VensureHR Privacy Policy

Overview

This Privacy Policy describes VensureHR, and our subsidiaries and affiliates collect, use, share, and protect business, financial, and personal information. This Policy applies to all information collected or submitted on this website and mobile applications ("Site"). This policy is available on the homepage of this Site and at every login page where personally identifiable information may be requested.

Purpose

Your privacy, and the privacy of the information provided, is important to us. We responsibly protect your data from loss, misuse, unauthorized access, disclosure, alteration, and untimely destruction. We do not grant access to your personal information except as otherwise set forth herein. We do not share or sell personal information collected on the Site with any third parties for their marketing purposes. At times, we will provide you with links to other websites. We encourage our users to be aware when they leave our Site, and to read the privacy statements of every website that collects personally identifiable information

Information Collection and Use

WHAT INFORMATION IS COLLECTED

We limit the collection of personal information to the information that we need to administer and improve the Site, to provide our products and services ("Services") to our customers, and to fulfill any legal and regulatory requirements.

THE CATEGORIES OF PERSONAL INFORMATION THAT WE COLLECT MAY INCLUDE, BUT ARE NOT LIMITED TO:

- Contact information to allow us to communicate with you.
- Company name, address, and business information to provide Services.
- If a quotation is requested, employee information, including Social Security number, date of birth, financial, bank account, biometric, geolocation, medical, and beneficiary information, to provide Services.
- Credit, debit, or cash/payment card information if used, such as for billing.
- Credit or debt history regarding your creditworthiness or credit history.
- Employment history and application information can be used to determine eligibility for a job opening via our recruiting page.

HOW PERSONAL INFORMATION IS COLLECTED

We do not require you to provide any personal information in order to have general access to the Site. However, to access or use certain information, features, or services at the site, you may be required to provide personal information.

PERSONAL INFORMATION IS PRIMARILY COLLECTED:

- When you utilize the services, we obtain the information we need to provide the services.
- From applications, forms, and other information you provide us on the site.
- When you establish an account or an account is established for you at the direction of your employer, to receive services.
- From survey information and/or Site registration.
- If you provide us with comments or suggestions, request information about our services, or contact our Customer Service Department via phone, email, or other forms of communication.
- From consumer and business reporting agencies regarding your creditworthiness or credit history.
- From third parties to verify information given to us.
- From information you may provide via social media.

SMS Terms And Conditions

By providing your mobile number and opting in to receive SMS (Short Message Service) messages from VensureHR, you consent to receive event-based text messages related to your account, services, customer support, alerts, and other information relevant to your relationship with VensureHR.

- **Message Type:** Event-based (messages are only sent in response to specific actions, triggers, or events).
- **Message Frequency:** Varies depending on your interaction with our services. You will only receive messages relevant to events such as account changes, service updates, appointment reminders, or transactional notices.
- **Message & Data Rates:** Standard message and data rates may apply.
- **Opt-Out Instructions:** You can opt out of SMS messages at any time by replying STOP to any message you receive. For help, reply HELP or contact us using the methods below.
- **Help:** Reply HELP for more information. You may also contact Vensure at 800.941.8731 or privacy@vensure.com
- **Use of Phone Numbers:** Your mobile number will be used solely for the purposes described in this policy. We will not sell your number or use it for unrelated marketing without additional consent.

Your consent to receive SMS messages is not a condition of purchasing any goods or services. See additional information on SMS messaging below. Carriers are not liable for delayed or undelivered messages

HOW PERSONAL INFORMATION IS USED

We use the information provided on the site to perform the services you request.

WE LIMIT THE COLLECTION OF PERSONAL CUSTOMER INFORMATION USED TO:

- Facilitate customer requested services, transactions, investments, distributions, and benefits.
- Provide superior service to our customers.

- Comply with legal, reporting, and regulatory requirements.
- Administer and improve our sites.
- Detect fraud or theft to protect our business and client information.
- Contact you with information on services, new services or products, or upcoming events.
- Facilitate applicant tracking and recruitment.

