

## **PRIVACY POLICY**

Last Updated on April 21, 2025

This PRIVACY POLICY is effective as of April 21, 2025 (the “Policy”).

The Policy describes our policies on the collection, use, and disclosure of information about you in connection with your use of our services, including those offered through our websites, emails, and mobile applications (collectively, the "Service"). The terms "we", "us", "our" and "Influenergy" refer to Influenergy LLC. When you use the Service, you consent to our collection, use, and disclosure of information about you as described in this Policy.

1. **INFORMATION WE COLLECT AND HOW WE USE IT:** We may collect and store information about you in connection with your use of the Service, including any information you transmit to or through the Service. We use that information to provide the Service’s functionality, fulfill your requests, improve the Service’s quality, engage in research and analysis relating to the Service, personalize your experience, track usage of the Service, market the Service, provide customer support, message you, back up our systems, allow for disaster recovery, enhance the security of the Service, and comply with legal obligations. Even when we do not retain such information, it still must be transmitted to our servers initially and stored long enough to process. Additionally:
  - **Account Information:** If you create an account with Influenergy, we may store and use the information you provide during that process, such as your full name, email address, zip code, physical address, social media handles and other information you may provide with your account, such as your gender, phone number, and birth date. You can modify some of the information associated with your account through the applicable product’s account settings.
  - **Communications:** When you sign up for an account or use certain features, you are opting to receive messages from other users, businesses, and Influenergy. You can manage some of your notification preferences through the Service, but note that you cannot opt out of receiving certain administrative, transactional, or legal messages from Influenergy. We may also store information that you provide through communications to us, including from phone calls, emails and other electronic messages, or through the Service. Our calls with you may be monitored and recorded for quality purposes.
  - **Transactions:** If you initiate a transaction through the Service, such as a purchase, we may collect and store information about you, such as your name, phone number, address and email, as well as any other information you provide to us, in order to process your transaction, send communications about them to you, and populate forms for future transactions. Notwithstanding the foregoing, Influenergy does not collect or store your credit card information as part of any transaction. Any payment information, excluding your name and contact details, provided by you is not stored by us.
  - **Activity:** We may store information about your use of the Service, such as your search activity, the pages you view and the date and time of your visit. We also may store information that your computer or mobile device may provide to us in connection with your use of the Service, such as your browser type, type of computer or mobile device, browser language, IP address, WiFi information such as SSID, mobile carrier, phone number, unique device identifier, advertising identifier, location (including geolocation, beacon based location, and GPS location), and requested and referring URLs. We may also receive and store your location whenever our mobile applications are running, including

when running in the background, if you enable our mobile apps to access such information in the course of using the Service. You may be able to limit or disallow our use of certain location data through your device or browser settings, for example by adjusting the "Location Services" settings for our applications in iOS privacy settings.

- Different Devices: You may access the Service through different devices (e.g., your mobile phone or desktop computer) and different platforms (e.g., the Influenenergy website or Influenenergy mobile app). The information that we collect and store through those different uses may be cross-referenced and combined, and your contributions through one Influenenergy platform will typically be similarly visible and accessible through all other Influenenergy platforms.
2. Cookies: We, and third parties with whom we partner, may use cookies, web beacons, tags, scripts, local shared objects such as HTML5, advertising identifiers (including mobile identifiers such as Apple's IDFA or Google's Advertising ID) and similar technology ("Cookies") in connection with your use of the Service, third party websites, and mobile applications. Cookies may have unique identifiers, and reside, among other places, on your computer or mobile device, in emails we send to you, and on our web pages. Cookies may transmit information about you and your use of the Service, such as your browser type, search preferences, IP address, data relating to advertisements that have been displayed to you or that you have clicked on, and the date and time of your use. Cookies may be persistent or stored only during an individual session. You can set some Cookie preferences through your device or browser settings, but doing so may affect the functionality of the Service. The method for disabling Cookies may vary by device and browser, but can usually be found in your device or browser preferences or security settings. For example, iOS and Android devices each have settings which are designed to limit forms of ad tracking. Please note that changing any of these settings does not prevent the display of certain advertisements to you. The purposes for which we use Cookies in the Service include:
- Processes. Intended to make the Service work in the way you expect. For example, we use a Cookie that tells us whether you have already signed up for an account.
  - Authentication, Security, and Compliance. Intended to prevent fraud, protect your data from unauthorized parties, and comply with legal requirements. For example, we use Cookies to determine if you are logged in.
  - Preferences. Intended to remember information about how you prefer the Service to behave and look. For example, we use a Cookie that tells us whether you have declined to allow us to send push notifications to your phone.
  - Notifications. Intended to allow or prevent notices of information or options that we think could improve your use of the Service. For example, we use a Cookie that stops us from showing you the signup notification if you have already seen it.
  - Analytics. Intended to help us understand how visitors use the Service. For example, we use a Cookie that tells us how our search suggestions correlate to your interactions with the search page.
3. Third Parties: Third parties may receive information about you as follows:
- Service Providers: We may rely on third party providers to support or provide some of the services that are available through the Service. We may also rely on third party providers to perform certain services for us in connection with your use of the Service, such as communications and hosting services, network security, technical and customer support, tracking and reporting functions, quality assurance testing, payment processing, our own marketing of the Service, and other functions. We may share information from or about you with these third-party providers so that they can perform their services or complete your requests. These third-party providers may share information with us that they obtain from or about you in connection with providing their services or completing your requests.

