

Ouro HR Privacy Notice

Updated July 31, 2025, Effective: July 31, 2025

This HR Privacy Notice (“Notice”) applies to Ouro Global, Inc. (“Ouro Global”), Ouro Insurance Agency, LLC (“Ouro Insurance”), and their affiliates (collectively, “Ouro” “we” or “us”). If you’re an Ouro consumer, please see our [Ouro U.S. Privacy Notice](#).

About Ouro

Ouro is a financial technology company, not a bank or insurance company. Ouro is an authorized agent and program manager for Netspend® and other bank products issued by Pathward®, National Association (“Pathward”), Republic Bank & Trust Company, (“Republic”), The Bancorp Bank, N.A., (“Bancorp”) and Texas First Bank (“TFB”); Members FDIC, each a “Bank”; and a licensed producer agent assisting individuals in the procurement of certain policy coverages from the Chubb Group of Insurance Companies (“Chubb”) and Direct Auto Insurance, a subsidiary of Allstate (“Direct Auto”), each an “Insurer”.

Ouro HR Privacy Notice

Ouro understands that like consumers, its applicants also have questions and concerns about privacy. This Notice describes the types of personal information (“Personal Information”) we collect, how we use it, who we may disclose it to, and your choices in the context of your employment application with Ouro. This Notice does not apply to the practices of third-party websites, services, or applications, including third parties with whom we partner for which Ouro is not responsible.

I. PERSONAL INFORMATION WE COLLECT

In connection with your employment application, Ouro may collect personal information about you as described below. Ouro collects your personal information to the extent that you disclose it to Ouro directly or through third parties such as recruiting platforms, job-posting sites, talent professionals, or representatives (e.g. attorneys). Ouro also collects certain personal information from you automatically when you access our network, electronic communication systems, or internal services. Ouro also may generate or infer personal information about you.

Identifiers:

Ouro collects identifiers you or third parties provide us during the application process. These include your name, date of birth, physical address, email address, and phone number. Ouro

may automatically collect digital identifiers such as device ID and IP address when you interact with online application tools.

Ouro may collect this information from you, third-party benefits platforms, third party background-check platforms, third party application platforms (such as LinkedIn), Ouro's internal application tools, or your resume.

Employment Information:

In addition to the information you provide us, Ouro may collect information relating to your employment history, including through background and reference checks with your explicit consent after a formal job offer has been extended. Ouro may also collect employment information about you from social or career networking sites, your former employers, and other people familiar with your employment history.

Education Information:

In addition to the information you provide us, Ouro may collect information relating to your education history through background and reference checks with your explicit consent. Ouro may also collect education information about you from your resume, education institutions, social or career networking sites, your former employers, and other people familiar with your education history.

Characteristics of protected classes:

During the application process, Ouro may learn information about your race, age, ethnicity, sex, gender, sexual orientation, marital or family status (including pregnancy), religion, national origin, immigration or work permit status, alienage, military/veteran status, or disability from you or other persons familiar with you.

Audio, electronic, and visual information:

Ouro may collect audio recordings, video recordings, photos, or screen grabs containing your likeness.

Internet or other electronic network activity information:

Ouro collects analytics and monitoring data such as data related to your communications and use of Ouro's external websites such as our careers pages; information collected through web beacons, like cookie IDs; information collected through mobile apps, such as mobile device IDs; features used and actions taken in Ouro's websites or platforms ("Ouro Systems"), including page views, links clicked, and documents downloaded; contents, header, metadata, delivery and access information for voice calls, voicemail, emails, chats, messaging, documents, and other communications, data, and files stored or transmitted through Ouro Systems.

Biometric and health information:

Ouro does not collect information from you related to your exposure or risk of exposure to an epidemic disease (e.g. COVID), including symptomatic, diagnostic, and behavioral (e.g., travel to an outbreak location) indicators.

Ouro does not collect certain biometric information (e.g. picture, faceprint, fingerprint, voiceprint, retina or iris image, or any other biological characteristics) for the purpose of authentication and security while entering or navigating our offices.

Inferences, generated data, opinions, and other information:

Ouro may also receive or generate facts, opinions, inferences, or conclusions about you from other Ouro employees, contractors, business partners, investors, and vendors.

II. HOW WE USE PERSONAL INFORMATION WE COLLECT

Ouro uses the information we collect about you for the purpose of processing job applications, evaluating candidates for employment, and carrying out recruiting functions and activities, including as described below.

Managing applicant activities and recruiting generally:

This includes verifying your identity; processing and evaluating job applications; performing background checks with your explicit consent after a formal job offer has been extended; determining suitability for employment; determining physical and/or mental fitness for work; discussion, review, and approval or denial of disability accommodations; determining salary and other forms of compensation; screening references; securing immigration sponsorship and/or transfer; revising hiring decisions; and providing access to facilities.

Ensuring business continuity and protecting the health and safety of our staff and others:

This includes safeguarding, monitoring, and maintaining our IT infrastructure, office equipment, facilities, and other property; detecting or preventing theft or fraud, or attempted theft or fraud; enabling internal and external communications and collaboration; and facilitating communication with you and your designated contacts in an emergency.