HOW AGGREGATED, NON-PERSONAL INFORMATION IS USED

We may collect general, non-personal, statistical information about the users of the site and our services in order to determine information regarding the use of our site and general information about our customers. We may also group this information to provide general aggregated data. The aggregated data will not personally identify any customers or visitors to the site.

HOW COOKIES ARE USED

A “cookie” is a piece of data that our site may provide to your browser while you are at our site. The information stored in a cookie is used for user convenience purposes, such as reducing repetitive messages, tracking helper tool versions, and retaining user display preferences. If a user rejects the cookie, they will be able to browse the site but will be unable to use our online application.

VensureHR may use third-party service providers to use cookies, web beacons, and similar technologies to collect or receive information from our site and elsewhere on the Internet and use that

information to provide measurement services and target ads. You can opt-out of this information tracking using a web browser that supports a “Do Not Track” functionality.

CHILDREN UNDER 13 YEARS OF AGE

This site is not intended for children under 13 years of age. We do not knowingly collect personal information from children under 13 years of age. All dependent data needed for benefits enrollment is customarily provided by the employee/guardian and kept secure as indicated in this policy.

Privacy Notice For California Consumers Only

This PRIVACY NOTICE FOR CALIFORNIA CONSUMERS supplements the information contained in the Privacy Statement of the VensureHR family of companies (collectively, “we,” “us,” or “our”) and applies solely to California consumers (“consumers” or “you”), effective January 1, 2020. We adopt this notice to comply with the California Consumer Privacy Act of 2018, as amended (“CCPA”) and other applicable California privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice. For purposes of this notice, a “third party” is an entity that is not a wholly owned or majority-owned and controlled subsidiary of the VensureHR family of companies.

CALIFORNIA PRIVACY RIGHTS

Under California Civil Code 1798, California residents with an established business relationship can request information about sharing their personal information with third parties for the third parties’ direct marketing purposes. If you are a California resident and would like more information, please contact your service provider.

PARTIES WITH WHOM INFORMATION MAY BE SHARED

Information is shared to facilitate the Services needed in order to properly and efficiently handle duties related to your account.

WE MAY SHARE INFORMATION WITH:

- Government agencies to fulfill legal, reporting, and regulatory requirements.
- Attorneys, accountants, and auditors.
- Credit reporting agencies to supply vendor references on client's behalf.
- Our employees, affiliated companies, subsidiaries, agents, and third-party service vendors to perform Services related to your account, to offer additional Services, perform analysis to determine qualification to receive future services, or collect amounts due.
- Banking and brokerage firms to complete payroll processing and securities transactions.
- Credit bureaus and similar organizations, 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 legal process, in a fraud investigation, an audit, or examination.
- Affiliated companies that you select on our site for the purposes of obtaining more information or a proposal for services.

HOW TO ACCESS AND CORRECT YOUR INFORMATION

Keeping your information accurate and up to date is very important. You can review or correct your account information by contacting a customer service representative. If you have an account at the site, you can make changes to your account information after you log in to the Site from your PC or wireless device and use the online tools. Note that some information changes may be made by or have to be done through your employer.

CHANGES TO THIS PRIVACY STATEMENT

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

Information We Collect

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer ("personal information").

WE COLLECT THE FOLLOWING CATEGORIES OF PERSONAL INFORMATION AS INDICATED BELOW:

CATEGORY	EXAMPLES	COLLECTED?
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	**YES**

B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)	A 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. Some personal information included in this category may overlap with other categories.	**YES**
C. Protected classification characteristics under California or federal law	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth, and related medical conditions), sexual orientation, veteran or military status, and genetic information (including familial genetic information).	**YES**
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	**YES**
E. Biometric information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints.	**YES**
F. Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	**YES**
G. Geolocation data	Physical location or movements.	**YES**
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information.	**YES**
I. Professional or employment-related information	Current or past job history or performance evaluations.	**YES**
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99))	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	**YES**
K. Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	**YES**

PERSONAL INFORMATION DOES NOT INCLUDE:

- Publicly available information from government records
- De-identified or aggregated consumer information
- Information excluded from the CCPA's scope, like:
    - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data.
    - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

WE OBTAIN THE CATEGORIES OF PERSONAL INFORMATION LISTED ABOVE FROM THE FOLLOWING CATEGORIES OF SOURCES:

- Directly from our clients, prospects, or employees. For example, from documents that our clients provide to us related to the services for which they engage us.
- Indirectly from our clients, prospects, or their employees. For example, through information we collect from our clients in the course of providing services to them.
- Directly and indirectly from activity on our website (www.vensure.com) or other portals. For example, from submissions through our website or website usage details collected automatically.
- From third parties that interact with us in connection with the services we provide. For example, from government agencies when we verify data associated with payroll processing and withholding tax payments.

We may also collect personal information about you from other categories of sources, such as our affiliates; our other clients; public and publicly available sources; our third-party referral partners, vendors, data suppliers, and service providers; partners with which we offer co-branded services or engage in joint event or marketing activities; social networks; news outlets and related media; and organizations with which you are employed or affiliated.

Use Of Personal Information

WE MAY USE OR DISCLOSE THE PERSONAL INFORMATION WE COLLECT FOR ONE OR MORE OF THE FOLLOWING BUSINESS PURPOSES:

- To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal information in order for us to prepare a proposal for services, we will use that information to prepare the proposal.
- To provide you with information, products, or services that you request from us.
- To provide you with email alerts, event registrations, and other notices concerning our products or services, or events or news, that may be of interest to you.
- To operate, manage, and maintain our business.
- To accomplish our business purposes and objectives.

- To communicate with you.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections.
- To improve our website and present its contents to you.
- For testing, research, analysis, and service offering development.
- For vendor management purposes.
- As necessary or appropriate to protect the rights, property, or safety of us, our clients, or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- To evaluate or conduct 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 information held by us is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

WE DO NOT, AND WILL NOT, SELL YOUR PERSONAL INFORMATION.

We may share your personal information within the VensureHR family of companies to provide services to you or in an effort to assess your needs and how we can help fulfill those needs.

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we require the recipient to keep that personal information confidential and secure, to not disclose that personal information to others, and to not use it for any purpose except performing the services related to the business purpose.

IN THE PRECEDING TWELVE (12) MONTHS, WE HAVE NOT DISCLOSED THE FOLLOWING CATEGORIES OF PERSONAL INFORMATION FOR A BUSINESS

- Category A: Identifiers
- Category B: California Customer Records Personal Information Categories
- Category C: Protected Classification Characteristics Under California or Federal Law
- Category D: Commercial Information
- Category E: Biometric Information
- Category F: Internet or Other Electronic Network Activity Information
- Category G: Geolocation Data
- Category I: Professional or Employment-Related Information
- Category K: Inferences Drawn from Other Personal Information

WE DISCLOSE YOUR PERSONAL INFORMATION FOR A BUSINESS PURPOSE TO OUR AFFILIATES AND/OR TO ONE OR MORE OF THE FOLLOWING CATEGORIES OF THIRD PARTIES:

- Third-party service providers.
- Administrators authorized by your organization.
- Licensors or third-party applications (if you access a third-party application on our services through a license agreement with a licensor).
- Other parties where required by law or to protect our rights.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

In the preceding twelve (12) months, we have not sold any personal information to third parties within the scope of the application of the CCPA.

Your Rights And Choices

The CCPA provides California consumers with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

ACCESS TO SPECIFIC INFORMATION AND DATA PORTABILITY RIGHTS

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past twelve (12) months.

ONCE WE RECEIVE AND CONFIRM YOUR VERIFIABLE CONSUMER REQUEST, WE WILL DISCLOSE TO YOU:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or sharing that personal information.
- The affiliates with whom we shared your personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information to a third party for a business purpose, separate lists identifying the personal information categories that each category of recipient obtained.

