

MERATIVE JOB APPLICANT PRIVACY NOTICE

Last Updated: July 2026

This Job Applicant Privacy Notice (“**Privacy Notice**”) explains how Merative L.P. and/or its subsidiaries (collectively, “**Merative**,” “**we**,” “**us**,” “**our**”) processes, collects, uses and discloses Personal Information about job applicants and prospective candidates who apply for or are considered for a position with us, including individuals identified or sourced through recruitment intermediaries (“**you**,” “**your**,” “**applicant**”).

In this Privacy Notice, “**Personal Information**” means information that identifies, relates to, describes, or could reasonably be linked to you. References to “**Personal Information**” also include “**personal data**,” and references to “**Sensitive Personal Information**” also include “**special categories of personal data**,” as those terms may be used under applicable data protection laws. For purposes of this Privacy Notice, references to Personal Information include Sensitive Personal Information, unless otherwise indicated. Personal Information does not include information that is de-identified or anonymized, in each case in accordance with applicable law, or lawfully made publicly available from government records, the applicant, or widely distributed media.

1. CHANGES TO THIS PRIVACY NOTICE

We may modify this Privacy Notice from time to time, in which case we will update the “Last Updated” date at the top of this Privacy Notice. If we make material changes to the ways in which we process your Personal Information, we will use reasonable efforts to notify you (such as by posting a notice on our careers site).

2. SOURCES OF YOUR INFORMATION

We collect Personal Information about you in connection with your application and our recruitment process from a variety of sources, including:

- Directly from you, including the information in your application, CV or résumé, cover letter, assessments, and interviews.
- Third party sources, such as recruiters and staffing agencies, your references, background-check and verification providers, and government agencies and regulators.
- Publicly available sources and tracking technologies, such as professional networking platforms (e.g., LinkedIn), used to identify and evaluate prospective candidates where relevant, and information collected automatically when you access our careers site or recruitment tools using cookies, pixels, and similar tracking technologies.

3. COLLECTION AND USE OF YOUR INFORMATION

Where required or permitted by local laws, we collect, and over the past 12 months have collected, the following categories of Personal Information:

- **Identifiers** such as name, email address, IP address, home address, date of birth, and phone number.
- **Contact and identification records** (including personal information categories listed in the California Customer Records statute) such as name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number.

- **Protected classification characteristics** (including characteristics protected under California and U.S. federal law) such as race, color, ancestry, sex (including gender, pregnancy, sexual orientation and gender identity), age, physical or mental disability, veteran status, and citizenship.
- **Internet or other similar network activity** such as information regarding your interaction with our careers site and recruitment tools.
- **Geolocation data** such as IP address (approximate location), location data if you use a mobile device to access our systems or use our internet or Wi-Fi connections.
- **Audio, electronic, visual, or similar information** such as recordings of video-enabled assessments or interviews, and any code you create during a coding assessment.
- **Professional or employment-related information** such as your CV or résumé, cover letter, work history, professional background, references and reference information, and interviewer or recruiter notes.
- **Education information** (including non-public education information protected under U.S. federal law) such as degree verifications and records of certifications or vocational training.
- **Inferences drawn from other Personal Information** such as assessments of your skills, qualifications, experience, and suitability for the role.
- **Government identifiers** such as Social Security number, driver's license, state identification card or passport number for onboarding.
- **Account access credentials** such as login credentials for any careers or recruitment account you create with us.
- **Health information** such as information related to reasonable accommodations for the recruitment process or onboarding.
- **Sensitive Personal Information.** The categories above include Sensitive Personal Information, such as government identifiers, account access credentials, health information, religious or philosophical beliefs, and information concerning sex life or sexual orientation.

We use the above Personal Information for various purposes in connection with the recruitment and hiring process, as permitted or required by law in the relevant jurisdiction, including:

- Assessing and progressing your application, including verifying your information; conducting relevant and legally permitted pre-employment, identity, and eligibility (including right-to-work) verification checks; and assessing your skills, qualifications, and experience.
- Communicating with you about your application and the recruitment process, including scheduling and conducting interviews, and about Merative events, jobs, and career opportunities.
- Completing the selection process and making hiring decisions.
- Conducting surveys and research to improve our recruitment process and analyzing our applicant pool to better understand who applies to Merative and how to attract talent.
- Safeguarding our business interests, including the security, availability, and resilience of our premises, IT systems, and recruitment tools, and preventing fraud and other unlawful activity.
- Complying with legal and regulatory obligations, including responding to requests from data subjects, law enforcement, regulators and courts, equal opportunities monitoring, and meeting legal reporting requirements.

- Where you accept an offer of employment, onboarding you and transitioning your information into your employment record.

We only use and disclose your Sensitive Personal Information for purposes necessary to assess and progress your application and for other purposes permitted under applicable law, such as ensuring security and integrity, short-term transient use, and conducting activities you reasonably expect, or where otherwise permitted or required by law.

We may deidentify your Personal Information such that it cannot reasonably be used to infer information about you or otherwise be linked to you (or we may collect information that has already been deidentified), and we may use and disclose such information for any purpose.