Third party providers may also share this information with their subsidiaries, joint ventures, or other companies under common control.

- Aggregate or Anonymous Information: We may share user information in the aggregate with third parties, such as data analytics, engagement rates and other information related to the Service. We may also disclose anonymized information about your use of the Service.
  - Business Transfers: We may share information from or about you with our parent companies, subsidiaries, joint ventures, or other companies under common control, in which case we will require them to honor this Policy. If another company acquires Influenery, or all or substantially all of our assets, that company will possess the same information, and will assume the rights and obligations with respect to that information as described in this Policy.
  - Investigations and Legal Disclosures: We may investigate and disclose information from or about you if we have a good faith belief that such investigation or disclosure: (a) is reasonably necessary to comply with legal process and law enforcement instructions and orders, such as a search warrant, subpoena, statute, judicial proceeding, or other legal process or law enforcement requests served on us; (b) is helpful to prevent, investigate, or identify possible wrongdoing in connection with the Service; or (c) protects our rights, reputation, property, or that of our users, affiliates, or the public.
  - Links: The Service may link to third party services, such as Facebook, YouTube and Instagram. Except as set forth herein, we do not share your personal information with them, and are not responsible for their privacy practices. We suggest you read the privacy policies on or applicable to all such third-party services.
  - Third Party Accounts: If you sign up for, or log into, Influenery using a third-party service like Facebook or Google, or link your Influenery account to your account with a third-party service like Facebook or Twitter, we may receive information about you from such third-party service.
4. **Controlling Your Personal Data:** Please note that the messages you send or receive using the Service are only private to the extent that both you and the person you are communicating with keep them private. Also, we may access and disclose such messages in the course of investigations relating to use of the Service.
5. **Mediation:** If you are a resident of a country outside of the European Union, you also agree that, in the event any dispute or claim arises out of or relating to this Policy that you and Influenery will attempt in good faith to negotiate a written resolution of the matter directly between the parties. You agree that if the matter remains unresolved for forty-five (45) days after notification (via certified mail or personal delivery) that a dispute exists, all parties shall join in mediation services in Clark County, Nevada with a mutually agreed mediator in an attempt to resolve the dispute. Should you file any arbitration claims, or any administrative or legal actions without first having attempted to resolve the matter by mediation, then you agree that you will not be entitled to recover attorneys' fees, even if you would otherwise be entitled to them.
6. **Users Outside Of The United States:** Our site is hosted in the United States. If you are a user accessing our site from the European Union or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that your personal data will be processed outside of the European Economic Area (the "EEA"). We will take all steps necessary to ensure that your information is adequately protected and processed in accordance with this Policy. You consent to such cross-border transfers of your information. Please contact us using the contact details set out in Section 11 if you want further information.
7. **Your Rights:**
- You have certain rights in respect of the information that we hold about you, including:

- the right to ask us not to process your personal data for marketing purposes;
  - the right to request access to the information that we hold about you;
  - in certain circumstances, the right to object to processing, i.e. to ask us to stop processing information about you; and
  - the right to lodge a complaint about us to the UK Information Commissioner's Office [LINK: [HTTPS://ICO.ORG.UK](https://ico.org.uk)]. You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances. We will try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. Please note that we may need to retain certain information for our own record-keeping and research purposes. We may also need to send you service-related communications relating to your website user account even when you have requested not to receive marketing communications.
- Additional Rights Under GDPR: In accordance with new data protection laws which will be in force from that date, you may have certain additional rights in respect of the information that we hold about you, including:
    - the right to lodge a complaint about us to the UK Information Commissioner's Office [LINK: [HTTPS://ICO.ORG.UK](https://ico.org.uk)] or the relevant authority in your country of work or residence;
    - the right to withdraw your consent for our use of your information in reliance of your consent, which you can do by contacting us using the details set out in Section 11;
    - the right to object to our using your information on the basis of our legitimate interests; and
    - the right to receive a copy of any information we hold about you in connection with the performance of our contract with you or on the basis of your consent (or request that we transfer this to another service provider) in a structured, commonly-used, machine readable format; and
    - the right to ask us to limit or cease processing or erase information we hold about you in certain circumstances.
  - How Can I Exercise My Rights?: You may exercise your rights above by contacting us using the details set out in Section 11 or by using the unsubscribe option available on email communication you receive from us. We will comply with your requests unless we have a lawful reason not to do so.
8. Data Retention And Account Termination: You can close your account by contacting us as provided in Section 11. We will remove certain account information, but we may retain information about you for the purposes authorized under this Policy unless prohibited by law. For example, we may retain information to prevent, investigate, or identify possible wrongdoing in connection with the Service or to comply with legal obligations.
9. Children: The Service is intended for general audiences and is not directed to children under 13.

We do not knowingly collect personal information from children under 13. If you become aware that a child has provided us with personal information without parental consent, please contact us on the address listed in Section 11. If we become aware that a child under 13 has provided us with personal information without parental consent, we take steps to remove such information and terminate the child's account.

10. Security: We use various safeguards to protect the personal information submitted to us, both during transmission and once we receive it. However, no method of transmission over the Internet or via mobile device, or method of electronic storage, is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your personal information, we cannot guarantee its absolute security.
11. Contact Us: If you have any questions or concerns regarding this Policy or the Service, please feel free to contact us at the following email: [connect@influenergy.co](mailto:connect@influenergy.co)
12. Modifications To This Policy: We may revise this Policy from time to time. The most current version of the Policy will govern our collection, use, and disclosure of information about you. If we make material changes to this Policy, we will notify you by email or by posting a notice on the Service prior to the effective date of the changes. By continuing to access or use the Service after those changes become effective, you acknowledge the revised Policy.

Nevada, California, Virginia, Connecticut, Colorado, Utah, Texas, Oregon, Florida and Montana Residents: If you are a Nevada, California, Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Florida or Montana resident, please see below for additional rights you may have under your state's laws relating to your personal data.

## ADDITIONAL STATE PRIVACY LAWS

### Nevada Residents

Under Nevada law, certain Nevada consumers may opt out of the sale of “covered information” for monetary consideration to a person for that person to license or sell such information to additional persons. “Covered information” includes first and last name, address, email address, phone number, Social Security Number, or an identifier that allows a specific person to be contacted either physically or online. We do not engage in such activity; however, if you are a Nevada resident who has purchased services from or performed services for us, you may submit a request to opt out of any potential future sales under Nevada law by emailing us at [connect@influenergy.co](mailto:connect@influenergy.co). Please note we will take reasonable steps to verify your identity and the authenticity of the request. Once verified, we will maintain your request in the event our practices change.

If you have additional questions about the supplement or how to exercise your rights under the supplement, please contact us as specified in Section 11.

### California Residents

If you are a California resident, the processing of certain personal data about you may be subject to the California Consumer Privacy Act of 2018, California Civil Code Sections 1798.100-1798.199 (“CCPA”), California Privacy Rights Act of 2020 (“CPRA”) and other applicable California state privacy laws.

Beginning January 1, 2020, the CCPA gives you certain rights with respect to the processing of your personal data (known as “personal information”, as described under the CCPA). Beginning January 1, 2023, the CPRA amends CCPA and gives you certain rights with respect to the processing of your personal information as described under the CPRA.