DELETION REQUEST RIGHTS

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

WE MAY DENY YOUR DELETION REQUEST IF RETAINING THE INFORMATION IS NECESSARY FOR US OR OUR SERVICE PROVIDERS TO:

- Complete the transaction for which we collected the personal information, provide a product or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, And Deletion Rights

TO EXERCISE THE ACCESS, DATA PORTABILITY, AND DELETION RIGHTS DESCRIBED ABOVE, PLEASE SUBMIT A VERIFIABLE CONSUMER REQUEST TO US BY EITHER:

- Calling us at 833-463-6068
- Emailing us at privacy@vensure.com
- Visiting vensure.com

Only you or a person registered with the California Secretary of State that you authorize to act on your behalf may make a verifiable consumer request related to your personal information.

YOU MAY ONLY MAKE A VERIFIABLE CONSUMER REQUEST FOR ACCESS OR DATA PORTABILITY TWICE WITHIN A TWELVE (12) – MONTH PERIOD. THE VERIFIABLE CONSUMER REQUEST MUST:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or that you are an authorized representative of a person about whom we collected personal information.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information

provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

RESPONSE TIMING AND FORMAT

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to ninety (90) days), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the twelve (12) – month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily usable and should allow you to transmit the information from one entity to another without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

NONDISCRIMINATION

We will not discriminate against you for exercising any of your CCPA rights.

UNLESS PERMITTED BY THE CCPA, WE WILL NOT:

- Deny you products or services.
- Charge you different prices or rates for products or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of products or services.
- Suggest that you may receive a different price or rate for products or services or a different level or quality of products or services.

Data Retention

We will retain your personal data only as long as necessary to fulfill the purposes for which it was collected, comply with our legal obligations, resolve disputes, and enforce our agreements.

How to Make a Request

You may make a request for the disclosures or deletion described above by contacting us using one of the methods described below methods.

You may be required to submit proof of your identity for these requests to be processed as a verifiable consumer request. We may not be able to comply with your request if we are unable to confirm your identity or to connect the information you submit in your request with personal information in our possession. You may designate an authorized agent to make a request on your behalf subject to proof of identity and authorization.

We will respond to your request consistent with the CCPA, which does not apply to certain information, such as information made available from government records, certain data subject to the (FCRA), (GLBA) and certain other laws, and where its application is preempted by, or in conflict with, federal law or the United States or the California Constitution.

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer ("personal information").

Changes To Our Privacy Notice

At a minimum, this notice will be reviewed and updated on an annual basis. We reserve the right to amend this notice at our discretion and at any time. Any changes will be posted on this page with an updated revision date.

Contact Information

If you have any questions or comments about this notice, our Privacy Statement, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us

- Toll Free Phone Number: 833-463-6068
- Email: privacy@vensure.com
- Website: www.vensure.com

First Class Mail, Return Receipt:

VensureHR

ATTN: HR Compliance Team

1475 S Price Rd

Chandler, AZ 85286

General Data Protection Regulations

LEGAL BASIS FOR PROCESSING – GDPR

- We process your personal data only when we have a legal basis, including providing the services or information that you have requested.
- Consent: When you have given us permission to process your personal data for a specific purpose.
- Contract: When processing is necessary to perform a contract with you or to take steps at your request before entering into such a contract.
- Legal Obligation: When we are required by law to process your personal data.
- Legitimate Interests: When we process your data to pursue our legitimate business interests and those interests are not overridden by your rights and interests.

RIGHTS UNDER THE GDPR

European Economic Area (EEA) residents have the right to:

- Access their personal data
- Rectify inaccurate data
- Erase their data (“right to be forgotten”)
- Restrict or object to processing
- Data portability
- Withdraw consent at any time

- Lodge a complaint with a supervisory authority

Rights Under the New York SHIELD Act

New York residents are entitled to reasonable administrative, technical, and physical safeguards to protect their private information.

Data Security

We implement reasonable organizational, technical, and physical security measures designed to protect your information in accordance with the SHIELD Act, GDPR, and CCPA. However, no electronic transmission or storage of information can be entirely secure, so we cannot guarantee absolute security.