Operating, managing, monitoring, protecting, and improving our IT, facilities, and electronic communications systems:

This may include the recording or interception of activities or communications conducted using our electronic communications systems, such as our applicant portal; detect and protect against unauthorized access to and use of Ouro systems; perform data analytics, including application and device performance and usage; improve our applicant intake; allocate and manage our assets and human resources; develop tailored recruiting programs; personalization of services to understand your preferences and enhance your applicant experience; strategic planning; project management; compiling audit trails and other reporting tools; maintaining records relating to business activities, budgeting, and financial management; managing

mergers, acquisitions, sales, reorganizations or disposals and integration with business partners; detecting and preventing security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity; debugging to identify and repair errors that impair existing intended functionality; undertaking internal research for technological development and demonstration; undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by Ouro, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by Ouro.

Complying with legal requirements, such as tax, record-keeping, and reporting obligations:

This may include conducting audits; management and resolution of health and safety matters; complying 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 internal complaints or claims; conducting investigations; and complying with internal policies and procedures.

Data retention and assessing applicants for additional opportunities

To the extent permitted by applicable law, Ouro may retain the personal information it collects and any opinions or conclusions made about you as a record of your candidacy. In addition, Ouro may periodically review your record for fit with additional opportunities and may use your information to contact you regarding additional career opportunities at Ouro.

III. HOW WE DISCLOSE PERSONAL INFORMATION WE COLLECT

Additionally, Ouro may disclose any personal information, including sensitive personal information, to the following categories of third parties for the purposes described below, if required by law, or with your consent:

Subsidiaries and affiliates:

This may include Ouro's subsidiaries and affiliates which share business processes and common data systems;

Vendors and agents:

This may include Ouro's vendors or agents to perform services on our behalf, including providers of our background-checking services and applicant tracking services. To the extent that we provide personal information to such third parties, that personal information is governed by their privacy statements and any contractual requirements we have entered into with them.

Parties to a corporate transaction or proceeding:

This may include parties that are part of a merger, financing, acquisition, bankruptcy, dissolution, or a transfer, divestiture, or sale of all or a portion of our business or assets.

Law enforcement and those with legal necessity:

This may include disclosing personal information to comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies; operate and maintain the security of our systems, network, and information, including to prevent or stop an attack on our systems or networks or the disclosure of our information; protect the rights or property or ourselves or others, including enforcing our agreements, terms, and policies; to act in urgent circumstances such as protecting the health or personal safety of an employee, worker, agent, customer, user of Ouro services, or member of the public.

IV. CALIFORNIA SPECIFIC DISCLOSURES

Ouro may collect your signature, physical characteristics or descriptions, state identification card number, education information, or any other information subject to Cal. Civ. Code § 1798.80 provided by you.

Ouro does not “sell” or “share” your personal information and only discloses your information for a valid “Business Purpose” as those terms are defined by the California Consumer Privacy Act (“CCPA”), as amended and expanded by the California Privacy Rights Act (“CPRA”), and in the context of your applicant relationship with the Company. If you use Ouro products or services that information is governed by the [Ouro U.S. Privacy Notice](#).

Ouro may retain personal data for as long as necessary to carry out and support applicant functions and activities, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes. Because these needs can vary for different data types in the context of different services, actual retention periods can vary significantly based on criteria such as business expectations, the sensitivity of the data, and our legal or contractual obligations.

V. YOUR CHOICES

You have the right to opt out of the selling or sharing of your data. To opt-out, submit your privacy request to Ouro at P.O. Box 2136, Austin, TX 78768-2136, email: privacy@ouro.com, Tel: 1-866-387-7363. We may request certain information to verify your identity to complete your request.

VI. HOW TO EXERCISE YOUR PRIVACY RIGHTS

You or your authorized agents may submit a request by phone at 1-866-387-7363, or by submitting a [Privacy Request Form](#) to us by mail at P.O. Box 2136, Austin, TX 78768-2136, or by email at privacy@ouro.com. If you’re making a request as an Authorized Agent, you must also

fill out, sign and attach the [Authorized Agent Form](#) to your request. If the request is submitted by someone with a power of attorney (POA), the POA may be submitted instead of the Authorized Agent Form.

Authentication/Verification. To help protect your privacy and maintain security when you submit a privacy request, we are required to reasonably validate your identity. To fulfill your request, we may require you to sign a declaration under penalty of perjury that you are the consumer whose Personal Data is the subject of the request. If we cannot validate the requestor based on the information provided, we will notify the requestor that we are unable to fulfill the request. We will only use Personal Data provided in the request to verify the requestor's identity or authority to make it. We will confirm receipt of a request within ten (10) business days. We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period. We do not charge a fee to process or respond to a verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will detail why we made that decision and provide a cost estimate before completing the request.

Declining Requests. Except for the automated controls described in this Notice, if you send us a request to exercise your rights or the choices in this section, to the extent permitted by applicable law, we may charge a fee or decline requests in certain cases. For example, we may decline requests where granting the request would be prohibited by law, could adversely affect the privacy or rights of another person, would reveal a trade secret or other confidential information, would interfere with a legal or business obligation that requires retention or use of the data, or because the data at issue is not covered under the law you are asserting.

Changes to This Privacy Notice. This Notice may be revised from time to time due to legislative changes, changes in technology, our privacy practices, or new uses of your information not previously disclosed in this Policy. Revisions are effective upon posting and your continued use of this Platform or Services will indicate your acceptance of those changes. Please refer to this Policy regularly.

VII. QUESTIONS ABOUT THIS PRIVACY NOTICE

If you have questions about this Notice, please contact us at privacy@ouro.com.