

Recruitment Privacy Statement

Last Modified – 28th January 2025

This Recruitment Privacy Statement (“**Statement**”) describes how Mitsogo.Inc (“**Company**”, “**we**”, “**us**” and “**our**”) collects, uses, and discloses information about individuals who apply for open positions at our Company (“**Applicants**”).

This Statement does not apply to our handling of data gathered about you in your role as a user of our services. If you interact with us as in that role, the [Privacy Policy](#) applies.

Please read this Statement carefully. Please note that this Statement does not form part of any employment contract or contract to provide services.

Personal Information collected

We collect, store, and use various types of information that identifies, relates to, or could reasonably be linked to you (“**personal information**”) in connection with your application for employment with us. We may collect additional personal information throughout the course of your application process.

The information we collect from and about Applicants includes, where applicable:

Identifiers such as first and last name, postal address, telephone number, and email address, and, if provided an offer, identifiers related to your citizenship documents, such as driver’s license or passport.

Professional or employment-related information, including:

- **Recruitment, employment, or engagement information** such as application forms and resumes, cover letter, CV, contact details of your references, desired salary range, or other data you provide through the application and recruitment process;
- **Career information** such as current employment, past employers, titles, job history, work dates and work locations, salary expectations, notice period, and information about skills, qualifications, membership in professional organizations, and experience.
- **Education information** such as institutions attended, degrees, academic record, certifications, licenses, transcript information, and professional memberships.
- **Geolocation data**: such as approximate location inferred from your IP address, city, or county.
- **Potentially protected classification information** to the extent required or as permitted by law and voluntarily provided such as race/ethnicity, color, sex/gender, military and veteran status, disability, accommodation information, nationality, citizenship, and other information (insofar as such information is “sensitive personal information,” we use it for the purposes set forth below specific to sensitive personal information).

- **Other information** that you may voluntarily choose to include on your resume, in connection with your application, during your interview, or otherwise.

Use of Personal Information

We may collect, use, disclose, and store personal information for the following, where applicable:

- **Engaging in the recruitment process**, including communicating with you; contacting you about jobs you may be interested in; interviewing, selecting and hiring new personnel; responding to your inquiries or requests; verifying eligibility for employment; conducting applicant reference checks to assist in hiring decisions; conducting background and related checks; employee onboarding; maintaining and administering payroll and employee benefit plans maintaining personnel records; and complying with record retention requirements.
- **HR management and administration**, including determining compensation, scheduling, IT and informational security purposes, fraud prevention, conducting internal analyses and audits, promoting the Company's diversity and inclusion, and perform workforce analytics, data analytics, and benchmarking; providing you with HR and employment-related services and support; engaging in human capital analytics (including to identify correlations about individuals and job success, analyze data to improve retention and productivity, and analyze employee preferences) to inform human resources policies and procedures; and communicating with you, your emergency contacts, or your beneficiaries.
- **Security operations**, including detecting security incidents, debugging and repairing errors, and preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution; facilitating the efficient and secure use of Company information systems; ensuring compliance with Company information systems policies and procedures; and safeguarding the Company and its locations, services, and employees.
- **Safeguarding Company and the services**, including the protection of the Company, our workforce, users, partners, and others.
- **Legal compliance and exercising our legal rights**, such as complying with applicable laws; responding to and cooperating with legal or regulatory requests and investigations; conducting internal audits; investigating grievances, complaints, and suspected violations of the law or Company policies; exercising or defending the legal rights of the Company and its employees; seeking legal advice from our external lawyers or in connection with litigation with a third party; and responding to requests as required by applicable law or court order.

- **At your request**, in order to fulfil your instructions.

We may also use personal information for any other legally permitted purpose (subject to your consent, where legally required).

Some personal information we collect in the recruitment process, such as ethnicity and veteran status, may be considered “**sensitive**” under applicable law. We use such information only for the following purposes: government reporting purposes, such as to help us monitor compliance with equal opportunity legislation; designing, implementing, and promoting our diversity and inclusion programs; analyzing and understanding our workforce; conducting internal audits; investigating grievances and suspected violations of Company policy; and exercising or defending the legal rights of Company or our employees. Some “sensitive” information may be required for certain job applications

In countries where we are required to state the “legal basis” on which we process personal information, we process Applicants’ personal information where:

- The processing is necessary to enter into or perform a contract to which you are party, such as to evaluate whether we want to enter into an employment contract with you.
- We, or a third party, have a legitimate interest in using your personal information for business purposes such as evaluating your candidacy for employment, determining compensation, and security.
- The processing is necessary for compliance with a legal obligation.
- You have consented to such processing.