Policy On Compliance With Telephone Consumer Protection Act 47 U.S.C. § 227 For Sending SMS Text Messages

INTRODUCTION

The Telephone Consumer Protection Act (TCPA), codified at 47 U.S.C. § 227, is a significant federal statute enacted to safeguard consumer privacy against unwanted telemarketing calls, faxes, and SMS (Short Message Service) text messages. This policy outlines VensureHR procedures and standards our organization will adhere to in order to ensure compliance with the TCPA when sending SMS text messages to consumers.

OBJECTIVE

The primary objective of this policy is to establish a framework that ensures all SMS text messages sent by our organization are in compliance with TCPA regulations, thereby protecting consumer rights and avoiding legal penalties.

SCOPE

This policy applies to all employees, contractors, and third-party vendors involved in the creation, approval, and dissemination of SMS text messages on behalf of our organization.

DEFINITIONS

- TCPA: The Telephone Consumer Protection Act, a federal law that restricts telemarketing calls, auto-dialed calls, prerecorded calls, text messages, and unsolicited faxes.
- SMS Text Message: A short message service text message, which can include marketing, informational, or transactional content.
- Consent: Prior express written consent from the consumer, which is required for sending marketing SMS text messages.

CONSENT REQUIREMENTS

To comply with TCPA regulations, our organization must obtain prior express written consent from consumers before sending any SMS text messages for marketing purposes. This consent should be:

- Explicit: Clearly stating that the consumer agrees to receive marketing messages via SMS.
- Written: Documented in written form, which can be electronic or physical.
- Voluntary: Given freely by the consumer without any coercion.

Transactional or informational SMS text messages may be sent without prior consent but must comply with applicable regulations.

OPT-OUT MECHANISM

Every SMS text message must include an opt-out mechanism, allowing consumers to easily and promptly unsubscribe from receiving future messages. This can be achieved by including instructions within the message, such as replying with “STOP” to opt-out.

DATA SHARING

No mobile information will be shared with third parties/affiliates for marketing/promotional purposes. All other categories exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties

DOCUMENTATION AND RECORD KEEPING

Our organization will maintain comprehensive records of consumer consent and opt-out requests. These records will include:

- Date and time consent was obtained.
- Method used to obtain consent.
- Copies of consent forms or applicable logs.
- Details or log of opt-out requests and confirmations.

MESSAGE CONTENT AND FREQUENCY

SMS text messages should be concise, relevant, and respectful of consumer privacy. Our organization will:

- Limit the frequency of messages to avoid overwhelming consumers.
- Ensure messages do not contain inappropriate or misleading content.
- Provide accurate information regarding the identity of the sender.

THIRD-PARTY VENDORS

Any third-party vendors involved in sending SMS text messages on behalf of our organization must comply with TCPA regulations. Our organization will conduct due diligence and establish contractual agreements to ensure vendors adhere to these standards.

TRAINING AND AWARENESS

Employees and contractors involved in SMS text messaging activities must receive regular training on TCPA compliance. This training will cover:

- Overview of TCPA regulations and requirements.
- Procedures for obtaining and documenting consumer consent.
- Opt-out mechanisms and record-keeping practices.

MONITORING AND ENFORCEMENT

Our organization will implement monitoring systems to ensure ongoing compliance with this policy. Non-compliance may result in disciplinary action, including termination for employees and contract termination for vendors.

REVIEW AND AMENDMENTS

This policy will be reviewed annually and amended as necessary to reflect changes in TCPA regulations or organizational practices. All amendments will be communicated to relevant stakeholders.

CONCLUSION

Adhering to TCPA regulations is crucial for maintaining consumer trust and avoiding legal penalties. This policy serves as a comprehensive guide to ensure our organization's SMS text messaging practices are compliant, respectful, and transparent.

