



State Privacy Notice Addendum

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

Currently nineteen states have passed and signed privacy legislation into law. State laws, among other provisions, provide consumers with certain privacy rights, such as the right to know, right to delete, right to correct, right to opt-out, and right to non-discrimination. Specific state notices are provided below.

Generally State privacy laws exclude Personal Data already covered by Federal financial services privacy laws such as the Gramm-Leach-Bliley Act (GLBA). As a result, these rights granted do not apply to Personal Data related to a financial account. However, California, Minnesota, and Oregon impose additional obligations for data not covered by GLBA. Specifically, this includes marketing data collected through prospect lists, tools like Google Analytics on Ouro websites, employee information, business contact data (such as contacts at retail stores, distributors, or vendors), and mobile app usage data.

Click below to locate your resident state:

[California](#)

[Minnesota](#)

[Oregon](#)

For California Residents

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

The California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020 (collectively "CPRA" or "California Privacy Law") provide consumers residing in that state ("California Consumers", "you", or "your") with specific rights regarding their Personal Data ("Personal Data"). This notice ("CPRA Privacy Notice") supplements the information contained in the [Ouro U.S. Privacy Policy](#) ("Ouro Privacy Policy") and explains how Ouro, and our subsidiaries and affiliates, ("Ouro," "we," "us," or "our") collect, use, disclose and retain Personal Data and how California Consumers may exercise their rights under the CPRA.

Except for those terms defined within this CPRA Privacy Notice, all other capitalized terms shall have the same meaning as those designated in the Ouro Privacy Policy.

Information We Collect:

Under the CPRA, "Personal Data" means any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment

history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. “Personal Data” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

We may collect (and may have collected during the 12-month period prior to the effective date of this Statement) the following categories of Personal Data about you:

- **Identifiers.** Identifiers such as a real name, signature, postal address, physical characteristics or description, unique personal identifiers (such as a device identifier; cookies, beacons, pixel tags, mobile ad identifiers and similar technology; photographs and images, customer number, unique pseudonym, or user alias; telephone number and other forms of persistent or probabilistic identifiers), online identifier, physical address, internet protocol address, email address, account name, social security number, driver’s license number or state identification card number, passport number, debit card number, credit card number, or any other financial information, insurance policy number, insurance claim number, and other similar identifiers. Some Personal Data included in this category may overlap with other categories.
- **Additional Data Subject to Cal. Civ. Code § 1798.80.** Signature, physical characteristics or description, passport number, driver’s license or other state identification card number, education, bank account number, credit card number, debit card number, and other financial information.
- **Protected Classifications.** Characteristics of protected classifications under California or federal law, such as race, ancestry, national origin, religion, age, sex, gender, marital status, citizenship status, military and veteran status, among others.
- **Commercial Information.** Commercial information, including records of personal property; products or services purchased, obtained, or considered; policy and claim information; and other purchasing or consumer histories or tendencies.
- **Online Activity.** Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding your interaction with websites, applications or advertisements.
- **Geolocation Data.** We use your IP address to determine your general location (such as city, state, or zip code).
- **Sensory Information.** Audio, electronic, visual, and similar information.
- **Employment Information.** Professional or employment-related information.
- **Inferences.** Inferences drawn from any of the information identified above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

- **Sensitive Personal Data.** We will not process your “Sensitive Personal Data” without your consent. Under the CPRA, Sensitive Personal Data consists of:
 - **Government ID.** Government identification such as social security numbers, driver’s license, state identification card, or passport number.
 - **Account access information.** Information such as account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account,
 - **Precise geolocation data.** Data derived from a device and that is used or intended to be used to locate you within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.
 - **Communications Content:** The contents of mail, email, and text messages (unless Ouro is the intended recipient).
 - **Sensitive demographic data.** Racial or ethnic origin, religious or philosophical beliefs, or union membership.
 - **Genetic Data:** We do not collect or use genetic data.
 - **Biometric Information:** We do not collect or use biometric information to uniquely identify a consumer.
 - **Health Information:** We do not collect or use Personal Data concerning a consumer's health.
 - **Sex Life or Sexual Orientation:** We do not collect Personal Data concerning a consumer's sex life or sexual orientation.