Disclosure of Personal Information

We may disclose certain personal information to the following types of entities or in the following circumstances (where applicable):

- **Internally:** to employees within the Company that participate in the recruitment process, such as HR managers and employee interviewers, and among our corporate affiliates.
- **Vendors:** such as background check companies, security providers, information technology providers, travel management companies, and employment businesses that provide us with services relevant to recruiting and hiring.
- **Recruiters:** to the extent you are working with a recruiter in connection with your application for employment and your recruiter is authorized by you to obtain feedback from us regarding your application and interview process.
- **Legal compliance and exercising legal rights:** (i) when required to do so by law, regulation, or court order, (ii) in response to a request for assistance by the police

or other law enforcement agency; (iii) to seek legal advice from our external lawyers or in connection with litigation with you or a third party or (iv) as otherwise necessary to exercising our legal rights or to protect the Company or its employees.

- **Business transaction purposes:** in connection with the sale, purchase, or merger of all or a portion of our Company.
- **Consent:** with your consent and as permitted by law, we may disclose personal information to any other parties in any other circumstances.

Data Retention

The personal information we collect from Applicants will be retained until we determine it is no longer necessary to satisfy the purposes for which it was collected and our legal obligations. As described above, these purposes include our business operations and complying with reporting, legal and accounting obligations. In determining how long to retain information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the personal information, the purposes for which we process the personal information and whether we can achieve those purposes in other ways, the applicable legal requirements, and our legitimate interests.

Additional Privacy Information for Residents of Certain Jurisdictions

Residents of California, the European Economic Area ("EEA"), the United Kingdom ("UK"), and Switzerland have certain rights regarding their personal information. This section is solely applicable to such residents to the extent that such rights apply.

California: Subject to certain exceptions, if you are a California resident, you may request:

- access to certain of your personal information, including the right to know the categories of personal information we have or will collect about you and the reason we will or have collected such information;
- correction of certain of the personal information that we have about you that is inaccurate; or
- deletion or removal of certain of your personal information.

You also have the right not to be discriminated against (as provided for in California law) for exercising your rights.

EEA, UK, and Switzerland: Subject to certain exceptions, if you are in the EEA, UK, or Switzerland, you may request:

- access to your personal information;
- correction of certain of the personal information that we have about you that is inaccurate;

- deletion or removal of certain of your personal information;
- to receive personal information you provided to us to transmit it to another entity;
- to object to or restrict certain processing of your personal information; or
- to withdraw consent to our future processing of your personal information where the basis of such processing is your consent.

CPRA and CCPA

The California Privacy Rights Act (CPRA) [formerly the California Consumer Protection Act (CCPA)] reserves the right for consumers to request the disclosure of collection and usage of their Personal Data . It also reserves the right to opt-out from any kind of sale of Personal Data by the business.

We do not sell your Personal Data. We follow the standards mentioned in this Statement while handling Personal Data of any kind. We define all the data we collect under the “Personal Information collected” section and the usage of said data under the “Use of Personal Information” section. You can also read about how third parties make use of cookies from our Cookie Policy at <https://www.hexnode.com/legal/cookies-policy/>.

To request disclosure of any information as described by CCPA, you can mail to us at privacy@hexnode.com

Exceptions to Your Rights

There are certain exceptions to the above-mentioned rights. For instance, we may retain your personal information if it is reasonably necessary for us or our service providers to provide a service that you have requested or to comply with law or to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity or prosecute those responsible for that activity.

Exercising Your Rights

To exercise one of the rights above, you may contact us as provided below. We will take reasonable steps to verify your identity before responding to a request. In doing so, we may ask you for verification information so that we can match at least two verification points with information we maintain in our files about you. If we are unable to verify you through this method, we shall have the right, but not the obligation, to request additional information from you.

Changes

We reserve the right to modify and update this Statement at any time. When we make only minor modifications, we may do so without notifying you. If we make changes to this Statement that we believe materially impact the privacy of your Personal Data, we may notify you. We encourage you to periodically review this page for the latest information

on our privacy practices. The “Last Modified” date at the top of this Statement will allow you to quickly know when the last changes were made.

Contact Us

If you have any questions about this Statement, please contact us by email at privacy@hexnode.com.