Privacy Notice For Colorado, Connecticut, Nevada, Utah, & Virginia

This Notice, which forms part of our privacy policy, provides supplemental information for residents of Colorado, Connecticut, Nevada, Utah, and Virginia, regarding their rights under applicable state privacy laws. These include the Colorado Privacy Act (effective July 1, 2023); the Connecticut Personal Data Privacy Act (effective July 1, 2023); the Utah Consumer Privacy Act (effective December 31, 2023); and the Virginia Consumer Data Protection Act (effective January 1, 2023); and (collectively, the "Privacy Laws"). If you are a Consumer residing in Colorado, Connecticut, Utah, or Virginia, the following provisions may apply to our processing of information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer's ("personal information") as defined under the Privacy Laws.

Under the laws of Colorado, Connecticut, Utah, and Virginia, a 'Consumer' is defined as a resident acting in an individual or household context. This definition excludes individuals acting in an employment context (e.g., current, former, or prospective employees) or in a commercial context (e.g., employees, owners, directors, officers, or representatives of an entity engaging with us in that capacity).

Changes to This Privacy Statement

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

Categories of Personal Data

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer ("personal information").

WE COLLECT THE FOLLOWING CATEGORIES OF PERSONAL INFORMATION AS INDICATED BELOW:

1. Identifiers

A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.

2. Personal Information

Contact, name, employment information, financial, and educational information.

3. Protected Classifications

Race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, gender expression, gender identify, age, sexual orientation, military and veteran status.

4. Commercial Information

Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

5. Biometric Information

Colorado: Fingerprint, Voiceprint, Scan or record of an eye retina or iris, facial map, facial geometry, facial template, or other unique biological, physical, or behavioral patterns or characteristics.

"Biometric Information" does not include the following unless the biometric data is used for identification purposes: (i) a digital or physical photograph; (ii) an audio or voice recording; or (iii) any data generated from a digital or physical photograph or an audio or video recording.

This section does not apply to Connecticut, Utah, or Virginia.

6. Internet or other similar network activity

Mobile device and online identifiers, Mac address, IP address, cookie IDs, browser activity, search history, social media information, and information regarding your interaction with our website or mobile application.

7. Geolocation data

Physical location or movements

8. Demographic Information

Age, gender, race, citizenship, ethnicity, date of birth, family or marital status, household income, education, professional and employment information.

9. Profile information

Any form of automated process performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

10. Sensitive Data

Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child; or precise geolocation data.

WE OBTAIN THE CATEGORIES OF PERSONAL INFORMATION LISTED ABOVE FROM THE FOLLOWING CATEGORIES OF SOURCES:

- Directly from our clients, prospects, or employees. For example, from documents that our clients provide to us related to the services for which they engage us.
- Indirectly from our clients, prospects, or their employees. For example, through information we collect from our clients in the course of providing services to them.
- Directly and indirectly from activity on our website (www.vensure.com) or other portals. For example, from submissions through our website or website usage details collected automatically.
- From third parties that interact with us in connection with the services we provide. For example, from government agencies when we verify data associated with payroll processing and withholding tax payments.

We may also collect personal information about you from other categories of sources, such as our affiliates; our other clients; public and publicly available sources; our third-party referral partners, vendors, data suppliers, and service providers; partners with which we offer co-branded services or engage in joint event or marketing activities; social networks; news outlets and related media; and organizations with which you are employed or affiliated.

Use Of Personal Information

WE MAY USE OR DISCLOSE THE PERSONAL INFORMATION WE COLLECT FOR ONE OR MORE OF THE FOLLOWING BUSINESS PURPOSES:

- To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal information in order for us to prepare a proposal for services, we will use that information to prepare the proposal.
- To provide you with information, products, or services that you request from us.
- To provide you with email alerts, event registrations, and other notices concerning our products or services, or events or news, that may be of interest to you.
- To operate, manage, and maintain our business.
- To accomplish our business purposes and objectives.
- To communicate with you.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections.
- To improve our website and present its contents to you.
- For testing, research, analysis, and service offering development.
- For vendor management purposes.
- As necessary or appropriate to protect the rights, property, or safety of us, our clients, or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information.