Our Purposes for the Collection and Use of Personal Data:

We may collect Personal Data directly from consumers (including customers, candidates, and employees), affiliates, business partners, agents, and vendors. Our collection of Personal Data is limited to the business and commercial purposes as described below:

1. Perform services, including maintaining or servicing accounts, processing transactions, and/or other benefits, providing customer service, and other related activities (“Services”).
2. Verify customers’ information, identity, and eligibility to receive Services.
3. Send transactional communications as part of our Services and marketing communications that we believe may interest you.
4. Determine your eligibility for, and administer your participation in, certain features of the Services, including, but not limited to, surveys, contests, sweepstakes, promotions and rewards;

5. Conduct research, assessments, and analytics relating to our Services and develop new services, products and technological improvements.
6. Administer, audit, and improve our Platform.
7. Improve, upgrade, or enhance our Services or business operations.
8. Administer quality and safety maintenance for our Platform or Services.
9. Facilitate applicant tracking and employee recruitment.
10. Contact customers and consumers with information on Services, new Services or products, or upcoming events, including via SMS or MMS text messaging if mobile phone number is provided for that purpose and auditing those interactions.
11. Perform advanced analytics and provide insights to customers.
12. Detect fraud, theft, or other activities to ensure security and integrity by detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
13. Comply with legal, reporting, and regulatory requirements or to defend against a legal claim.
14. For other purposes that are compatible with this Privacy Policy or where permitted by applicable law.
15. In any other way we may describe when you provide the information, or for which you provide authorization.

We may aggregate or de-identify your Personal Data for these same purposes.

Special Notes:

Treatment of Sensitive Personal Data. You have the right to limit our processing of your “sensitive” data for the purpose of inferring characteristics about you. We may collect or process your sensitive Personal Data for the purpose of inferring characteristics about you, under the following conditions:

- only as necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.
- To help ensure security and integrity to the extent the use of the consumer's Personal Data is reasonably necessary and proportionate for these purposes, such as:
 - Short term transient use as part of your current interaction with us provided that we do not disclose your Personal Data to another third party and do not build a profile about you or otherwise alter your experience outside the current interaction with the business.
 - Performing services on behalf of the business including maintaining or servicing accounts, providing customer service, processing and fulfilling orders or transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage or similar services on behalf of the business.

- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Should we seek to process sensitive Personal Data for users outside these categories and to infer characteristics about you, we shall (1) provide notice to you explaining those uses and (2) allow you to opt out of those uses. If you exercise your right to limit our use or disclosure of your Sensitive Personal Data, we shall refrain from using or disclosing this information and wait at least twelve (12) months before requesting you again to authorize your use or disclosure of such information for additional purposes.

Sources of Personal Data:

During the 12-month period prior to the effective date of this Statement, we may have obtained Personal Data about you from the following categories of sources:

- Directly from you, such as when you sign up for an account, initiate a transaction, contact customer service or support departments via phone, email, chat or other forms of communication, or from applications, forms, webinars, surveys, and other information you provide us.
- Your devices, when you use our Platform or Services.
- Your comments or suggestions, interaction with us, requests for information or contact with our customer service or support departments.
- External banks (i.e., banks other than our Banks) if you link a non Ouro-serviced account.
- Vendors who provide services on our behalf.
- Our joint marketing partners.
- Our business partners (such as referring websites).
- Online advertising services and advertising networks.
- Government entities.
- Operating systems and platforms.
- Social networks.
- Data brokers, lead generation partners, and identity resolution service providers.

In order for us to receive your information from a lead generation partner, you must have opted-in to the partner sharing your information for direct marketing purposes or the partner may have collected your information from publicly available sources. We keep a record of your opt-in to ensure that we are not marketing to prospects without consent.

If you have received direct marketing from us, there are cases where we are not able to determine a prospect's current contact information with the information provided by our lead generation partners. In those cases, we use third-party identity resolution service providers in order to verify the address and aid us in determining whether to use the lead. In the past 12 months, We have shared contact information with these third-party service providers. Our identity resolution service providers are contractually not permitted to use your information for any other purpose.