We may use artificial intelligence, machine learning, and similar automated tools to support our recruitment process, including to help review, screen, or assess applications. We do not use these tools to make decisions that produce legal or similarly significant effects concerning you without human involvement.

4. LEGAL BASES FOR PROCESSING

If you are located in the EEA or the UK, we will only collect and use your Personal Information where we have a legal basis to do so under the GDPR (meaning the EU General Data Protection Regulation and, as applicable, the UK GDPR). The legal bases we rely on include:

- **Contractual necessity (Steps prior to entering into a contract).** Where processing is necessary to take steps at your request prior to entering into an employment contract, such as assessing and progressing your application.
- **Compliance with a legal obligation.** Where processing is necessary to comply with our legal and regulatory obligations, such as verifying your eligibility and right to work and meeting legal reporting requirements.
- **Legitimate interests.** Where processing is necessary for our legitimate interests or those of a third party, such as sourcing suitable talent, assessing and selecting candidates, analyzing our applicant pool, and protecting our business and IT systems, provided these interests are not overridden by your interests or fundamental rights and freedoms.
- **Vital interests.** Where processing is necessary to protect your vital interests or those of another person, such as responding to a medical emergency or addressing a public health concern in the workplace.
- **Consent.** Where you have given consent to a specific processing activity, which you may withdraw at any time without affecting the lawfulness of processing before withdrawal.

Where we process special categories of personal data (such as information revealing racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic or biometric data, or data concerning health, sex life, or sexual orientation), we do so only where an additional condition under Article 9 of the GDPR applies, such as where processing is necessary for carrying out our obligations and exercising our rights in the field of employment, social security, and social protection law; for reasons of substantial public interest; for the assessment of your working capacity; for the establishment, exercise, or defense of legal claims; or with your explicit consent.

Where we collect Personal Information from you, the provision of certain Personal Information is necessary for us to consider and progress your application or to comply with our legal obligations. If you do not provide such Personal Information when requested, we may be unable to consider your application or progress it through the recruitment process.

5. DISCLOSURE OF YOUR INFORMATION

In certain circumstances, we may disclose your Personal Information to third parties for legitimate purposes, subject to this Privacy Notice, including:

- Related entities in our corporate group as may be necessary to consider and progress your application, including hiring managers, recruiters, talent acquisition personnel, and the relevant business line (including where your prospective management line is located in another country) (“**Related Entities**”).
- Vendors who provide recruitment-related services such as human resources information systems (such as Workday) and applicant tracking systems, recruitment process outsourcing providers, background-check and verification providers, assessment providers, occupational health and safety management systems, cloud storage and IT services, and providers of artificial intelligence and machine learning tools that support our operations (“**Service Providers**”).
- Government agencies, regulators, and other authorities, as necessary to meet legal reporting requirements and comply with our legal and regulatory obligations (“**Government Agencies**”).
- Professional advisors, such as auditors, outside legal counsel, accountants, and forensic specialists, who support our business and assist with investigations and audits (“**Professional Advisors**”).
- Law enforcement, courts, regulators, and other third parties, in connection with a legal obligation, such as to comply with applicable law or legal process, respond to lawful requests, exercise or defend legal claims, and protect our rights, property, or safety, or that of third parties, as required or permitted by law (“**Legal Parties**”).
- Third parties in connection with or anticipation of an asset sale, merger, bankruptcy, or other business transaction (“**Business Transaction Parties**”).
- Other third parties with your permission or at your direction.
- Other third parties in other limited circumstances, such as where we believe disclosure is necessary to prevent physical harm or financial loss, or in connection with an investigation of suspected or actual illegal activity or where we need to contact your referees to confirm your references.

In the preceding 12 months, we disclosed the following categories of Personal Information about you:

Categories of Personal Information	Categories of Recipients
Identifiers	Related Entities; Service Providers; Government Agencies; Professional Advisors; Business Transaction Parties

Contact and identification records	Related Entities; Service Providers; Government Agencies; Professional Advisors
Protected classification characteristics	Related Entities; Service Providers; Government Agencies; Business Transaction Parties
Education information	Related Entities; Service Providers; Government Agencies
Internet or other electronic network activity information	Related Entities; Service Providers
Health information	Related Entities
Geolocation data	Related Entities; Service Providers
Audio, electronic, visual, or similar information	Related Entities; Service Providers
Professional or employment-related information	Related Entities; Service Providers; Government Agencies
Inferences drawn from other Personal Information	Related Entities; Service Providers
Government identifiers	Related Entities; Service Providers; Government Agencies
Account access credentials	Related Entities; Service Providers
Sensitive Personal Information	Related Entities; Service Providers; Government Agencies

We do not sell Personal Information or share Personal Information for cross-context behavioral advertising purposes, nor have we done so in the preceding 12 months. We do not have actual knowledge that we sell or share for cross-context behavioral advertising purposes Personal Information of individuals under 16 years of age.

6. DATA SECURITY

We maintain reasonable physical, administrative, and technical safeguards designed to protect your Personal Information against loss, theft, and unauthorized access, use, disclosure, alteration, or destruction. However, no method of transmission or storage is completely secure, and we cannot guarantee absolute security.

