processing of your personal data, please contact please contact Bhanu Gudipati in your local Human Resources Department at Bgudipati@verisk.com.