Categories of third parties with whom Personal Data was shared:

We may use, disclose, or transmit Personal Data we collect to other service providers or other third parties for business purposes, to provide our Services, or for other purposes as provided by the CPRA as described below:

- A. Our affiliates, partners, or subsidiary organizations.
- B. Government agencies to fulfill legal, reporting and regulatory requirements.
- C. Our employees, affiliated companies, subsidiaries, contractors, agents, third-party partners including distributors and employers for payroll cards, and vendors to perform Services related to your account, to offer additional services, perform analysis to determine qualifications to receive other services, collect amounts due, or for our business operations.
- D. Third-party providers for services that you may sign up for via our Site or Services or other business partners with whom we work to develop or market certain products or services.
- E. Bank partners, insurance provider partners, data, payroll, and payment processors to process transactions.
- F. Cloud providers, customer management platforms, security providers, and similar services in connection with providing products, and, in the support of, our Services.
- G. Law enforcement or government officials. We reserve the right to release information if we are required to do so by law or if, in our business judgment, such disclosure is reasonably necessary to comply with any court order, law, or legal process, in a fraud investigation, an audit or examination.
- H. Attorneys, accountants and auditors.
- I. To a buyer or successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us is among the assets transferred.
- J. Any other entity we disclose when you provide the information, or for which you provide authorization.

Categories of Personal Data Sold or Shared to Third Parties:

We do not sell Personal Data with third parties for monetary consideration. We only make business purpose Personal Data disclosures as detailed above and pursuant to written contracts that describe the purposes of use, require the recipient to keep Personal Data confidential, and prohibit using the disclosed Personal Data for any purpose except performing the contract.

The chart below describes the categories of Personal Data collected in the previous twelve (12) months, the business or commercial purposes for such collection, and the categories of third parties with whom we may have disclosed Personal Data for a business purpose in the previous twelve (12) months:

Category of Personal Data that We May Collect and Transmit	Examples	Collected During the Past 12 Months	Business or Commercial Purpose	Categories of Third Party with Whom We May Have Disclosed Personal Data During Past 12 Months
Personal Data	Full name, address, telephone number, Social Security number, date of birth, driver's license number, passport numbers, financial, bank account, geolocation data, medical and beneficiary information, signatures, vaccination related information, and similar identifiers	Yes	1-15	A-J
Sensitive Personal Data	Social Security number, driver's license, state ID card, passport number, a consumer account login, financial account, debit card or credit card number in combination with any: required security code, password, credentials allowing access to an account, a consumer's precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, contents of: a consumer's mail, email and text messages (unless the business is the intended	Yes	1-4, 6-15	A-J

	recipient), consumer's genetic data, processing of biometric information for the purpose of uniquely identifying a consumer, Information collected and analyzed concerning a consumers health, sex life and sexual orientation			
Protected Personal Characteristics	Age (40 years or older), race, color, ancestry, sex, gender identity, sexual orientation, national origin, marital status, veteran or military status, medical information (including medial conditions, disabilities), and similar identifiers	Yes	1-4, 6-7, 9-11, 13-15	A-D, F-J
Profession and Employment Related Information (job applicants)	Employment history, job title(s), work descriptions, locations, dates worked, performance evaluations, and similar information	Yes	9	A-D, F-J
Education Information (non-public)	Institution name, degree, GPA, years attended, professional certifications, visa sponsorship and similar information	No		
Internet and Other Electronic Identifiers	Unique user ID, browsing history, cookie data, IP address, unique device information, session logs, analytics logs, geolocation data, and similar identifiers	Yes	1-2, 5-10, 12-15	A, C-D, F-J
Inference Information	Profile reflecting preferences, characteristics or predispositions, product and service interests, order histories, search histories and similar information	Yes	1, 3-4, 6-7, 10, 14-15	A, C-D, F, I-J
Biometric Information	Iris, finger, facial scan, or voice used in the creation of identification templates for	No		

	time products and voice assistance services			
Geolocation Data	Physical location, Device coordinates/location, or movements	Yes	1-2, 4,7-8, 14-15	A-C, G-J
Sensory Information	Images, visual, thermal, olfactory information, audio or video recordings related to the services	Yes	1,2, 4-8, 10, 12-15	A-C, G-J

California Consumer Rights under the CPRA:

As a California resident, you have rights regarding your Personal Data. Those rights and other state-specific information is described below:

- **Right to Inquire and Access.** You have to ask if we have collected Personal Data about you and to request that we disclose that Personal Data to you at no charge, twice in a 12-month period. You also have a right to request additional information about our collection, use, disclosure, or sale of such Personal Data, which is also provided in this Notice.
- **Right to Correction.** You have the right to request that we correct inaccurate Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Delete.** You have the right to request that we delete your Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Opt-Out of the Selling or Sharing of your Data, or Use of Automated Decision-Making Technology that uses Personal Data for Profiling.** You have the right to opt out of the selling or sharing of your Personal Data. The CPRA requires us to describe the categories of Personal Data we sell or share to third parties and how to opt-out of future sales. The CPRA definition of “sale” and “share” is very broad and the common flow of information for advertising and analytics may be considered a sale or sharing. Under the CPRA, Personal Data includes unique identifiers, including things like IP addresses, cookie IDs, pixel tags, and mobile ad IDs. The law defines a “sale” broadly to include simply making such Personal Data available to third parties in some cases. “Share” is defined as providing Personal Data to a third party to target advertising to a consumer based on information about their activity on multiple websites across the internet. We do not knowingly receive monetary compensation for the sale or sharing of information to third parties; however, in the last 12 months, when you access our Services, we may let advertising and analytics providers collect IP addresses, cookie IDs, advertising IDs, and other unique identifiers, which may be collected along with device and usage data, and information about your interactions with our Services and advertisements.
- **Right to Limit Use or Disclosure of Sensitive Personal Data.** You have the right to limit our use or disclosure of Sensitive Personal Data to the following purposes (and direct our

service providers, contractors, and third parties, and their business partners to do the same):

- To provide you with the services or goods you requested;
- To ensure security and integrity of your information;
- To prevent, detect, and investigate security incidents that affect your information;
- To avoid illegal actions against us and prosecute responsible parties;
- To ensure the physical safety of persons;
- To advertise to you during your visit to the websites linking to this Policy and other short-term uses, where your information is not disclosed to a third party or used to affect your web experience or build a consumer profile;
- To collect or process Sensitive Personal Data for purposes other than inferring characteristics about you;
- To maintain/service accounts, provide customer service, process payments, provide analytics, complete transactions, and perform other services on our behalf; or
- To verify and maintain the quality or safety of, or to improve, a product or service.

Once we receive and process your request, we will stop using and disclosing your Personal Data for purposes other than those listed above (and direct our service providers, contractors, and third parties, and their business partners to do the same).

- **Right to Non-Discrimination.** You have the right not to be discriminated against for exercising any of your privacy rights.

How to Exercise Your Privacy Rights:

California Consumers or their 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.

Appeal. You have the right to appeal our decision to refuse to act on a CPRA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to privacy@ouro.com for our Privacy Team to review your data subject request. Within 45 days, we will provide you with a written explanation of the justification for declining to act on your request. If you disagree with our explanation, you have the right to file a complaint with the State’s Attorney General [HERE](#).

Data Retention. We retain personal data for as long as necessary to provide the Services and fulfill the transactions you have requested, 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 user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

Notice of Financial Incentives. We may offer rewards or prizes for participation in certain activities that may be considered a “financial incentive”. These activities may involve the collection of Personal Data. The categories of Personal Data we collect are limited to what information you provide us, but may include: identifiers, protected class/demographic information, commercial information, online activities, geolocation information (general and precise), sensory information, employment information, and inferences. Activities we engage in that may be considered as a financial incentive include surveys where we may provide compensation such as a gift card in exchange for your time and responses, or a prize through your participation in promotions and sweepstakes. Participation in these programs may be subject to separate terms and conditions. Your participation in these programs is voluntary and you can terminate at any time as explained in any applicable terms. When we offer gift cards in exchange for your participation in a survey or when we engage in promotions or sweepstakes, the amount provided is reasonably related to the value of the data you provide, which takes into account a number of factors, including, the anticipated benefit we receive such as product improvement, better understanding how you use our products, to enhance our understanding of consumer and market trends, increased consumer engagement, and the anticipated expenses we incur in relation to the collection, storage, and use of the information we receive. The value may vary across surveys, promotions, and sweepstakes.

Where we offer you a financial incentive for providing your Personal Data, our accompanying disclosure will provide:

- A succinct summary of the financial incentive or price or service difference offered;

- A description of the material terms of the financial incentive or price or service difference, including the categories of Personal Data that are implicated by the financial incentive or price or service difference and the value of your Personal Data;
- How the consumer can opt-in to the financial incentive or price or service difference;
- A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- An explanation of how the financial incentive or price or service difference is reasonably related to the value of your Personal Data.

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.

Contact Information. If you have any comments, concerns, or questions about this Privacy Policy, please contact us at privacy@ouro.com.