- To evaluate or conduct 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 information held by us is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

WE DO NOT, AND WILL NOT, SELL YOUR PERSONAL INFORMATION.

We may share your personal information within the VensureHR family of companies to provide services to you or in an effort to assess your needs and how we can help fulfill those needs.

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we require the recipient to keep that personal information confidential and secure, to not disclose that personal information to others, and to not use it for any purpose except performing the services related to the business purpose.

WE DISCLOSE YOUR PERSONAL INFORMATION FOR A BUSINESS PURPOSE TO OUR AFFILIATES AND/OR TO ONE OR MORE OF THE FOLLOWING CATEGORIES OF THIRD PARTIES:

- Third-party service providers.
- Administrators authorized by your organization.
- Licensors or third-party applications (if you access a third-party application on our services through a license agreement with a licensor).
- Other parties where required by law or to protect our rights.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

Your Rights Under The CPA, CTDPA, UCPA, and VCDPA, and How To Exercise Them

Residents of Colorado [Colorado Privacy Act (CPA)], Connecticut [Connecticut Data Protection Act (CTDPA)], Utah [Utah Consumer Privacy Act (UCPA)], and Virginia [Virginia Consumer Data Protection Act (VCDPA)], have certain personal data rights.

- Opt-out of the processing of your personal data for purposes of:
    - Targeted advertising
    - Sale of personal data
    - Profiling that produces legal or significant effects on you
- Access your data and to confirm that your data is being processed by us.
- Request deletion of your data held by us.
- Request correction of your data held by us.
- Receive your requested data in a usable and transferable form.

- Non-discrimination or retaliation for exercising any of these rights.
- Designate an agent to exercise your rights on your behalf.
- Appeal if your request is denied.

REQUEST FOR DATA

Once We Receive And Confirm Your Verifiable Consumer Request, We Will Disclose To You:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or sharing that personal information.
- The affiliates with whom we shared your personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information to a third party for a business purpose, separate lists identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, unless otherwise permitted by law, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

WE MAY DENY YOUR DELETION REQUEST IF RETAINING THE INFORMATION IS NECESSARY FOR US OR OUR SERVICE PROVIDERS TO:

- Complete the transaction for which we collect the personal information, provide a product or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise fulfil our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, And Deletion

Rights

To Exercise The Access, Data Portability, And Deletion Rights Described Above, Please Submit A Verifiable Consumer Request To Us By Either:

- Calling us at 833-463-6068
- Emailing us at privacy@vensure.com
- Visiting vensure.com

YOU MAY ONLY MAKE A VERIFIABLE CONSUMER REQUEST FOR ACCESS OR DATA PORTABILITY TWICE WITHIN A TWELVE (12) – MONTH PERIOD. THE VERIFIABLE CONSUMER REQUEST MUST:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or that you are an authorized representative of a person about whom we collected personal information.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request. You may designate an authorized agent to make a request on your behalf subject to proof of identity and authorization.

RESPONSE TIMING AND FORMAT

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to ninety (90) days), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the twelve (12) – month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily usable and should allow you to transmit the information from one entity to another without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

APPEAL PROCESS

If you are a Colorado, Virginia, or Connecticut consumer, and we refuse to take action on your request, you may appeal our refusal within a reasonable period after you have received notice of the refusal. You may file an appeal by contacting us via email at privacy@vensure.com.

NONDISCRIMINATION

We will not discriminate against you for exercising any of your privacy rights.

Unless Permitted By The State Law, We Will Not:

- Deny you products or services.
- Charge you different prices or rates for products or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of products or services.

Suggest that you may receive a different price or rate for products or services or a different level or quality of products or services.