This supplement provides additional privacy disclosures and informs you of your additional rights as a California resident, and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

## Consumer Rights under CCPA and CPRA

- **Right to Request Disclosure of Personal Information Collected (Right of Access).** A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected. (CCPA 1798.100(a), 1798.110(c)(5) and 1798.130(a)(5)(A)) (CPRA)
- **Right of Rectification.** The right for a consumer to request that the incorrect or outdated personal information be corrected but not deleted. (CPRA)
- **Right to Request Deletion.** A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer unless exceptions apply. (CCPA 1798.105(a))(CPRA)
- **Right of Restriction.** The right for a consumer to restrict a business's ability to process personal information (i.e., sensitive information that reveals an individual's government ID, finances, geolocation, race, religion, and union membership, consumer's private communications, genetics, biometrics, consumer's health, sexual orientation ) about the consumer. (CPRA)
- **Right to Request Disclosure of Personal Information Collected, Sources, Purposes for Collection or Sale and Third Parties with whom Shared (Right of Access).** A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
  - The categories of personal information it has collected about that consumer in the preceding 12 months.
  - The categories of sources from which the personal information is collected.
  - The business or commercial purpose for collecting or selling personal information.
  - The categories of third parties with whom the business shares personal information.
  - The specific pieces of personal information it has collected about that consumer.

(CCPA 1798.110(a)-(b) and 1798.130(a)(3))(CPRA)

- **Right to Request Disclosure of Personal Information Collected, Sold and Disclosed and Third Parties to whom Sold (Right of Access).** A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:
  - The categories of personal information that the business collected about the consumer.
  - The categories of personal information that the business sold about the consumer in the preceding 12 months and the categories of third parties to whom the personal information was sold in the



preceding 12 months, by category or categories of personal information for each category of third parties to whom the personal information was sold.

- The categories of personal information that the business disclosed about the consumer for a business purpose in the preceding 12 months.

(CCPA 1798.115(a)-(b) and 1798.130(a)(4))(CPRA)

- Right of Portability. The right for a consumer to request personal information about the consumer be disclosed in a common file format. (CCPA, CPRA)
- Right to opt-out of sales. The right for a consumer to opt out of the sale of personal information about the consumer to third parties. (CCPA, CPRA)
- Right Against Automated Decision making. A prohibition against a business making decisions about a consumer based solely on an automated process without human input. (CPRA)
- Private Right of Action. The right for a consumer to seek civil damages from a business for certain violations of the statute.

Business Obligations under CCPA and CPRA

- Opt-In Default (Requirement Age). A restriction placed on a business to treat consumers under a certain age (here, age 16) with an opt-in default for the sale of their personal information. (CCPA, CPRA)
- Notice/Transparency Requirement. An obligation placed on a business to provide notice to consumers about certain data practices, privacy obligations and/or privacy programs. (CCPA, CPRA).
- Risk Assessments. An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects and or procedures (CPRA)
- Prohibition on Discrimination (Exercising Rights)/Right of Non-Discrimination. A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:
  - Denying goods or services to the consumer.
  - Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
  - Providing a different level or quality of goods or services to the consumer.
  - Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(CCPA 1798.125(a))(CPRA)

- Purpose/Process Limitation. Prohibits the collecting/processing of personal information except for a specific purpose (CCPA, CPRA)

To exercise your “right to know,” your “right to request deletion,” or any other right under the CCPA and

CPRA, contact us as specified in Section 11.

Please note that to protect your information and the integrity of our Service, we may need to verify your identity before processing your request. In some cases we may need to collect additional information to verify your identity, such as a government issued ID.

Under the CCPA, you may exercise these rights yourself or you may designate an authorized agent to make these requests on your behalf. We may request that your authorized agent have written permission from you to make requests on your behalf and may need to verify your authorized agent's identity.

If you have additional questions about the supplement or how to exercise your rights under the supplement, please contact us as specified in Section 11.

## Virginia Residents

If you are a Virginia resident, the processing of certain personal data about you may be subject to the Virginia Consumer Data Protection Act of 2021, Chapter 53 Section 59.1-575 ("VCDPA") and other applicable Virginia state privacy laws. Beginning January 1, 2023, the VCDPA gives you certain rights with respect to the processing of your personal data.