For Minnesota Residents

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

The Minnesota Consumer Data Protection Act ("MCDPA" or "Minnesota Privacy Law") provides consumers residing in that state ("Minnesota Consumers", "you", or "your") with specific rights regarding their Personal Data. This notice ("MCDPA Privacy Notice") supplements the information contained in the [Ouro U.S. Privacy Policy](#) ("Ouro Privacy Policy") and explains how Ouro, and our subsidiaries and affiliates, ("Ouro," "we," "us," or "our") collect, use, disclose and retain Personal Data and how Minnesota Consumers may exercise their rights under the MCDPA.

Except for those terms defined within this MCDPA Privacy Notice, all other capitalized terms shall have the same meaning as those designated in the Ouro Privacy Policy.

Information We Collect:

Under the MCDPA, Personal Data means any information that can be linked to a particular natural person. "Personal data" does not include de-identified data or publicly available information.

Minnesota Privacy Law defines "Sensitive Personal Data" as a subset of Personal Data that (1) reveals racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; (2) contains biometric data or genetic information for the purpose of uniquely identifying an individual; (3) the personal data of a known child; or (4) specific geolocation data.

Minnesota Consumer Rights under the MCDPA:

If you are a Minnesota resident, you have rights regarding your Personal Data. Those rights and other state-specific information is described below:

- **Right to Inquire and Access.** You have to ask if we have collected Personal Data about you and to request that we disclose that Personal Data to you at no charge, once in a 12-month period. You also have a right to request additional information about our collection, use, disclosure, or sale of such Personal Data, which is also provided in this Notice.
- **Right to Correct.** You have the right to request that we correct inaccurate Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Delete.** You also have the right to request that we delete your Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Opt-Out of the Selling of your Data, Targeted Advertising, or Use of Automated Decision-Making Technology that uses Personal Data for Profiling.** You have the right to opt out of the sale of your Personal Data, targeted advertising and processing Personal Data for purposes of profiling. When permitted, we limit the use of profiling for marketing purposes only. Personal Data may include unique identifiers, including things like IP addresses, cookie IDs, pixel tags, and mobile ad IDs. When you access our Services, we may let advertising and analytics providers collect IP addresses, cookie IDs, advertising IDs, and other unique identifiers, which may be collected along with device and usage data, and information about your interactions with our Services and advertisements. We do not knowingly receive monetary compensation for the sale of information to third parties.
- **Right to Data Portability.** You have the right to obtain a portable copy of your Personal Data. To obtain a copy of your Personal Data that you previously provided to us in a portable format, please submit an “Access” request as described above. While these requests are distinct, we have not identified any technically feasible and readily usable format that would allow you to transmit this data to another controller. Therefore, we will provide you a copy of your Personal Data so that we honor your request as best as is technically feasible.
- **Right to Request.** You have the request a list of the specific third parties to which we have disclosed your Personal Data.
- **Right to Non-Discrimination.** You have the right not to be discriminated against for exercising any of your privacy rights.

How to Exercise Your Privacy Rights:

Minnesota Consumers or their 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.

Appeal. You have the right to appeal our decision to refuse to act on a MCDPA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to privacy@ouro.com for our Privacy Team to review your data subject request. Within 45 days, we will provide you with a written explanation of the justification for declining to act on your request or, if circumstances dictate, an additional 60 days' extension. If you disagree with our explanation, you have the right to file a complaint with the State's Attorney General [HERE](#).

Miscellaneous:

Data Retention. We retain personal data for as long as necessary to provide the Services and fulfill the transactions you have requested, 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 user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

Notice of Financial Incentives. We may offer rewards or prizes for participation in certain activities that may be considered a "financial incentive". These activities may involve the collection of Personal Data. The categories of Personal Data we collect are limited to what information you provide us, but may include: identifiers, protected class/demographic information, commercial information, online activities, geolocation information (general and precise), sensory information, employment information, and inferences. Activities we engage in that may be considered as a financial incentive include surveys where we may provide compensation such as a gift card in exchange for your time and responses, or a prize through your participation in promotions and sweepstakes. Participation in these programs may be subject to separate terms and conditions. Your participation in these programs is voluntary and you can terminate at any time as explained in any applicable terms. When we offer gift cards in exchange for your participation in a survey or

when we engage in promotions or sweepstakes, the amount provided is reasonably related to the value of the data you provide, which takes into account a number of factors, including, the anticipated benefit we receive such as product improvement, better understanding how you use our products, to enhance our understanding of consumer and market trends, increased consumer engagement, and the anticipated expenses we incur in relation to the collection, storage, and use of the information we receive. The value may vary across surveys, promotions, and sweepstakes.