7. INTERNATIONAL TRANSFERS OF YOUR INFORMATION

If you are located in the EEA or the UK, your Personal Information may be transferred to, stored in, or accessed from countries outside the EEA or the UK, including the United States, Canada, India, and Singapore, where we, our Related Entities, and our Service Providers operate. These countries may not provide the same level of data protection as your home jurisdiction. Where we transfer your Personal Information outside the EEA or the UK, we implement appropriate safeguards required under the GDPR,

such as transfers to countries that the European Commission or, as applicable, the relevant UK authorities have determined provide an adequate level of protection, or transfers made pursuant to the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism. You may obtain a copy of the safeguards we have put in place by contacting us using the information provided below.

8. RETENTION OF YOUR INFORMATION

We retain your Personal Information for as long as is reasonably necessary for the purposes specified in this Privacy Notice and to comply with our legal and regulatory obligations, resolve disputes, and establish, exercise, or defend legal claims. When determining the length of time to retain information about you, we consider various criteria, including whether we need the information to continue to provide you with the services, resolve a dispute, enforce our contractual agreements, prevent harm, promote safety, security and integrity, protect ourselves, including our rights, property or product, or otherwise in accordance with applicable law.

If you accept an offer of employment, the Personal Information collected during the recruitment process may become part of your employment record and be retained in accordance with our employee retention practices. If we do not employ you, we will retain your Personal Information in accordance with Merative's records management policy or otherwise in accordance with applicable law, after which it will be erased or anonymized in accordance with applicable law.

Personal Information may be maintained in various formats, including in digital and physical records, and in other automated systems that are capable of outputting Personal Information.

9. YOUR RIGHTS

Depending on where you are located, you may have the rights listed below in relation to Personal Information that we have collected about you. The availability of these rights, and the conditions for exercising them, depend on the law that applies to you. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by applicable law.

- **Right to Know/Access.** Request a copy of the personal data we hold about you, along with information about how we process that data.
- **Right to Correct.** Request that we correct inaccurate, incomplete, or out of date Personal Information maintained about you.
- **Right to Delete.** Request that we delete your Personal Information. You may request that we delete your personal data in certain circumstances, such as when it is no longer necessary for the purposes for which it was collected, or if you have withdrawn your consent (where applicable). Please note that there are exceptions where we may be required by law to retain certain information.
- **Right to Restrict Processing.** Request that we restrict the processing of your Personal Information in certain circumstances. You have the right to request that we limit the processing of your personal data under specific conditions, such as when you contest the accuracy of the data or object to its processing. In some instances, we may continue processing the data if it is necessary for legal claims or compliance with other legal obligations.

- **Right to Data Portability.** Request that we provide certain Personal Information you have provided to us in a structured, commonly used, and machine-readable format, and that we transmit it to another controller where technically feasible.
- **Right to Object.** Object to our processing of your Personal Information where we rely on legitimate interests.
- **Right to Withdraw Consent.** Where we rely on your consent to process your Personal Information, you can withdraw that consent at any time, without affecting the lawfulness of processing before withdrawal.
- **Right to Lodge a Complaint.** Lodge a complaint with a supervisory authority, such as the data protection authority in the country where you live or work or where an alleged infringement occurred or, for the UK, the Information Commissioner's Office.

You may exercise any of these rights by contacting us using the information provided below. We will not discriminate against you for exercising any of these rights. We may need to collect information from you to verify your identity, such as your email address or government-issued ID, residence address, or date of birth, before providing a substantive response to the request. Some jurisdictions, depending on your location, permit you to authorize an agent to make requests on your behalf to exercise your rights. If you have a registered agent to act on your behalf, we have the right to authenticate such agent's authority to act. Please be aware that, depending on the circumstances, if you ask us to delete your Personal Information, withdraw your consent, or otherwise stop processing your Personal Information, we may be unable to consider or continue to progress your application.

10. HOW TO CONTACT US

Should you have any questions about our privacy practices or this Privacy Notice, or if you would like to exercise any of your rights, please contact us by submitting a [Merative Privacy Contact Request Form](#). Your message will be forwarded to the appropriate member of Merative's data protection and compliance team. You may also contact us at 1-866-457-3206 or 100 Phoenix Drive, Suite 200, Ann Arbor, Michigan 48108.

For EEA and UK Applicants. For purposes of the GDPR, the data controller responsible for your Personal Information is the Merative subsidiary (legal entity) to which you applied or that is considering your application, unless Merative or another Merative subsidiary identifies itself as the controller for a specific interaction with you. Our Data Protection Officer can be contacted at Privacy@Merative.com. If you have any questions or concerns about how we process your Personal Information, we encourage you to contact us first so that we can try to address them. You also have the right to lodge a complaint with the supervisory authority in the EEA or UK jurisdiction where you live or work or where an alleged infringement occurred, including, for the UK, the Information Commissioner's Office (ICO); contact details for the EU data protection authorities are available on the European Commission's website.