Nevada Privacy Rights

Privacy rights for residents of Nevada are governed by NRS Chapter 603A , enacted in 2005, and Senate Bill 220, enacted in 2019, granting Nevada consumers the ability to restrict the sale of their “Covered Information.” This term refers to one or more types of personally identifiable information collected by an operator through a website or online service operated by that entity, including:

- First and last name
- A home or other physical address that includes the street name and city or town
- Email address
- Telephone number
- Social Security number
- Any identifier that enables a specific individual to be contacted either physically or online
- Any other information collected from the individual via the operator’s website or online service and maintained in combination with an identifier in a way that renders the data personally identifiable

If you wish to submit an additional inquiry concerning the sale of your Covered Information, as defined by Nevada law, please contact us via email at privacy@vensure.com.

For additional details about how we collect, use, disclose, and sell Personal Information, please refer to our privacy policy. The policy can be accessed at the bottom of our main page, https://vensure.com/.

VensureHR Biometric Data Privacy Policy

1. Introduction

VensureHR ("Company," "we," or "us") has established the following Biometric Data Privacy Policy (the "Policy") for [type(s) of data subjects/end users, e.g., "clients,” “client employees,” “internal employees,” " "customer users," etc.] of the Company's biometric [type of biometric system, e.g., "authentication," "access control," etc.] system (the "Biometric System"). This Policy describes how the Company treats [type(s) of biometric data, e.g., facial images, face geometry, fingerprints, etc.], and other data that may be considered "biometric identifiers" or "biometric information" under applicable law (collectively, "Biometric Data") that is collected, obtained, and/or processed by the Company from [type(s) of data subjects/end users] through its operation of the Biometric System. The Company reserves the right to amend this Policy at any time, without notice.

2. Collection and Processing

Biometric systems are computer-based systems that scan an individual's face, finger, hand, or other physical feature for purposes of recognition and/or verification. These systems generate unique data points and create a unique mathematical representation, or algorithm, that is used to identify or verify an individual's identity, such as when an individual uses their face or fingerprint as an authentication measure to gain access to a restricted area or an electronic device. The Company's Biometric System operates by scanning and analyzing

[type(s) of data subjects/end users]s' Biometric Data to [recognize]/[verify] their identities.

Any Biometric Data collected or processed by the Company will be used solely for purposes of [processing purposes, e.g., "identity verification," "fraud prevention and detection," "security," "access control," etc.], and to comply with our legal obligations under applicable law. In the event we begin collecting or using Biometric Data in connection with the Biometric System for any additional purpose, we will update this policy. VensureHR will not sell or trade any Biometric Data that we receive from our clients and client employees.

3. Disclosures

We may disclose Biometric Data with our third-party service providers (e.g., cloud hosting providers) that assist with or otherwise facilitate our operation of the Biometric System, for purposes of [disclosure purposes, e.g., "when you request that we provide you with a product or service," "to facilitate your use of the Biometric System," etc.]. We may also disclose Biometric Data: (1) when required to do so by law; (2) when necessary to establish, exercise, or protect our rights; (3) to protect the vital interests of natural persons; (4) to investigate fraud or other criminal acts; or (5) in the context of merger, acquisition, or similar commercial transaction. Any Biometric Data disclosed by us will be solely for these purposes.

4. Retention and Destruction

Any Biometric Data collected, obtained, or otherwise processed by us will be permanently deleted if the Company receives a verifiable deletion request. Such requests may come from an employee, or a client request with a written agreement from the employee to discontinue the use of the biometric technology for any specific employee. Biometric Data may also be deleted due to the termination of a client's contractual relationship and deletion will be executed in accordance with VensureHR's client services agreement or the Company's record retention schedule, as applicable, whichever is earlier.

5. Security

We use a commercially reasonable standard of care, consistent with our industry, to store, transmit, and protect from disclosure, use, unauthorize access, or loss of any Biometric Data collected or otherwise obtained through use of the Biometric System. Such storage, transmission, and protection is performed in a manner that is the same as, or more protective than, the manner in which we store, transmit, and protect other forms of confidential and sensitive information, including personal information that can be used to uniquely identify an individual.

6. Contact Us

For more information, or if you have any questions about this Biometric Data Privacy Policy, you may contact us using the information below:

- Calling us at 833-463-6068
- Emailing us at privacy@vensure.com
- Visiting vensure.com

Last updated August 28, 2025