This supplement provides additional privacy disclosures and informs you of your additional rights as a Virginia resident, and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

## Consumer Rights under VCDPA

- **Right of Access.** A consumer shall have the right to confirm whether a controller is processing the consumer's personal data, the categories of personal data, the categories of personal data shared with third parties and with whom by category, the purpose for processing such personal data and to access such personal data.
- **Right of Rectification.** The right for a consumer to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.
- **Right of Deletion.** A consumer shall have the right to request to delete personal data provided by or obtained about the consumer.
- **Right of Restriction.** Obtain consumer consent before processing sensitive data, or, with regards to known children, process such data in accordance with the federal Children's Online Privacy Protection Act. Sensitive data includes genetic data, biometric data, mental health diagnoses, physical health diagnoses, citizenship status, immigration status, and personal data collected from a known child.
- **Right of Portability.** The consumer has a right to obtain a copy of the consumer's personal data



that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

- Right to Opt-Out. The right for a consumer to opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

To exercise your “right to know,” your “right to request deletion,” or any other right under the VCDPA, contact us as specified in Section 11.

In addition, except as otherwise provided under VCDPA, we shall comply with a request by a consumer to exercise the consumer rights authorized as follows:

- We shall respond to you without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described here. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of your requests, so long as we inform you of any such extension within the initial 45-day response period, together with the reason for the extension.
- If we decline to take action regarding your request, we shall inform you without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.
- Information provided in response to your request shall be provided by us to you free of charge, up to twice annually. If requests from you are manifestly unfounded, excessive, or repetitive, we may charge you a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. We bear the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.
- If we are unable to authenticate the request using commercially reasonable efforts, we shall not be required to comply with a request to initiate an action under here and may request that you provide additional information reasonably necessary to authenticate you and your request.
- Where we have obtained personal data about you from a source other than from you, we shall be deemed in compliance with your request to delete such data pursuant by either (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring your personal data remains deleted from our records and not using such retained data for any other purpose or (ii) opting you out of the processing of such personal data for any purpose except for those exempted.
- We have established a process for your appeal to our refusal to take action on a request within a reasonable period of time after your receipt of our decision. The appeal process is similar to the process for submitting requests to initiate action pursuant to above. You may appeal our refusal to take action on a request after receipt of our decision by submitting a request to us specifying you would like to appeal our decision. Your parent or legal guardian may invoke your rights on behalf of you regarding the appeal. Within 60 days of receipt of an appeal, we shall inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, we shall also provide you with an online mechanism, if available, or other method through which you may contact the Attorney General to submit a complaint.

Please note that to protect your information and the integrity of our Service, we may need to verify your identity before processing your request. In some cases we may need to collect additional information to verify your identity, such as a government issued ID.

Under the VCDPA, you may exercise these rights yourself or you may designate an authorized agent to make these requests on your behalf. We may request that your authorized agent have written permission from you to make requests on your behalf and may need to verify your authorized agent's identity.

If you have additional questions about the supplement or how to exercise your rights under the supplement, please contact us as specified in Section 11.

## Colorado Residents

If you are a Colorado resident, the processing of certain personal data about you may be subject to the Senate Bill 21-190, Article 1-Title 6-Part 13 (the "CPA"). Beginning July 1, 2023, the Colorado Privacy Act gives you certain rights with respect to the processing of your personal data.

This supplement provides additional privacy disclosures and informs you of your additional rights as a Colorado resident and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

### Consumer Rights under the CPA:

- Right to Access
- Right to Correct
- Right to Delete Personal Data
- Right to Opt-Out of targeted advertising, the Sale of Personal Data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

### CPA 6-1-1306 (a)

- Right to Opt-Out of the Collection and Use of Personal Data

### Business Obligations under the Colorado Privacy Act:

- To safeguard personal data
- To provide clear understandable and transparent information to consumers about how their personal data is used

- To strengthen compliance and accountability by requiring data protection assessments in the collection and use of personal data

To exercise your rights, contact us as specified in Section 11.

Please note to protect your information and the integrity of our Service, we may need to verify your identity before processing your request. In some cases, we may need to collect additional information to verify your identity such as a government issued ID.

Under the Colorado Privacy Act, you may exercise these rights yourself or you may designate an authorized agent to make these requests on your behalf. We may request that your authorized agent have written permission from you to make requests on your behalf and may need to verify your authorized agent's identity.

If you have additional questions about the supplement or how to exercise your rights under the supplement, please contact us as specified in Section 11.