Where we offer you a financial incentive for providing your Personal Data, our accompanying disclosure will provide:

1. A succinct summary of the financial incentive or price or service difference offered;
2. A description of the material terms of the financial incentive or price or service difference, including the categories of Personal Data that are implicated by the financial incentive or price or service difference and the value of your Personal Data;
3. How the consumer can opt-in to the financial incentive or price or service difference;
4. A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
5. An explanation of how the financial incentive or price or service difference is reasonably related to the value of your Personal Data.

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.

Contact Information. If you have any comments, concerns, or questions about this Privacy Policy, please contact us at privacy@ouro.com.

For Oregon Residents

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

The Oregon Consumer Privacy Act ("OCPA" or "Oregon Privacy Law") provides consumers residing in that state ("Oregon Consumers", "you", or "your") with specific rights regarding their Personal Data. This notice ("OCPA Privacy Notice") supplements the information contained in the [Ouro U.S. Privacy Policy](#) ("Ouro Privacy Policy") and explains how Ouro, and our subsidiaries and affiliates, ("Ouro," "we," "us," or "our") collect, use, disclose and retain Personal Data and how Oregon Consumers may exercise their rights under the OCPA.

Except for those terms defined within this OCPA Privacy Notice, all other capitalized terms shall have the same meaning as those designated in the Ouro Privacy Policy.

Information We Collect:

Under the OCPA, “Personal Data” means data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household. “Personal Data” does not include deidentified data or data that is lawfully available through federal, state or local government records or through widely distributed media; or a controller reasonably has understood to have been lawfully made available to the public by a consumer.

Under the OCPA, Sensitive Personal Data is information revealing racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or nonbinary, status as a victim of crime or citizenship or immigration status; is a child’s personal data; accurately identifies within a radius of 1,750 feet a consumer’s present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates; or is genetic or biometric data.

How to Exercise Your Privacy Rights:

Oregon Consumers or their 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.

Appeal. You have the right to appeal our decision to refuse to act on a CPRA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to privacy@ouro.com for our Privacy Team to review your data subject request. Within 45 days, we will provide you with a written explanation of the justification for declining to act on your request. If you disagree with our explanation, you have the right to file a complaint with the State’s Attorney General [HERE](#).

Miscellaneous:

Data Retention. We retain personal data for as long as necessary to provide the Services and fulfill the transactions you have requested, 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 user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

Notice of Financial Incentives. We may offer rewards or prizes for participation in certain activities that may be considered a “financial incentive”. These activities may involve the collection of Personal Data. The categories of Personal Data we collect are limited to what information you provide us, but may include: identifiers, protected class/demographic information, commercial information, online activities, geolocation information (general and precise), sensory information, employment information, and inferences. Activities we engage in that may be considered as a financial incentive include surveys where we may provide compensation such as a gift card in exchange for your time and responses, or a prize through your participation in promotions and sweepstakes. Participation in these programs may be subject to separate terms and conditions. Your participation in these programs is voluntary and you can terminate at any time as explained in any applicable terms. When we offer gift cards in exchange for your participation in a survey or when we engage in promotions or sweepstakes, the amount provided is reasonably related to the value of the data you provide, which takes into account a number of factors, including, the anticipated benefit we receive such as product improvement, better understanding how you use our products, to enhance our understanding of consumer and market trends, increased consumer engagement, and the anticipated expenses we incur in relation to the collection, storage, and use of the information we receive. The value may vary across surveys, promotions, and sweepstakes.

Where we offer you a financial incentive for providing your Personal Data, our accompanying disclosure will provide:

1. A succinct summary of the financial incentive or price or service difference offered;
2. A description of the material terms of the financial incentive or price or service difference, including the categories of Personal Data that are implicated by the financial incentive or price or service difference and the value of your Personal Data;
3. How the consumer can opt-in to the financial incentive or price or service difference;

4. A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
5. An explanation of how the financial incentive or price or service difference is reasonably related to the value of your Personal Data.

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.

Contact Information. If you have any comments, concerns, or questions about this Privacy Policy, please contact us at privacy@ouro.com.