#### Connecticut Residents

If you are a Connecticut, the processing of certain personal data about you may be subject to the Connecticut Data Privacy Act, Public Act No. 22-15 (the "CTDPA"). Beginning July 1, 2023, the CTDPA gives you certain rights with respect to the processing of your personal data.

This supplement provides additional privacy disclosures and informs you of your additional rights as a Connecticut resident and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

#### Consumer Rights under the CTDPA:

- Right to Access personal data that a business has collected about them. Right to obtain a copy of their personal data in a portable and readily usable format that allows them to transfer the data to another controller with ease. A consumer can request information from a controller free once every twelve (12) months. Under certain circumstances beyond the annual request, the controller may charge an administrative fee.
- Right to Correct inaccuracies in their personal data
- Right to Delete their personal data, including data that a business collected through third parties
- Right to Opt-Out of sale of their personal data, the processing of personal data for the purposes of targeted advertising, and profiling that may have a legal or other significant impact.

Business Obligations under the CTDPA include:

- To provide and maintain a privacy notice that clearly describes:
  - The purpose(s) for processing the personal data, and whether and why the controller shares personal data with third parties, and
  - How consumers may exercise their rights under the CTDPA. [Among other methods, a controller must provide an easily accessible link on its website through which consumers can opt-out of targeted advertising or the sale of their personal data. Soon, consumers will also be able to opt-out through universal opt-out mechanisms.]
- To protect the personal data of children and teens. To permit a child's parent or legal guardian to exercise privacy rights on the child's behalf. To obtain opt-in consent before selling the personal data of a consumer under sixteen (16) years old or sending the consumer target ads. Controllers must follow all regulations concerning children's online privacy established pursuant to the Children's Online Privacy Protection Act ("COPPA"), including parental consent requirements.
- To conduct assessments before processing personal data in a manner that presents a heightened risk of harm to consumers (called "Data Protection Assessments"). This includes processing personal data for the purposes of targeted advertising, sale, or profiling, and processing sensitive data.
- To obtain consent before processing a consumer's sensitive data. Sensitive data is a subset of personal data that includes:
- Any data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual activity or orientation, citizenship, or immigration status;
- Genetic or biometric data used to uniquely identify an individual;
- Personal data of a child under the age of thirteen (13); and
- Information that identifies an individual's specific location with a defined degree of precision and accuracy (called "precise geolocation data").

To exercise your rights, contact us as specified in Section 11.

Please note to protect your information and the integrity of our Service, we may need to verify your identity before processing your request. In some cases, we may need to collect additional information to verify your identity such as a government issued ID.

Under the CTDPA, you may exercise these rights yourself or you may designate an authorized agent to make these requests on your behalf. We may request that your authorized agent have written permission from you to make requests on your behalf and may need to verify your authorized agent's identity.

If you have additional questions about the supplement or how to exercise your rights under the supplement, please contact us as specified in Section 11.

Utah Residents

Beginning December 31, 2023, the Utah Consumer Privacy Act gives you certain rights with respect to the processing of your personal data.

This supplement provides additional privacy disclosures and informs you of your additional rights as a Utah resident and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

Consumer Rights under the Utah Consumer Privacy Act:

Consumer Rights -- Access -- Deletion -- Portability -- Opt Out of Certain Processing:

(1) A consumer has the right to:

- (a) confirm whether a controller is processing the consumer's personal data; and
- (b) access the consumer's personal data.

(2) A consumer has the right to delete the consumer's personal data that the consumer provided to the controller.

(3) A consumer has the right to obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that:

- (a) to the extent technically feasible, is portable;
- (b) to the extent practicable, is readily usable; and
- (c) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.

(4) A consumer has the right to opt out of the processing of the consumer's personal data for purposes of:

- (a) targeted advertising; or
- (b) the sale of personal data.

(5) Nothing in this section requires a person to cause a breach of the security system as defined in Section 13-44-102 of the Utah Consumer Privacy Act.

#### Exercising Consumer Rights:

- (1) A consumer may exercise a right by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise.
- (2) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise a right on the child's behalf.
- (3) In the case of processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under the Utah Uniform Probate Code Title 75, Chapter 5, Protection of Persons Under Disability and Their Property, the guardian or the conservator of the consumer shall exercise a right on the consumer's behalf.

#### Controller's Response to Requests:

- (1) Subject to the other provisions of this chapter, a controller shall comply with a consumer's request under Section 13-61-202 of the Utah Consumer Privacy Act to exercise a right.
- (2)
  - (a) Within 45 days after the day on which a controller receives a request to exercise a right, the controller shall: (i) take action on the consumer's request; and (ii) inform the consumer of any action taken on the consumer's request.
  - (b) The controller may extend once the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller.
  - (c) If a controller extends the initial 45-day period, before the initial 45-day period expires, the controller shall: (i) inform the consumer of the extension, including the length of the extension; and (ii) provide the reasons the extension is reasonably necessary as described in Subsection (2)(b).
  - (d) The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires.
- (3) If, in accordance with this section, a controller chooses not to take action on a consumer's request, the controller shall within 45 days after the day on which the controller receives the request, inform the consumer of the reasons for not taking action.
- (4)



(a) A controller may not charge a fee for information in response to a request, unless the request is the consumer's second or subsequent request during the same 12-month period.

(b) (i) Notwithstanding Subsection (4)(a), a controller may charge a reasonable fee to cover the administrative costs of complying with a request or refuse to act on a request, if:

(A) the request is excessive, repetitive, technically infeasible, or manifestly unfounded;

(B) the controller reasonably believes the primary purpose in submitting the request was something other than exercising a right; or

(C) the request, individually or as part of an organized effort, harasses, disrupts, or imposes undue burden on the resources of the controller's business.

(b) (ii) A controller that charges a fee or refuses to act in accordance with this Subsection (4)(b) bears the burden of demonstrating the request satisfied one or more of the criteria described in Subsection (4)(b)(i).

(5) If a controller is unable to authenticate a consumer request to exercise a right described in Section 13-61-201 of the Utah Consumer Privacy Act using commercially reasonable efforts, the controller: (a) is not required to comply with the request; and (b) may request that the consumer provide additional information reasonably necessary to authenticate the request.

Responsibilities of Controllers -- Notice -- Purpose Specification-- Security:

(1)

(a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(i) the categories of personal data processed by the controller;

(ii) the purposes for which the categories of personal data are processed;

(iii) how consumers may exercise a right;

(iv) the categories of personal data that the controller shares with third parties, if any; and

(v) the categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the:

(i) sale of the consumer's personal data; or

(ii) processing for targeted advertising.

(2)

(a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:

(i) protect the confidentiality and integrity of personal data; and

(ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.

(b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

(3) Except as otherwise provided in the Utah Consumer Privacy Act, a controller may not process sensitive personal data collected from a consumer without:

(a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or

(b) in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. Sec. et seq., and the act's implementing regulations and exemptions.

To exercise your rights, contact us as specified in Section 11.

Please note to protect your information and the integrity of our Service, we may need to verify your identity before processing your request. In some cases, we may need to collect additional information to verify your identity such as a government issued ID.

Under the Utah Consumer Privacy Act, you may exercise these rights yourself or you may designate an authorized agent to make these requests on your behalf. We may request that your authorized agent have written permission from you to make requests on your behalf and may need to verify your authorized agent's identity.

If you have additional questions about the supplement or how to exercise your rights under the supplement, please contact us as specified in Section 11.

## Texas Residents

Beginning July 1, 2024, the Texas Data Privacy and Security Act gives consumers certain rights with respect to the processing of consumer personal data.

This supplement informs on consumer rights as a Texas resident and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

### Consumer Rights under the Texas Data Privacy and Security Act:

- (1) confirm whether a controller is processing the consumer's personal data and to access the personal data;
- (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
- (3) delete personal data provided by or obtained about the consumer;
- (4) if the data is available in a digital format, obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; or
- (5) opt out of the processing of the personal data for purposes of:
  - (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

To exercise consumers' rights, a consumer can contact us as specified in Section 11.

Please note to protect a consumer's information and the integrity of our Service, we may need to verify the consumer identity before processing the consumer request. In some cases, we may need to collect additional information to verify the consumer identity/authorized agent's identity such as a government issued ID.

If a consumer has additional questions about the supplement or how to exercise a consumer's rights under the supplement, please contact us as specified in Section 11.

## Oregon Residents

Beginning July 1, 2024, the Oregon Consumer Privacy Act gives consumers certain rights with respect to the processing of consumer personal data.

This supplement informs on consumer rights as an Oregon resident and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

### Consumer Rights under the Oregon Consumer Privacy Act:

A consumer may: (a) Obtain from a controller: (A) Confirmation as to whether the controller is processing or has processed the consumer's personal data and the categories of personal data the controller is processing or has processed; (B) At the controller's option, a list of specific third parties, other than natural persons, to which the controller has disclosed: (i) The consumer's personal data; or (ii) Any personal data; and (C) A copy of all of the consumer's personal data that the controller has processed or is processing; (b) Require a controller to correct inaccuracies in personal data about the consumer, taking into account the nature of the personal data and the controller's purpose for processing the personal data; (c) Require a controller to delete personal data about the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source and derived data; or (d) Opt out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes: (A) Targeted advertising; (B) Selling the personal data; or (C) Profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance. A controller is not required to disclose the controller's trade secrets, as defined in ORS 646.461.

To exercise consumers' rights, a consumer can contact us as specified in Section 11.

Please note to protect a consumer's information and the integrity of our Service, we may need to verify the consumer identity before processing the consumer request. In some cases, we may need to collect additional information to verify the consumer identity/authorized agent's identity such as a government issued ID.

If a consumer has additional questions about the supplement or how to exercise a consumer's rights under the supplement, please contact us as specified in Section 11.

## Florida Residents

Beginning July 1, 2024, the Senate Bill 262 Technology Transparency Bill (the "Florida's Digital Bill of Rights") gives consumers certain rights with respect to the processing of consumer personal data.

This supplement informs on consumer rights as a Florida resident and should be read in conjunction with

our PRIVACY POLICY, which describes what information we collect and how we use it.

#### Consumer Rights under the Florida's Digital Bill of Rights:

501.705 Consumer rights.— 780 (1) A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller which specifies the consumer rights that the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise these rights on behalf of the child. (2) A controller shall comply with an authenticated consumer request to exercise any of the following rights: (a) To confirm whether a controller is processing the consumer's personal data and to access the personal data. (b) To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. (c) To delete any or all personal data provided by or obtained about the consumer. (d) To obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format. (e) To opt out of the processing of the personal data for purposes of: Targeted advertising; The sale of personal data; or Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer. (f) To opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data. (g) To opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature. (3) A device that has a voice recognition feature, a facial recognition feature, a video recording feature, an audio recording feature, or any other electronic, visual, thermal, or olfactory feature that collects data may not use those features for the purpose of surveillance by the controller, processor, or affiliate of a controller or processor when such features are not in active use by the consumer, unless otherwise expressly authorized by the consumer.

To exercise consumers' rights, a consumer can contact us as specified in Section 11.

Please note to protect a consumer's information and the integrity of our Service, we may need to verify the consumer identity before processing the consumer request. In some cases, we may need to collect additional information to verify the consumer identity/authorized agent's identity such as a government issued ID.

If a consumer has additional questions about the supplement or how to exercise a consumer's rights under the supplement, please contact us as specified in Section 11.

#### Montana Residents

Beginning October 1, 2024, the Consumer Data Privacy Act gives consumers certain rights with respect to the processing of consumer personal data.

This supplement informs on consumer rights as a Montana resident and should be read in conjunction with our PRIVACY POLICY, which describes what information we collect and how we use it.

## Consumer Rights under the Consumer Data Privacy Act :

- (1) confirm whether a controller is processing the consumer's personal data and to access the personal data, unless such confirmation or access would require the controller to reveal a trade secret;
- (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
- (3) delete personal data about the consumer;
- (4) obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance when the processing is carried out by automated means, provided the controller is not required to reveal any trade secret;
- (5) opt out of the processing of the consumer's personal data for the purposes of:
  1. targeted advertising; (B) the sale of the consumer's personal data, except as provided in [section 7(2) of the Consumer Data Privacy Act]; or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

To exercise consumers' rights, a consumer can contact us as specified in Section 11.

Please note to protect a consumer's information and the integrity of our Service, we may need to verify the consumer identity before processing the consumer request. In some cases, we may need to collect additional information to verify the consumer identity/authorized agent's identity such as a government issued ID.

If a consumer has additional questions about the supplement or how to exercise a consumer's rights under the supplement, please contact us as specified in Section 11.